Mahaska County

HIPAA

Policies and Procedures Manual

Ver: 7.5.2017 17:01:04

This HIPAA Policies and Procedures Manual has been reviewed, accepted and approved by:

_____

The policies and procedures herein are effective as of:

_____

Administrative Safeguards

AS-100: Security and Privacy Program Specifications Formulating the HIPAA Compliance Plan

Purpose:

The privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA) are divided into administrative, physical and technical safeguard requirements -- now called "standards," in keeping with the language used in the HIPAA statute and the other rules. These requirements specify each of the implementation specifications (74 Security and 66 Privacy) needed to be addressed in Mahaska County's HIPAA Compliance Plan.

Formulating Mahaska County's HIPAA Compliance Plan is a necessary first step in achieving HIPAA compliance, which communicates to Mahaska County's Workforce members, Elected Officials and volunteers, Business Associates, and patients how Mahaska County secures Protected Health Information (PHI) and electronic Protected Health Information (ePHI).

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all Workforce members, Elected Officials and volunteers and non-employee workforce members who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

A HIPAA compliance plan is required to cover all the safeguards contained in both the federal regulations for HIPAA (74 Security and 66 Privacy). This overview discusses the general areas that ultimately encompass all the required safeguards:

- Naming a Chief Security Officer (CSO) and Chief Privacy Officer (CPO)
- Conduct an accurate and complete Security Risk Assessment (SRA)
- Conduct an accurate and complete Privacy Risk Assessment (PRA)
- Create a time phased Remediation Plan
- Remediate identified gaps in the Security and Privacy Plan
- Address Business Associate (BA) Relationships
- Training workforce members and volunteers

Procedures:

Mahaska County must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This

decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

1. Conduct an accurate and complete risk assessment (security and privacy)

   A comprehensive analysis of threats is conducted, as outlined in Policy and Procedure AS-210 "Risk Analysis," at least once every year, reviewed annually and updated as needed. The risk analysis comprehensively describes the provider's information system, including the following components:

   - Threat Identification
   - Vulnerability Identification
   - Control Analysis
   - Likelihood Determination
   - Risk Determination
   - Control Recommendation
   - Results Documentation
   - Risk Mitigation
   - Controls Selection

   Once completed, the Chief Technology Officer will determine and implement a risk management schedule for continuous review, assessment and update of the Security Risk Assessment.

2. Remediation plan

   Once threats and risks profiles have been identified, the CSO and CPO will create a time phased remediation plan to address each of the identified risks. The plan will include:

   - Segregation of risk categories into High, Medium and Low risk gaps.
   - Assigned responsibilities to remediate each of the gaps.
   - Identification of an individual to approve and sign off on the remediation of each of these gaps and the implementation of each safeguard.
   - Development of a time frame to implement each safeguard.

   High risk gaps will be remediated within 90 days, medium risk gaps within 120 days and low risk gaps within 180 days.

3. Privacy and Security Policies and Procedures

   Policies and procedures need to be updated regularly and any changes need to be clearly notated and communicated to workforce members. Elected Officials and volunteers. Policies and procedures, at the discretion of the CPO and/or CSO, will be segregated into groups, for regular review at 12, 24 or 36 months.

   Additionally, all policies and procedures will be reviewed and updated, as necessary when a security and/or privacy incident occurs. Additional review will occur when a breach is reported to a regulatory agency, as part of the investigation and remediation of the breach.

   Each policy and procedure is written to reflect the actual operational steps taken by the organization for that specific safeguard.

4. Business Associates
   Persons or entities outside Mahaska County's workforce who use or have access to PHI or ePHI in performing service on behalf of Mahaska County are identified as Business Associates. Each of these persons and/or entities is documented in the organization's Risk Assessment. Mahaska County will conduct due diligence on each person or entity identified as a business associate, as outlined in the Policy/Procedure AS-261 "Business Associate Due Diligence."

5. Training
   Mahaska County will train all employees, volunteers and contractors on the following basis, and as outlined in the Policy/Procedure AS-270 "Education and Training." Training will occur within the 90-day employee (volunteer and contractor) probationary period, quarterly, and as part of the remediation of a privacy/security incident and/or breach. Each individual will train on the specific Privacy and Security required for the individual to complete their assigned tasks. All training will be logged with:
   - Who has been trained,
   - When the training occurred,
   - Who conducted the training,
   - What regulations were covered by the training, and
   - A copy of the training will be maintained.

The log of this training shall be retained for the regulatory requirement of 6 years.

Applicable Standards and Regulations:

45 C.F.R. §164.306(d)(1)
45 C.F.R. §164.306(d)(2)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren	Darin Hite	

AS-105: Confidentiality and Privacy of PHI

Purpose:

In becoming compliant with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information and Technology for Economic and Clinical Health (HITECH) and the applicable rules issued by the Department of Health and Human Services (HHS), it is the policy of Mahaska County to maintain patient privacy and confidentiality at all times. Workforce members, Elected Officials and volunteers are specifically required to use and/or access protected health information (PHI) needed to reasonably accomplish the intended purpose only to the extent of the function and duties they are providing as employees of Mahaska County. We further maintain that all protected health information will be secured and continually protected during its collection, use, disclosure, dissemination, storage and destruction at Mahaska County.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All persons associated with Mahaska County including workforce members, Elected Officials, volunteers, contractors, vendors, auditors, researchers, administrators, members of the Board of Supervisors and /or agents of the above mentioned, shall be bound by this policy of Confidentiality and Privacy of PHI. All Mahaska County workforce members, Elected Officials, volunteers and persons associated with Mahaska County are responsible to be trained in Mahaska County's privacy policies and procedures for protecting the security and confidentiality of all PHI whether oral, written or electronic format. This applies to any PHI that is obtained, handled, learned, heard or viewed while in the course of their work or association with Mahaska County.

Policy:

Use or disclosure of PHI is acceptable only in the discharge of responsibilities and duties based on the need to know as minimally necessary. Discussion regarding PHI should not take place in the presence of persons not entitled to such information or in public places, such as break rooms, common hallways, and outdoor spaces immediately adjacent to the Mahaska County facilities, parking areas or off premises of Mahaska County. The execution of the confidentiality pledge as defined in Policy and procedure PR-110 "Pledge of Confidentiality" is required as a condition of employment/contract or other association appointment with Mahaska County. All persons associated with Mahaska County are to sign the Pledge at the commencement of their relationship with Mahaska County. Existing employees will sign the pledge.

Those who breach confidentiality/privacy will be subject to disciplinary actions as outlined in Policy and procedure AS-130 "Disciplinary Actions for Breach of Confidentiality/Privacy" and subject to the civil and/or criminal penalties pursuant to the HIPAA and HITECH laws and rules. All persons who become aware of a possible breach of confidentiality/privacy should report this incident, as outlined in Policy and procedure AS-170 "Reporting of Privacy Concern and Security Breach."

Procedures:

All workforce members and Elected Officials of Mahaska County, as a condition of employment are to sign a “Pledge of Confidentiality”. Human Resources is responsible for the distribution of this form to new workforce members and Elected Officials prior to starting employment at Mahaska County.

All others not included above, will sign the pledge at the time of signing a contract for services at Mahaska County. This will include auditors, consultants, vendors, and volunteers.

Applicable Standards and Regulations:

45 C.F.R. §164.502(a)
45 C.F.R. §164.502(b)
45 C.F.R. §164.514
45 C.F.R. §164.308(a)(4)(ii)(B)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-110: Minimum Necessary Use and Disclosure of PHI/ePHI

Purpose:

To establish a policy and procedure for compliance with the "minimum necessary" requirements of HIPAA, in order to limit unnecessary or inappropriate access, use and disclosure of PHI.

Responsible for Implementation:

Privacy Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

For purposes other than those listed below, the use and disclosure of PHI must be limited to the minimum necessary to accomplish the intended purpose of the disclosure or request for disclosure, or to complete the task at hand. Further, it shall be Mahaska County's policy to provide data/PHI in the following levels of detail:

A. To the extent practicable, provide the user with a limited data set to accomplish the intended purpose.
   Note: A limited data set excludes any identifiers of the individual, relatives, employers or household members that allow a user of the data to reasonably identify the individual.

B. Or, if necessary, per the determination of the county's Chief Privacy Officer (CPO) as to what constitutes the minimum necessary PHI/ePHI to accomplish the intended purpose.
   Note: The minimum necessary disclosure requirement is not imposed in any of the following circumstances:
   1. Disclosure to or a request by a health care or mental health provider to coordinate or provide treatment;
   2. Disclosure to an individual who is the subject of the information, or the individual's personal representative demonstrating appropriate authorization;
   3. Use or disclosure made pursuant to an authorization;
   4. Use or disclosure that is required by the most restrictive of applicable federal and state law or regulation;
   5. Disclosure to the U.S. Department of Health and Human Services (HHS) for complaint investigation, compliance review or enforcement; or
   6. Use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Procedures:

1. Use and Disclosure Limitations

   All persons who handle PHI/ePHI in any manner are expected to know and abide by the following protocols:

   A. Determining workforce access to PHI/ePHI - Access to the PHI will be granted based on the individual's role and determination by the individual's department head. Mahaska County will identify:
      a. Those persons or classes of persons in Mahaska County's workforce, including students, trainees and interns who need access to PHI to carry out their duties; and
      b. For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access;
   B. Requests for Uses or Disclosures of PHI- Except in emergency situations, any person requesting PHI/ePHI from Mahaska County must include the requestor's name, unique identifier, and the amount of information requested;
   C. Audits- Mahaska County's Chief Privacy Officer (CPO) will be responsible for facilitating random checks to ensure the minimum necessary standard is being applied when using and disclosing PHI/ePHI. The CPO will forward the results of the audit to the Board of Supervisors; and
   D. Requests for Uses or Disclosures of Entire Clinical Records -Mahaska County will not release the entire medical record to internal departments or business associates unless necessary. For example, a workforce member, a care provider or business associate should request the specific document containing the time period of the particular individual visit at issue, instead of the entire set of records.

2. Good Faith Reliance

   Mahaska County may rely on the belief that the PHI requested is the minimum amount necessary to accomplish the purpose of the disclosure when:

   A. The information is requested by another person previously approved for access, provided the first request for release of PHI specifies a time limit to the authorization and the request by the approved individual and that person's current request falls within the time limit and scope of information authorized for release by the person to whom the PHI belongs;
   B. The information is requested by a professional (such as an attorney or accountant) providing professional services either as an employee or as a business associate;
   C. Making disclosure to entities or agencies related to mental health or health related purposes that do not require consent, authorization or opportunity to agree or object and that official represents that the information is the minimum necessary or is required by law; Note: Psychotherapy notes are not considered part of a person's PHI/ePHI and may not be disclosed without the permission of the CSO and should not be disclosed without advice of counsel;
   D. Investigative Review Board (IRB) or privacy board documentation represents that proposed research meets the minimum necessary disclosure standard;
   E. A requester asserts that the information is necessary to prepare a research protocol; or

F. A requester asserts that the information is for research on decedents; and
G. In general, Mahaska County personnel may use PHI/ePHI for treatment purposes although PHI/ePHI may not be released beyond Mahaska County, an affiliated healthcare provider, business associate, or other organization having executed a Data Use Agreement.

3. Disclosures for Payment
   Only the minimum necessary PHI shall be disclosed for payment functions, as provided through contractual agreement. Persons handling PHI in a payment context shall refrain from publicizing individual diagnosis or treatment information. This policy shall apply to checks collected, credit card paper receipts, and envelopes and invoices sent to consumers.

4. Disclosures Required by Law and Disclosures Ordered by a Court or Administrative Tribunal
   The minimum necessary standard does not apply to disclosures ordered from an administrative tribunal or by order of court. Only the information directly requested by such an order is to be provided. The minimum necessary standard shall apply to information released to law enforcement regarding victims of crime or abuse. However, if the law requires information to be released, then the disclosure will be in compliance with the subpoena, statute, law or regulation.

5. Disclosures for Worker's Compensation
   PHI, exclusive of session notes, may be disclosed to comply with Worker's Compensation laws and regulations without consent, authorization, or opportunity to object by the individual, but such disclosure shall still only be the minimum necessary. Requests for entire records should be scrutinized and approved by Mahaska County's Chief Privacy Officer (CPO) and Clinical Director.

6. Disclosures to Family and Friends
   Persons with access to and authority to disclose PHI may only make disclosures in accordance with Policy/Procedure PR-160 "Uses and Disclosures of PHI to Family and Friends" as noted in that section of Mahaska County's HIPAA Master Manual.

7. Minimum Necessary Use and Disclosure for Students, Trainees and Interns
   Students, trainees and interns are to adhere to the minimum necessary disclosure standard. Students, trainees and interns are not exempt from following the rules outlined in this policy. Students, trainees and interns are considered to be part of the treatment process if they are actively involved in the individual's care, and therefore are not limited in their access or use of the individual's medical information.

8. Minimum Necessary Use and Disclosure for Educational Purposes
   Instructors, supervisors, course facilitators, staff, interns, students, and trainees are to use de-identified information when in a classroom setting and the individual's identifying information (i.e. name, DOB, address, etc.) is not needed for the educational purpose.

9. Enforcement

All Elected Officials, Department Heads, supervisors and management personnel are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate applicable county disciplinary process.

Applicable Standards and Regulations:

45 CFR §164.502(b)
45 CFR §164.514(d)
45 CFR §164.308(a)(3)(ii)(A) and (B)
45 CFR §164.308(a)(4)(ii)(B)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-120: Implementation Specifications: Administrative, Physical and Technical Standards

Purpose:

The privacy and security regulations of the Health Insurance Portability and Accountability Act (HIPAA) are divided into administrative, physical and technical safeguard requirements -- now called "standards," in keeping with the language used in the HIPAA statute and the other rules. These requirements specify each of the implementation specifications (74 Security and 66 Privacy) needed to be addressed in Mahaska County HIPAA Compliance Plan.

The three safeguard categories are further divided into "implementation specifications" that delineate how each of the standards is to be implemented. In some cases, the standard itself contains enough information to describe implementation requirements, so there is no separate specification. (Note that in an earlier version of the rule, standards were called "requirements," and implementation specifications were called "implementation features.")

The Security Rule has both "required" and "addressable" provisions for its administrative, physical and technical safeguards.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

If an implementation specification is described as “required,” the specification must be implemented. The concept of "addressable” implementation specifications was developed to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification:

(a) implement the addressable implementation specifications;
(b) implement one or more alternative security measures to accomplish the same purpose;
(c) not implement either an addressable implementation specification or an alternative.

Procedures:

Mahaska County must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

Decisions made by Mahaska County regarding addressable specifications will be documented in writing and retained for a period of 6 years.

The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

Applicable Standards and Regulations:

45 C.F.R. §164.306(d)(1)
45 C.F.R. §164.306(d)(2)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-122: Asset Inventory

Purpose:

Mahaska County's information assets shall be properly inventoried, and classified in terms of their sensitivity and criticality. Asset types include information, information systems, computers, and electronic storage media.

Responsible for Implementation:

Chief Security Officer and/or designated IT Director

Scope:

This standard is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store electronic protected health information (ePHI) which is shared across the network and accessed by workforce members, Elected Officials and volunteers and/or Departments.

Policy:

Mahaska County shall maintain enterprise-wide inventories (registries) of assets. The designated owner of each information asset shall maintain accurate information about the asset in the appropriate registry.

Procedures:

Workforce members are responsible for understanding the classification level of the information that they handle, the restrictions on their use of that information, and their assigned data protection responsibilities.

Workforce members should access protected information only as authorized, and in the case of electronic information, only from authorized computers and locations.

Information Systems

1. The designated Owner of each Mahaska County System is responsible for providing accurate and timely inventory information to the appropriate registry.
2. The System Owner must ensure that the information that is created, received, stored and/or transmitted by the System has been accurately classified. If a System must handle Mahaska County protected information, the System's security controls must meet the minimum baseline data protection standards for Mahaska County's protected information.
3. Each User of a System must be aware of the System's requirements for information handling and data protection.

Computers

1. The owner or administrator of each Mahaska County computer is responsible for providing accurate and timely inventory information to the appropriate registry. This includes servers,

workstations, laptops and other portable computers, and smartphones and other interactive electronic devices.

2. If a computer must be used to store Mahaska County protected information, then the computer's location and its contents must be accurately tracked and documented at all times.

Electronic Storage Devices and Media

If an electronic storage device or other digital medium must be used to store Mahaska County protected information, then the location and the contents of the device or medium must be accurately tracked and documented at all times.

Applicable Standards and Regulations:

45 C.F.R. §164.308(a)(1)(i)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-125: Development and Maintenance of Privacy Policies and Procedures

Purpose:

Mahaska County's Chief Privacy Officer (CPO) shall be responsible for developing and maintaining written privacy policies and procedures pursuant to the Health Insurance Portability and Accountability Act (HIPAA) privacy standards.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

The HIPAA Privacy Rule requires the implementation and maintenance of policies in written or electronic form. This policy is designed to give guidance and ensure compliance with provisions of HIPAA requiring covered entities to implement and maintain documentation of policies, procedures, and other administrative documents.

Procedures:

Mahaska County's CPO will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for the protection of the privacy of health information. The CPO may delegate this responsibility to a workforce member, but such delegation must be reflected in that workforce member's job description, and the CPO will supervise the development of all privacy policies and procedures. The CPO must:

1) Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures;
2) Notify Mahaska County's Board of Supervisors and HIPAA compliance team, and affected business associates of the issuance of new or revised federal or state requirements (as pertinent) and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented;
3) Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations; and
4) Identify any revisions needed in the privacy orientation and training program to reflect revised policies and procedures. Before a revised policy or procedure is submitted for

approval, the CPO will review the Notice of Privacy Practices form and determine whether the notice must be revised to reflect the new privacy policies or procedures. The effective date of a revised policy or procedure must not be earlier than the date on which the revised notice of privacy practices is posted and made available to individuals. All policies and procedures must be approved by the Board of Supervisors and be reviewed to conform with any guidance from any government agencies (e.g., Medicare or Medicaid) with responsibility for relevant oversight of the county before they can be implemented.

New or revised policies and procedures are to be communicated to workforce members, Elected Officials and volunteers using one or more of the following means:

1) An all-county memorandum from the CPO will announce the adoption of the new or revised policies and indicate affected workforce members. Elected Officials and volunteers functions. This memorandum must describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for review.
2) The CPO or a designated representative will announce the adoption of the new policies at appropriate county and workforce members. Elected Officials and volunteers meetings and provide appropriate training.
3) A memorandum from the CPO to workforce members, Elected Officials and volunteers whose job responsibilities are directly affected by the new policies should indicate whether training or orientation meetings or programs will be held and whether background information on the new policies is available. A copy of the revised policy should be attached to the memorandum, or workforce members, Elected Officials and volunteers should be directed to consult the updated policy and procedure manual.
4) Copies of the revised policy will be distributed to Department Heads and Elected Officials and for updating their copies of Mahaska County's HIPAA Master Policy and Procedure Manual.

Applicable Standards and Regulations:

45 CFR §164.316(a)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-130: Disciplinary Actions for Breach of Confidentiality, Privacy or Security Sanctions and Penalties

Purpose:

Following a full investigation, appropriate sanctions will be brought against employees and county associates who have been found to have violated Mahaska County's privacy countys.

Responsible for Implementation:

Chief Privacy Officer, Chief Security Officer, Board of Supervisors

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) or electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created, used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires that covered entities have and apply appropriate sanctions against workforce members who violate the privacy policies and procedures, and that Mahaska County maintain documentation of such sanctions. Further, the HIPAA Privacy Rule prohibits covered entities from engaging in intimidating or retaliatory acts against individuals or others in certain circumstances. This policy is designed to give guidance to all Mahaska County workforce members, Elected Officials and volunteers and ensure compliance with all applicable laws and regulations related to sanctioning for violating the Mahaska County's Privacy Policies and Procedures.

Procedures:

1. General

There are two types of violations of privacy policies and procedures:

A. Technical violations that do not result in the use or disclosure of PHI; and

B. Violations that do involve the use or disclosure of PHI.

There also are two types of violations that involve use and disclosure:

A. Unintentional or accidental uses or disclosures; and

B. Intentional and deliberate uses and disclosures.

Incidental disclosures of information, such as disclosures that occur when a individual asks a question in a public area or the individual's name is called out in a lobby to summon him or her to a private area do not constitute violations and need not be reported, documented or investigated. No sanction will be imposed for incidental disclosures of information. Workforce members. Elected Officials and

volunteers members should nevertheless make reasonable efforts to minimize incidental disclosures, such as using the individual's first name only when summoning him or her from a public waiting area.

The severity of penalties varies with the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.

Examples of violations include:

- Technical violations, such as occurs when obtaining an authorization, a workforce member fails to notice that the individual signed but did not date the authorization form;
- Accidental disclosure, such as occurs when information on the wrong individual is accidentally sent to a third-party payer;
- Intentional disclosure, such as occurs when a workforce member provides a drug representative a list of individuals with an identified medical condition without obtaining the individual's authorization for this disclosure.

2. Sanctions and Penalties – General

Mahaska County's CPO shall establish and maintain files that document all actions taken to impose sanctions under this policy. The procedures and penalties that apply to each of these types of violation are defined below.

This information shall include:

A. A description of, and documenting evidence for, the violation;

B. A statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional; and

C. A description of the sanction that was imposed.

An unproven or unsubstantiated allegation of a violation of privacy policies and countys does not have to be documented.

3. Sanctions and Penalties - Technical Violations Not Involving Use or Disclosure

A workforce member who commits a technical violation of privacy policies and procedures that does not result in any use or disclosure of PHI will:

A. Meet with his or her supervisor to review the policies and procedures that were violated; and

B. Demonstrate to the satisfaction of the supervisor that he or she understands the policies and procedures that should be followed in similar circumstances.

The violation will be documented in the workforce members. Elected Officials or volunteers' personnel file. A pattern of repeated technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the workforce member.

4. Sanctions and Penalties - Unintentional Violations Involving Use and Disclosure

A workforce member, Elected Official and volunteer who unintentionally uses or discloses PHI in violation of the privacy policies and procedures will:

A. Meet with his or her supervisor to review the policies and procedures were violated and the workforce members, Elected Officials and volunteers' authority to use or disclose PHI; and

B. Demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under the county's policies and procedures.

The violation will be documented in the workforce member, Elected Official or volunteer's personnel file. A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension, or termination of the workforce member, Elected Official and volunteer.

5. Sanctions and Penalties for Intentional Violations Involving Use and Disclosure

The intentional violation of privacy policies and procedures may result in immediate suspension, pending further investigation and termination. Documentation of the investigation of the violation must show clear evidence that the disclosure of information was intentional and deliberate. That is, the workforce member, Elected Official or volunteer must have disclosed the information knowing that the disclosure violated the policies and procedures of the county. If the workforce member, Elected Official or volunteer has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presumed that the disclosure was intentional. A finding that the person intentionally disclosed PHI may result in further sanction up to and including termination of employment or other contractual relationships with Mahaska County.

Applicable Standards and Regulations:

45 CFR §164.308(a)(1)(ii)(C)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-132: Termination Procedure

Purpose:

Mahaska County has adopted this policy and procedure to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services (HHS) security and privacy regulations, as well as acknowledge our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All workforce members, Elected Officials and volunteers of Mahaska County must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every workforce members, Elected Officials and volunteers' responsibilities.

Responsible for Implementation:

Chief Security Officer

Scope:

All persons associated with Mahaska County including workforce members, Elected Officials, volunteers, contractors, vendors, auditors, researchers and /or agents of the above mentioned, shall be bound by this Termination policy. All Mahaska County workforce members, Elected Officials, volunteers and persons associated with Mahaska County are responsible to be trained in Mahaska County's privacy policies and procedures for protecting the security and confidentiality of all PHI whether oral, written or electronic format. This applies to any PHI that is obtained, handled, learned, heard or viewed, while in the course of your work or association with Mahaska County.

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This applies to any PHI that is obtained, handled, learned, heard or viewed, while in the course of work or association with Mahaska County. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

All Mahaska County workforce members, Elected Officials and volunteers and persons associated with Mahaska County are responsible to be trained in Mahaska County's privacy policies and procedures for protecting the security and confidentiality of all PHI whether oral, written or electronic format.

Policy:

If a Mahaska County workforce member, Elected Official or volunteer's employment or relationship with the County is terminated or if a Mahaska County workforce member, Elected Official or volunteer leaves Mahaska County, the supervisor or manager must immediately notify Human Resources and the IT Director and ensure that all system or application accounts with access to PHI are terminated.

Procedures:

Department Heads and Elected Officials are responsible for notifying the manager of Information Systems of workforce members and others, such as independent contractors, who will be leaving Mahaska County's employment or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to health information.

Mahaska County Elected Officials and Department Heads are responsible for notifying the IT Director of employees and others, such as independent contractors, who through reassignment or otherwise no longer need the level of access that they had had so that their level of access can be adjusted.

Any other data user who becomes aware that a data user is leaving Mahaska County's employment, either permanently or for an extended or unexplained absence, should report the matter to their Elected Official, Department Head or IT Director for a determination of whether to revoke/suspend that person's access.

Upon termination of a Mahaska County workforce member, Elected Official, volunteer or other person with access, the Director of IT will immediately take the following actions:

- Revoke access privileges, such as user IDs and passwords, to system and data resources and secure areas.
- Retrieve all hardware, software, data, access control items, and documentation issued to or otherwise in the possession of the data user.
- Arrange for an exit briefing to verify retrieval of all items, to discuss any security/confidentiality concerns with the data user, and to remind the data user of the continuing need to protect data security and patient confidentiality.
- Notify the appropriate Elected Official or Department Head of completion of the termination procedure so that the data user can receive any final pay due.
- Keep records of the termination procedure for each such person, including the retrieval of security related items, such as passwords, and information system assets, for not less than six years from the termination date.

When necessary, the Mahaska County Elected Official, Department Head or CSO will arrange for security escort of terminated personnel from the facility and for an immediate audit of their accounts to detect any security or confidentiality threats or breaches.

Applicable Standards and Regulations:

45 C.F.R. §164.308(a)(3)(ii)(C)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version
Implementation Date:

Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-134: Workforce Clearance Procedure

Purpose:

This policy reflects Mahaska County's commitment to ensure that all workforce members have appropriate authorization to access Mahaska County information systems containing protected health information (PHI) and electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

The background of all Mahaska County workforce members and volunteers must be adequately reviewed during the hiring process. When defining an organizational position, Human Resources and the hiring Elected Official or Department Head must identify and define both the security responsibilities of and level of supervision required for the position. All Mahaska County workforce members, Elected Officials and volunteers who access Mahaska County information systems containing PHI/ePHI must sign a confidentiality agreement. All Mahaska County workforce members, Elected Officials and volunteers must also sign a "conditions of employment" document that states their commitment to and understanding of their responsibility for the protection of the confidentiality, integrity, and availability of Mahaska County's protected health information.

Procedures:

The background of all Mahaska County workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks include, but are not limited to:

- Character references
- Confirmation of claimed academic and professional qualifications
- Professional license validation

When defining a position, Human Resources and the hiring Elected Official or Department Head must identify the security responsibilities and supervision required for the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of Mahaska County information systems or processes.

When job candidates are provided via an agency, Mahaska County's contract with the agency must clearly state the agency's responsibilities for reviewing the candidates' backgrounds.

It is the responsibility of each Mahaska County department that retains the services of a third party to ensure that the party or person(s) adheres to all appropriate Mahaska County policies.

All Mahaska County workforce members who access Mahaska County information systems containing ePHI must sign a confidentiality agreement in which they agree not to provide ePHI or to discuss confidential information to which they have access to unauthorized persons. Confidentiality agreements must be reviewed and signed annually by Mahaska County workforce members who access Mahaska County information systems containing ePHI.

Applicable Standards and Regulations:

45 CFR 164.308(a)(3)(ii)(B)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-135: Security Reminders

Purpose:

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to the confidentiality, integrity and availability of protected health information (PHI) and electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer and Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created, used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall publish periodic notices and security updates to maintain awareness of security procedures and sound security practices. Notices shall be prepared whenever significant new security threats are identified, whenever security features of computer hardware and software are revised or updated, and whenever the county's Chief Security Officer (CSO), Chief Privacy Officer (CPO) or Board of Supervisors believes that a security incident warrants calling the attention of workforce members, Elected Officials and volunteers to security policies and procedures.

Procedures:

Mahaska County's CSO is responsible for preparing, distributing, and issuing security notices and related updates to security policies, as well as providing training on such changes as needed or requested by Mahaska County's workforce. Similarly, the county's CPO is responsible for preparing, distributing, and issuing privacy notices and related updates to privacy policies, as well as providing training on such changes as needed or requested by Mahaska County's workforce members, Elected Officials and volunteers. The county's Board of Supervisors may require that such notices or policies be developed and training be provided as deemed necessary.

Policies, procedures and training shall be accomplished in a timely manner once the need has been assessed and policy and procedure notices, changes or training are deemed to be in the best interests of Mahaska County's clients and/or the county.

Applicable Standards and Regulations:

45 CFR § 164.308(a)(5)(ii)(A)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-140: Job Description - Chief Privacy Officer

Purpose:

The purpose of the Chief Privacy Officer (CPO) is to ensure that Mahaska County has an established mechanism for authorizing and an individual responsible for the development, implementation and dissemination of a comprehensive set of county privacy policies, as well as to monitor compliance with those policies.

Responsible for Implementation:

Board of Supervisors

Scope:

The CPO shall support the county's Chief Security Officer (CSO) and report to the Board of Supervisors.

Policy:

Mahaska County shall provide for and support the role of a Chief Privacy Officer (CPO) with the responsibilities listed below. The CPO shall support the county's Chief Security Officer and report to the Board of Supervisors. This job description will be reviewed annually and updated as needed for compliance with HIPAA laws and regulations.

Procedures:

The CPO shall –

A. Ensure that there are county privacy and security policies that comply with the federal, state, county and city legal and county privacy guidelines related to patient information;
B. Oversee the development and dissemination of privacy standards and documented procedures to implement the county's privacy policies;
C. Coordinate development and implementation of county privacy policies and procedures with the Board of Supervisors and related support personnel to ensure that policies and procedures are developed in keeping with the county's obligations, values, and ability to faithfully implement them;
D. Coordinate with the Board of Supervisors and County Attorney in all patient privacy related legal matters;
E. Coordinate with partners and business associates to ensure that their PHI privacy policies and standards enable Mahaska County to meet its responsibility to maintain and protect PHI and sensitive county data;
F. Direct and monitor the conduct of training for workforce members, Elected Officials, volunteers, supporting contractors and business associates, as necessary to ensure organizational and individual awareness of county privacy policies, standards and procedures;

G. Oversee and monitor all HIPAA and HITECH compliance activities, as outlined in Mahaska County's Master HIPAA Manual;
H. Coordinate with each internal and/or external regulatory body as required by law and/or county policy to ensure timely and accurate reporting of county compliance efforts and to facilitate county and/or governmental agency compliance reviews and security audits;
I. Maintain a working knowledge of all applicable federal, state, county, city and county privacy regulations and policies; and
J. Perform all other tasks and responsibilities as needed to ensure county compliance with relevant regulatory and county privacy requirements.

Qualifications:
The CPO shall –

A. Possess a working knowledge of governmental privacy regulations; and
B. Demonstrate organizational, management and communication insight and skills sufficient to accomplish the above listed responsibilities.

Applicable Standards and Regulations:

45 CFR § 164.503(a)(2)
45 CFR § 164.530

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-145: Job Description - Chief Security Officer

Purpose:

The purpose of the Chief Security Officer (CSO) is to ensure that Mahaska County has an established mechanism for authorizing and an individual responsible for the development, implementation and dissemination of a comprehensive set of county security policies, as well as to monitor compliance with those policies.

Responsible for Implementation:

Board of Supervisors

Scope:

The CSO shall support the county's Chief Privacy Officer (CPO) and report to the Board of Supervisors.

Policy:

Mahaska County shall provide for and support the role of a Chief Security Officer (CSO) with the responsibilities listed below. The CSO shall support the county's Chief Privacy Officer (CPO) and report to the Board of Supervisors. This job description will be reviewed annually and updated as needed for compliance with HIPAA laws and regulations.

Procedures:

The CSO shall –

A. Ensure that there are county security policies that comply with the federal, state, county and city legal and security guidelines related to individual information;
B. Oversee the development and dissemination of security standards and documented procedures to implement the county security policies;
C. Coordinate development and implementation of county security policies and procedures with the Board of Supervisors and related support personnel to ensure that policies and procedures are developed in keeping with the county's obligations, values, and ability to faithfully implement them;
D. Coordinate with the Board of Supervisors and County Attorney in all individual security related legal matters;
E. Coordinate with partners and business associates to ensure that their PHI security policies and standards enable Mahaska County to meet its responsibility to maintain and protect PHI and sensitive county data;
F. Direct and monitor the conduct of training for workforce members, Elected Officials, volunteers, supporting contractors and business associates, as necessary to ensure organizational and individual awareness of county security policies, standards and procedures;
G. Oversee and monitor all HIPAA and HITECH compliance activities, as outlined in Mahaska County's Master HIPAA Manual;

H. Coordinate with each internal and/or external regulatory body as required by law and/or county policy to ensure timely and accurate reporting of county compliance efforts and to facilitate county and/or governmental agency compliance reviews and security audits;
I. Maintain a working knowledge of all applicable federal, state, county, city and county security regulations and policies; and
J. Perform all other tasks and responsibilities as needed to ensure county compliance with relevant regulatory and county security requirements.

Qualifications:
The CSO shall –

A. Possess a working knowledge of governmental security regulations; and
B. Demonstrate organizational, management and communication insight and skills sufficient to accomplish the above listed responsibilities

Applicable Standards and Regulations:

45 CFR §164.308(a)(2)(i)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-150: Non-Retaliation Policy

Purpose:

Mahaska County is committed to protecting the privacy and security of protected health information (PHI) as mandated by city, state, and federal laws and regulations and expects its Workforce members, Elected Officials and volunteers and affiliates to report actual or suspected violations of confidentiality laws and regulations without fear of retaliation.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All Elected Officials and Department Heads are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

Policy:

All Mahaska County Workforce members, Elected Officials and volunteers have a personal obligation to report any activity that appears to violate applicable laws, regulations, rules, policies, procedures, or standards of conduct through the normal administrative process and procedures. Concerns should first be directed to the Chief Privacy Officer (CPO). However, individuals may also make reports to the Secretary of the Department of Health and Human Services (HHS).

Procedures:

Mahaska County shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against the following individuals or in the following situations:
Any individual, patient, legally authorized representative, workforce member, Elected Official and volunteer, association, organization or group that in good faith:

1. Discloses or threatens to disclose information about a situation they feel is inappropriate, or potentially illegal;
2. Provides information to or testifies against the alleged offending individual or Mahaska County;
3. Objects to or refuses to participate in an activity they feel are in violation of federal and state law, Mahaska County policy, regulatory or accrediting agencies;
4. Is involved in any compliance review or peer review process; or files a valid or legitimate report, complaint or incident report.

Mahaska County will not require individuals to waive these rights as a condition of treatment, payment, enrollment in a health plan or eligibility for benefits or full, part-time or contracted employment.

Investigation of Retaliation

The CPO will review any allegation of retaliation and will ensure that a proper investigation is conducted as appropriate. Mahaska County will not intimidate, threaten, coerce, discriminate against or take any other action against an individual for the exercise of any right to file a complaint under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information and Technology for Economic and Clinical Health (HITECH) Act or their related rules and regulations.

Applicable Standards and Regulations:

45 C.F.R. §164.530(g)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-155: Fax Transmittal of PHI

Purpose:

It is Mahaska County's policy to fax only de-identified PHI to the recipient wherever possible. Only authorized Mahaska County persons will send faxes containing PHI without prior approval. If a non-authorized sender believes it is necessary to send PHI using fax communications, the sender must get the approval of an authorized individual before sending the fax with the PHI.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All Elected Officials, Department Heads and supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

Policy:

Mahaska County protects the facsimile transmittal of PHI and holds individuals responsible for following the proper procedure when PHI is sent via facsimile. Mahaska County protects the confidentiality and integrity of confidential medical information as required by federal and state law, professional ethics, and accreditation requirements. This policy defines the minimum guidelines and procedures that must be followed when transmitting patient information via facsimile.

Procedures:

All workforce members, Elected Officials and volunteers must strictly observe the following standards relating to facsimile communications of patient medical records:

PHI will be sent by facsimile only when the original record or mail delivered copies will not meet the needs for Mahaska County. For example, personnel may transmit PHI by facsimile when urgently needed or required by a third-party payer for ongoing certification of payment for a patient.

The procedure for sending PHI using a fax will be:

1. The non-authorized Mahaska County sender will get approval from an authorized person before sending the fax and the PHI.
2. The Mahaska County sender will confirm the fax number of the person to whom the fax and PHI is being sent in advance of sending the fax.
3. The Mahaska County sender will use a Mahaska County fax cover sheet emphasizing the privacy of the attached information and that it is to be used for the intended purposes only (see Policy and Procedure PR-155a "Facsimile Cover Sheet").
4. The Mahaska County sender will confirm that the person to whom the fax is sent does receive the fax and attachments.

Information transmitted must be limited to the minimum necessary to meet the requester's needs. Mahaska County will determine the minimum necessary to accomplish the intended purpose. Except as authorized by the individual's consent, a properly completed and signed authorization must be obtained from the patient before releasing PHI for purposes other than treatment, payment or operations.

The following types of confidential medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization, unless required by law:

1. Psychotherapy (records of treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist);
2. Other professional services of a licensed psychologist;
3. Social work counseling/therapy;
4. Domestic violence victims' counseling;
5. Sexual assault counseling of HIV test results (Patient authorization required for EACH release request.);
6. Records pertaining to sexually-transmitted diseases; or
7. Alcohol and drug abuse records protected by federal confidentiality rules.

The Facsimile Cover Sheet must be used to send faxes containing PHI. All pages plus the cover page of all confidential documents to be faxed must be marked "Confidential" before they are transmitted. Personnel must make diligent efforts to ensure that they send the facsimile transmission to the correct destination including: Preprogramming frequently used numbers into the machine to prevent misdialing errors. Mahaska County will periodically and/or randomly check all speed-dial numbers to ensure their validity, accuracy, and authorization to receive confidential information. For a new recipient, the sender must verify the fax number by requesting the recipient submit a faxed or e-mail request for PHI, which would include the fax number of the recipient. Periodically, we remind those who are frequent recipients of PHI to notify Mahaska County if their fax number is to change.

<u>Procedure for Faxes Sent Successfully</u>

For Mahaska County purposes

The department sending the fax for Mahaska County purposes is not required to maintain a copy of the fax transmittal or fax confirmation sheet. However, at the discretion of Management, a copy may be maintained for future reference.

For Non- Mahaska County purposes

Individuals faxing medical information for non- Mahaska County purposes (external) and without a signed authorization from the patient must account for the Non- Mahaska County disclosure, per policy.

<u>Procedure for Misdirected Faxes (for both Mahaska County and non-Mahaska County purposes)</u>

If a fax transmission containing PHI is not received by the intended recipient because of a misdial, check the internal logging system of the fax machine to obtain the misdialed number.

If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax, requesting that the entire content of the misdirected fax be destroyed.

Note the unauthorized disclosure on the accounting of unauthorized disclosures (see Policy and Procedure PR-140 "Accounting of Disclosures"). This must include the date, the erroneous recipient, the information disclosed and the steps taken to correct the unauthorized disclosure. This record should be sent to the Chief Privacy Officer.

Receipt of Faxes Containing PHI

Fax machines used for patient care or client-related services shall not be located in areas accessible to the general public but rather must be in secure areas, and the department director or designee is responsible for limiting access to them.

Each department is responsible for ensuring that incoming faxes are properly handled. When receiving faxed PHI, immediately remove the fax transmission from the fax machine and deliver it to the recipient. Manage PHI received via fax as confidential in accordance with policy. Destroy, or follow sender's instructions for, patient information faxed in error and immediately inform the sender.

Applicable Standards and Regulations:

45 C.F.R.§164.530(c)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-165: Removal of/Transporting PHI

Purpose:

Mahaska County has a legal and ethical responsibility to maintain the confidentiality, privacy and security of all protected health information (PHI), electronic protected health information (ePHI) and personal information that they create or receive. The purpose of this policy is to ensure appropriate safeguards against the loss, theft and unauthorized access, use, disclosure, alteration or destruction of PHI/ePHI and personal information in paper form or stored in electronic form on any media by providing basic requirements for the physical removal or transport of such information from or within Mahaska County.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All Elected Officials and Department Heads are responsible for enforcing this policy. Individuals who violate this policy will be subject to disciplinary actions.

Policy:

The intention of this policy is to prevent the unauthorized disclosure of PHI/ePHI as a result of transporting PHI/ePHI from one location to another. Original records and case management records must be logged in the Department to track unauthorized disclosures. PHI that is not required to be in the original record, such as loose photocopies and extra printouts used for client care purposes, do not have to be logged; however, all other aspects of this policy will apply to loose photocopies and extra printouts of PHI.

Procedures:

1. Each Department responsible for the confidentiality, integrity and availability of client or employee medical records, such as in Public Health, Secondary Roads or other departments requiring the creation or use of medical records, may not be removed from Mahaska County premises unless there has been prior approval from the Mahaska County Department manager and/or Board of Supervisors.

2. Whenever PHI (original medical records) must be removed from Mahaska County premises, a record must be made that includes:
    a. Date;
    b. Purpose of removal;
    c. Description of the information involved; and
    d. Person(s) possessing the information.

3. Whenever ePHI is being removed from the Mahaska County premises, the ePHI will be encrypted with an appropriate encryption/decryption key that is consistent with Mahaska

County Standard Operating Procedures. The decryption key will be transmitted to the receiver of the data using communications other than with the transported media containing the ePHI.

4. Whenever a hardcopy version of PHI/ePHI (actual medical records, photocopies and extra printouts) is removed from Mahaska County premises, it must be secured and protected at all times. Best practice, PHI/ePHI is carried in a locked backpack or briefcase.

5. While transporting PHI/ePHI in a Mahaska County motor vehicle, or personal motor vehicle, the information must be placed in a secure locked container, where medical records are not physically visible. These containers should be fire proof if possible.

6. If the PHI/ePHI is for use in providing client care in a client's home, only the PHI/ePHI of the person you are treating at the time should be removed from the secured location for use. Any other individual's PHI/ePHI should remain securely stored and protected.

7. While using PHI/ePHI remotely (only as approved by the Chief Privacy Officer), workforce members, Elected Officials and volunteers should store PHI/ePHI in a secure manner when not in use. For example, best practice is to have PHI/ePHI locked in a file drawer or briefcase, when not in use. When viewing the information, you must do so in a manner so that other household members cannot inadvertently view the PHI/ePHI.

8. All PHI/ePHI must be returned to Mahaska County once there is no longer a need for it to be transported. However, if PHI was printed or copied for the sole purpose of "home use", the PHI/ePHI must be disposed of in accordance with Policy/Procedure PS-105 "Disposal of ePHI and/or Hardware" and Policy/Procedure PR-115 "Use of PHI" when access off premises is no longer needed.

Applicable Standards and Regulations:

45 C.F.R.§164.530(c)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-170: Reporting of Privacy Concern and Security Breach Policy

Purpose:

The purpose of this Breach Notification Policy is to provide guidance to the workforce members, Elected Officials and volunteers of Mahaska County when there is a breach, an acquisition, access, use, or disclosure of Mahaska County's citizens' unsecured protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing rules and regulations, which compromises the security or privacy of the Protected Health Information (PHI). HIPAA requires that Mahaska County notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances, Mahaska County must also report such breaches to the Secretary of the Department of Health and Human Services (HHS) and through the media. Mahaska County breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act (ARRA) of 2009 and its implementing rules and regulations, each as may be amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013), collectively "HIPAA."

Responsible for Implementation:

Chief Privacy Officer and Chief Security Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska CountyMahaska County.

Policy:

Any individual who believes the rights granted by the HIPAA or HITECH privacy or security regulations or any other state or federal laws dealing with privacy and confidentiality have been violated may file the "Privacy Concern or Security Breach Compliance Investigation Form" from Policy/Proceudre AS-175 regarding the alleged privacy or security violation.

Any individual who identifies a breach of Mahaska County's security policy or procedures needs to notify the Chief Security Officer (CSO) as soon as possible after identification of the security breach. To the extent that the Chief Privacy Officer (CPO) and/or Board of Supervisors are positions filled by different individuals, each should also be advised. The CSO shall be responsible to contact the US Department of Health and Human Service (HHS) Office of Civil Rights (OCR) once a breach has been confirmed and the individuals outlined above shall collaborate to implement Mahaska County's response. The County Attorney and HIPAA advisor shall also be contacted for guidance if instances where a breach is believed to have occurred.

Procedures:

1. Filing HIPAA Complaints

Any privacy or security related complaint made by a citizen, employee, or other individual, must be forwarded to Mahaska CountyMahaska County's CPO/CSO. The form "Privacy Concern or Security Breach Compliance Investigation Form" (Policy/Procedure AS-175) for alleged violations of rights relating to PHI must be completed and submitted to the county's CPO/CSO. Anonymous complaints can be made by phone or mail for Mahaska CountyMahaska County's CPO/CSO.

2. Investigation of Complaints

The CPO/CSO will investigate the alleged privacy or security breach violations. The CPO/CSO may request an investigation of information systems, to determine if a breach of systems security was responsible for the breach.

If during the course of investigation an individual is found to be in violation of Mahaska CountyMahaska County's PHI/ePHI privacy or security policies governing PHI/ePHI, he /she will be subject to the county's disciplinary actions.

Applicable Standards and Regulations:

45 CFR § 164.308(a)(6)(ii)
45 CFR § 164.530(d)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-180: What Constitutes a Breach of PHI

Purpose:

HIPAA covered entities and business associates must notify individuals about incidents involving a breach of protected health information (PHI). Covered entities and business associates must also notify the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) about breach incidents. In some situations they must notify the media as well.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

The HIPAA Breach Notification Rule (45 CFR §164.400-414) requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Procedures:

1. What is a breach?

   Under HIPAA, a breach is defined as "the unauthorized acquisition, access, use or disclosure of protected health information (PHI) which compromises the security or privacy of such information." There are three exceptions to this definition:
   - when a member of the covered entity's workforce, acquires, accesses or uses PHI in good faith without further using or disclosing the information in a way that the HIPAA Privacy Rule does not permit;
   - when a person authorized to access PHI inadvertently discloses PHI to another person who is authorized to access PHI; or
   - when there is a good faith belief that the unauthorized person to whom the PHI has been disclosed would not be able to retain the information.

2. When must a covered entity or business associate notify others of a breach?

   Covered entities and business associates do not have to provide notification in the case of every data breach. The protected health information (PHI) breached must have been unsecured (unencrypted data, for example). In addition, the covered entity or business associate may not

have to notify individuals if it determines there is a low chance that PHI was accessed, acquired, used, or disclosed as a result of the breach.
From 2009 until 2013, under HHS's Interim Final Rule, a covered entity did not need to report a breach unless, upon investigation, it determined that disclosure would pose a "significant risk of financial, reputational, or other harm to the individual." This was controversial because it allowed covered entities to use subjective judgment to determine whether to report a breach. This standard has been supplanted by the 2013 Omnibus Rule which replaced the "risk of harm" standard with a standard based on the chance PHI was compromised.

3. How does a covered entity or business associate decide when PHI is compromised?
   Covered entities must conduct a risk analysis to determine whether PHI has been compromised. The analysis must take into account:
   - the nature and extent of the PHI such as the types of identifiers (e.g. name, address, Social Security number);
   - the person who gained unauthorized access to PHI;
   - whether the PHI was actually acquired or viewed; and
   - the extent to which the risk has been mitigated

   If, after conducting the risk analysis, a covered entity determines there is a low risk that PHI was compromised, it does not have to provide notice. The HIPAA Omnibus Rule offers the following example of a low risk disclosure: A covered entity misdirects a fax to the wrong physician, and, upon receipt, the receiving physician says he has destroyed the fax.

4. How do individuals know if their PHI is breached?
   Individuals should be notified by first-class mail or email (if they choose to receive email notices) no later than 60 days after the breach is discovered or should have been discovered. However, notice may be delayed if law enforcement requires it, for example, to conduct an investigation of the breach.
   The covered entity may post a notice on its website if it has insufficient contact information for 10 or more individuals. If there are fewer than 10, it may try to telephone or provide other notice.

5. What information will be in a breach notice?
   The notice should include at least the following information:
   - a brief description of what happened as well as the date of the breach and the date it was discovered;
   - the types of information that were involved;
   - a description of what actions the covered entity took after the breach was discovered; and
   - contact information that allows individuals to ask questions and learn more about the breach, the follow-up, and what steps they should take to protect themselves. Contact information should be either a toll-free number, an email address, a website, or a postal address.

6. When must a covered entity notify HHS or the media about a breach?
   When there is a breach that affects more than 500 residents of a state, the covered entity must notify relevant media outlets.

Covered entities must notify HHS as well. They must notify HHS of breaches involving fewer than 500 people within a year after the breach is discovered. When a breach involves more than 500 people, HHS/OCR requires notice immediately and posts those breach incidents on its website.

7. Does the HHS website list data breaches caused by a covered entity's employees or other insiders?

   Not specifically. Incidents caused by insiders may be simply reported under the category of "unauthorized access." However, the HHS website only reports incidents involving more than 500 individuals. Unauthorized access by "insiders" often involves individuals snooping on neighbors, ex-spouses, celebrities, or other employees.

8. What role does the Federal Trade Commission (FTC) play in safeguarding health information?

   The FTC can issue rules regarding breaches of data stored by web-based consumer personal health records (PHR) vendors. However, FTC rules only apply to PHR companies that are not subject to HIPAA.

   According to the FTC's final data breach rule for web-based PHR vendors, the rule also applies to related entities that:

   - offer products or services through the website of the PHR vendor;
   - offer products or services through the websites of HIPAA-covered entities that offer individuals PHRs;
   - access information in a personal health record; or
   - send information to a personal health record.

   According to the FTC, an example of a PHR entity is an online weight-tracking program that sends information to a personal health record or pulls information from it. Another example would be a HIPAA-covered entity such as a hospital that offers its employees a PHR.

   Like covered entities that report breaches to HHS, web-based health data vendors must report a breach to the FTC. Unlike covered entities, even incidents involving a single individual are posted on the agency's website.

Applicable Standards and Regulations:

45 CFR § 164.404
45 CFR §164.400-414

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version
Implementation Date:

Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-182: Incidental Use and Disclosure of Protected Health Information

Purpose:

The HIPAA Privacy Rules permit certain incidental uses and disclosures of Protected Health Information (PHI). Accordingly, it is the policy of Mahaska County to comply with the limitations set forth in the Rules.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI and/or electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

The provisions regarding incidental use and disclosure were adopted to ease the day-to-day functioning of persons who deal with PHI on a regular basis, but do not provide license to disregard privacy obligations. The rules that must be followed are grounded in common sense.

Procedures:

1. Incidental disclosures are disclosures of PHI that:
   (a) occur as a by-product of a permissible use or disclosure;
   (b) are limited in nature; and
   (c) cannot be prevented through the use of reasonable measures.
2. Incidental disclosures do not violate the Privacy Policies as long as:
   (a) reasonable safeguards were taken to prevent the incidental disclosure; and
   (b) the disclosure resulted from a use or disclosure that is otherwise permissible under Mahaska County's privacy policies, including the Policy/Procedure AS-110 "Minimum Necessary Use and Disclosure of PHI/ePHI."
3. Workforce members must take all reasonable measures to avoid use or disclosure of PHI to persons who have no responsibilities or duties that require access to PHI. For example:
   (a) designated personnel with treatment responsibilities will reasonably safeguard PHI to limit the incidental uses and disclosures made to that which is necessary to carry out their treatment responsibilities. Such limitations may include:
      i) to the extent possible, limit discussions about individuals with other health care providers to areas that are reasonably secure and not open to the public;
      ii) avoid discussions about PHI in the elevator, break rooms and other public places;
      iii) to the extent possible, avoid using PHI on boards in triage areas or other areas to communicate individual status to case managers and health care professionals. Where such boards must be used, use the individual's initials rather than the individual's name. Limit other information to the minimum necessary;
      iv) for health department or case management sign-in logs, limit incidental disclosure of individual's name by blocking it out after the individual has been called. If the log is

retained, remove the sheets periodically and store in area not open to the public. Do not request diagnosis or treatment information on the sign in log;

v) speak quietly when discussing PHI in connection with your job responsibilities;
vi) protect the individual's chart with a cover;
vii) keep doors closed during appointments and treatment;
viii) mail test results to individual in a sealed envelope rather than on a post card.

(b) Designated personnel with billing, collections, or health care operations responsibilities will reasonably safeguard PHI to limit the incidental uses and disclosures made to that which is necessary to carry out their responsibilities. Such limitations may include:

i) speak quietly when discussing PHI in connection with your job responsibilities;
ii) to the extent possible, avoid using individuals' names, health benefit claims histories, treatment histories, and diagnoses when discussing PHI within the work place;
iii) avoid leaving work papers containing PHI on desks or other surfaces in plain view of others;
iv) keep papers and other materials in file cabinets or drawers when not in immediate use.

4. All contractors who are not Business Associates:
   (a) Shall receive training on incidential disclosures, what they are, and if one occurs, how it should be reported to their immediate supervisor, and the individual within the organization's workforce responsible for the contractor,
   (b) Each contractor shall acknowledge the reciept of such training, and
   (c) Each contracor shall sign a non-disclosure agreement regarding information from an incidential disclosure.
5. The following measures are considered reasonable with respect to the prevention of incidental disclosures and shall be followed when applicable:
   (a) Compliance with the Policy/Procedure AS-110 "Minimum Necessary Use and Disclosure"
   (b) Compliance with the Policy/Procedure AS-100 "Security and Privacy Program Specifications" regarding Administrative, Physical and Technical Safeguards.
6. In the event an incidental disclosure occurs, the incident should be reported to the Chief Privacy Officer, who will investigate the incident, decide on remedial actions and provide appropriate training. All these steps will be documented.

Applicable Standards and Regulations:

45 CFR §164.502 (a)
45 CFR §164.502 (b)
45 CFR §164.514 (d)
45 CFR §164.530 (c)(2)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-195: Tracking Privacy and Security Breach Disclosures

Purpose:

To provide guidance for breach notification by covered entities when unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), Modifications to the Health Information Portability and Accountability Act (HIPAA) Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (2013 Omnibus Rule), as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

Responsible for Implementation:

Chief Privacy Officer and Chief Security Officer

Scope:

This policy covers all protected health information(PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall track all breach incidents to their conclusion; and it shall be responsibility of the county's Chief Privacy and Security Officer (CPO/CSO) to track and manage the breach incident information. Further, it shall be the responsibility of all county workforce members, Elected Officials, volunteers, contractors and business associates to notify Mahaska County's CPO/CSO of incidents with all applicable information to ensure effective and timely tracking of the incidents.

Procedures:

The CPO/CSO will utilize a disciplined procedure for tracking HIPAA and HITECH breach incidents. To start, the CPO/CSO will use the spreadsheet AS-185a "Tracking Breach Incident Log" (and/or enter data into HIPAA Suite) to track the identification, assessment and notification of parties involved in a breach incident. The spreadsheet tracks the incidents for the information and actions required by the HITECH law and related HHS rules.

It is expected that Mahaska County's CPO has primary responsibility for entering data, making risk assessments, overseeing the notification process and monitoring the mitigation efforts that caused

the breach in coordination with the CSO. Below are instructions for identification and tracking, assessment, and notification included in the spreadsheet:

1. Privacy/Security Incident Tracking

The Tracking Breach Incident Log contains the information regarding the incident. The incident is first recorded on this worksheet by documenting the key issues related to the incident. This includes the incident number (e.g., 201x-1, 201x-2, etc.), description, the name of the person who disclosed the data, the relationship of the disclosing person to Mahaska County, whether the disclosure was oral, paper or electronic, the number of patient records disclosed, the number of individuals affected, the incident date, the incident discovery date, the name of the person who received the disclosed data, and how the PHI/ePHI data was breached.

The tracking process begins when anyone associated with Mahaska County (e.g., an employee, intern, business associate, or customer), notifies the county's CSO/CPO that a potential breach is believed to have occurred. Each of Mahaska County's workforce members. Elected Officials and volunteers will be trained to recognize a disclosure incident and to capture the information need to document and assess if a breach has occurred. All such information will be communicated to the county's CPO, who will collect and document the data using Mahaska County's Tracking Breach Incident Log.

2. Privacy/Security Incident Assessment

From the information logged in the Tracking Breach Incident Log, the next step is for Mahaska County's CPO to conduct an assessment to see if a breach has occurred. The Tracking Breach Incident Log leads the CPO through the steps necessary to determine if a breach did actually occur. The goal is to identify and understand the factors that are used to determine if a breach has occurred and, if it did, the nature of the breach.

Questions included are necessary to determine the scope and intent of the disclosure. This includes assessing whether the disclosure was intentional or inadvertent and if the disclosure was malicious or accidental.

The next step is to determine whether the data was de-identified and if sensitive data was disclosed or not.

The next set of information relates to determining whether the recipient actually saw the disclosed data and what the recipient did with the data. In this section Mahaska County's CPO also notes whether the situation that led to or caused the disclosure has been remedied.

The next set of data relates to whether the disclosure involved hardcopy or electronic data. If the disclosure involved hardcopy, then the disposition of the hardcopy data is recorded. If the disclosure involved electronic data, then the nature of the security of the electronic data is recorded (e.g., was the data encrypted; if so was the encryption key provided to the recipient separately; and was the data destroyed?)

The last data entered is the CPO's conclusion whether a breach has occurred or not. The conclusion also assesses the risk that the disclosure resulted in significant financial, reputational or other harm to the individual or the Covered Entity (CE)/Business Associate (BA).

3. Security Incident Notification

The HITECH law and subsequent rules generated by the Secretary of the U.S. Department of Health and Human Services (HHS) dictate the notification process to be followed by the CSO if a breach has occurred. The CSO retains responsibility for ensuring that information regarding a breach is recorded in the Tracking Breach Incident Log (e.g., the information that was breached, the persons affected, etc.) and that the HHS Office of Civil Rights (OCR) is notified.

Note: The CSO, in coordination with the CPO, Board of Supervisors, County Attorney and a HIPAA advisor, must: 1) notify the HHS Office of Civil Rights of all breaches within 60 days of the end of the calendar year if the total number of persons who's PHI/ePHI is breached is less than 500; or 2) notify the Office of Civil Rights within 60 days of the point at which Mahaska County should have known of a breach of ePHI/PHI belonging to 500 or more persons.

In either case, the persons who's PHI/ePHI has been disclosed must be notified by the CSO within 60 days of the point at which Mahaska County should have known of the breach.

4. Incident Notification Worksheet

Based on the number of patients affected and a determination that a breach did occur, definitive responsibilities are required for notifying various parties. Any breaches requiring notification of the HHS Office of Civil Rights and names of individuals who information is breached must be logged by the CSO using the Incident Notification Worksheet.

If a breach occurs, the first issue is to identify and document how many of the affected patients have outdated contact information. This determines how they are to be notified.

The next issue to define is how many patients reside in particular states. This also determines how Mahaska County responds to the notification requirements. Completing this worksheet for each incident allows the county to meet its minimum notification criteria and responsibility to log each incident, in support of its annual report to HHS Office of Civil Rights for incidents involving PHI/ePHI belonging to fewer than 500 individuals and any reports required within 60 days of the point where Mahaska County should have detected the breach when any such breach involves PHI/ePHI belonging to 500 or more individuals.

5. Enforcement

All supervisors are responsible for monitoring the disclosure of PHI data and adherence to county data security procedures by their assigned personnel. The CSO/CPO is/are responsible for conducting the incident assessment and documenting the incident, assessing the breach and ensuring the notification process is completed, except that the CSO/CPO shall maintain primary responsibility for areas specifically assigned as outlined in this Tracking Privacy and Security Breach Disclosures policy and Policy and Procedure AS-170 "Reporting of Privacy Concern and Security Breach Policy."

Failure by individuals to comply with county policy and procedure regarding the logging, assessment, and notification requirements specified is subject to discipline including termination of employment or internship. Additionally, the county may be subject to significant penalties imposed by the HHS Office of Civil Rights.

Applicable Standards and Regulations:

45 CFR §164.308(a)(1)(ii)(d)
45 CFR §164.400

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-190: Mitigation After Improper Use and Disclosure of PHI

Purpose:

Mahaska County has a duty to ensure the proper use and/or disclosure of protected health information (PHI). This policy shall provide guidance to Mahaska County facilities and employees to the extent practicable, to mitigate (lessen or alleviate) any harmful effect that becomes known to them as a result of an improper use or disclosure of PHI.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All Elected Officials and Department Heads are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

Policy:

To the extent practicable, Mahaska County will mitigate (i.e., lessen or alleviate) any harmful effect that becomes known to Mahaska County as a result of a use or disclosure of PHI in violation of Mahaska County's policies and procedures or applicable law.

Procedures:

Mitigation may include, but is not limited to, the following:

1. Taking operational and procedural corrective measures to remedy violations;
2. Taking employment actions to re-train, reprimand, or discipline employees as necessary up to and including termination;
3. Make all reasonable efforts to recover or destroy any hardcopy or electronic PHI that has been disclosed to an unauthorized user to minimize the risk of harm to the individual whose PHI was subject to the breach;
4. Take all reasonable steps necessary to notify those individuals affected by any breach consistent with Mahaska County's policies and Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act laws and subject regulations to mitigate any harm to the individuals;
5. Addressing problems with business associates once Mahaska County is aware of a breach of privacy;
6. Incorporating mitigation solution into Mahaska County's policies/procedures as appropriate;
7. Addressing and investigating employee violations.

Violation of this policy may result in disciplinary action up to and including termination for employees, a termination of employment relationship in the case of contractors or consultants, or suspension or expulsion in the case of a student. Additionally, individuals may be subject to loss of access privileges and civil and/or criminal prosecution.

Applicable Standards and Regulations:

45 C.F.R. §164.530(f)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-195: HIPAA Fraud and Abuse

Purpose:

The purpose of this policy is to prevent and detect fraud, waste and abuse by providing detailed information regarding (1) the federal False Claims Act (FCA), (2) state laws and penalties pertaining to false claims, and (3) whistleblower protections under such laws.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy applies to all Mahaska County workforce members, Elected Officials and volunteers.

Policy:

Mahaska County is dedicated to the prevention and detection of fraud, waste and abuse. This policy details in written form the laws described in this policy and procedures for detecting and preventing fraud, waste and abuse. This fraud and abuse policy is to give summary guidance regarding federal and state laws involving false claims and whistleblower protections under such laws.

Procedures:

False Claim: Is a claim for payment for services or supplies that were not provided specifically as presented or for which the provider is otherwise not entitled to payment, including but not limited to the following:

- A claim for a service or supply that was never provided.
- A claim indicating the service was provided for some diagnosis code other than the true diagnosis code in order to obtain reimbursement for the service (which would not be covered if the true diagnosis code were submitted).
- A claim indicating a higher level of service than was actually provided.
- A claim that the provider knew or should have known was not reasonable and necessary.
- A claim for services provided by an unlicensed individual.

False Claims Act (FCA): Is a federal law (31 U.S.C. § 3729-3733) used to bring a case against a health care provider for the submission of a false claim involving any federally funded contract or program (with the exception of tax fraud) and includes the following:

- knowingly presenting (or causing to be presented) to the Federal Government a false or fraudulent claim for payment or approval.
- knowingly making or using (or causing to be made or used) a false record or statement to conceal, avoid or decrease an obligation to get a false or fraudulent claim paid or approved by the Federal Government or State program.
- conspiring with others to get a false or fraudulent claim paid or approved by the Federal Government or State program.

Forgery: The state law that prohibits falsely making, completing or altering a document with intent to defraud and would include making false statements on eligibility forms to obtain health care services.
Fraud and Abuse: Is an umbrella term that applies to a series of statutes and regulations designed to prevent government health programs from paying excessive and inappropriate claims.
Fraudulent schemes and artifices: The law that prohibits a scheme to obtain a benefit by means of false or fraudulent pretenses, representations, promises or material omissions.

Fraudulent schemes and practices; willful concealment: the law that prohibits any person from knowingly falsifying, concealing or covering up a material fact by trick, scheme or device when related to the business conducted by a state department or agency.
Prohibited acts and duty to report: The law that prohibits any person to present or cause to be presented:

- A claim for medical items or services that were not provided as claimed.
- A claim for medical items or services that is false or fraudulent.
- A claim for medical items or services that are substantially in excess of the needs of the individual or of a quality that fails to meet professional standards.
- A claim submitted for a physician's service or item or service incidental to a physician's service, when the service was not rendered or supervised by a licensed physician.

Theft: Is a state law that among many things prohibits obtaining services or property by means of any material misrepresentation, which would include, for instance, obtaining healthcare services when not eligible to do so.
Whistleblower: Is an individual who reports misconduct to state or federal agencies involved with enforcing laws prohibiting fraud and abuse such the OIG.

PROCEDURES TO PREVENT, DETECT AND EDUCATE
Mahaska County, through its Ethics and Compliance Program, requires that Mahaska County business will be conducted in an ethical manner and will comply with the above described federal and state laws involving false claims.
Mahaska County activities to prevent fraud, waste and abuse include the following:

- A decentralized Ethics and Compliance Program designed to build ethics and compliance accountability into the core operations of each Mahaska County Department.
- A Code of Conduct emphasizing the necessity for and the responsibility of all workforce members, Elected Officials, volunteers and Agents to perform their duties in compliance with laws, regulations and Mahaska County policies.
- Mandatory ethics and compliance training and education programs.
- Screening processes ensuring that Mahaska County does not employ or contract with individuals or entities that have been sanctioned
- Workforce members' performance evaluations that include a component assessing compliance with their obligations as defined by the Ethics and Compliance Program.
- Education that the consequences for violating the above described laws can include, in addition to imprisonment and fines, civil monetary penalties, loss of licensure, and exclusion from participation in federal health care programs.

Mahaska County activities to detect fraud, waste and abuse include the following:

- Reporting resources such as a phone number available for reporting,
- Monitoring and auditing systems.
- Prompt investigation and corrective action for all instances of suspected non-compliance with the Mahaska County Ethics and Compliance Program.

Mahaska County is dedicated to disseminating information and educating individuals regarding the above laws through the following processes:

- The Mahaska County Ethics and Compliance Program including a copy of this Fraud and Abuse Policy will be distributed to workforce members, Elected Officials, volunteers and Contractors,

- Subcontractors, Agents, or other persons which or who, on behalf of the Mahaska County, furnish, or otherwise authorize the furnishing of, perform billing or coding functions, or is involved in the monitoring of health care provided by the entity.
- Annual mandatory Mahaska County Ethics and Compliance Program education will be held for all workforce members, Elected Officials, volunteers, contractors, and Agents.
- The Mahaska County Ethics and Compliance Program and Policies are posted on the Mahaska County Intranet and accessible to all employees.

PROCEDURES FOR REPORTING

Mahaska County provides mechanisms as described above to report potential acts of fraud, abuse and waste through the Ethics and Compliance Program:

- U.S. Mail: Mahaska County, 106 S 1st St, Oskaloosa, IA, 52577
  Attn: Ethics and Compliance Program or Chief Security Officer
- Email:
  County Attorney, James Blomgren
  blomgren@mahaskacounty.org
  Chief Security Officer, Darin Hite
  dhite@mahaskacounty.org

Individuals seeking advice from the Ethics and Compliance Department have the option to remain anonymous and all inquiries are confidential subject to the limitations imposed by law.
Individuals may choose to report potential acts of fraud, abuse and waste to the Legal Department.
Civil liability for violating the False Claims Act is equal to three times the dollar amount that the Government is defrauded and civil penalties of $5,000 to $10,000 for each false claim.
An individual can share in a percentage of a government recovery in an FCA action or settlement if they bring an action on behalf of the United States as a "qui tam relator."

ANTI-RETALIATION PROVISIONS

Mahaska County strictly prohibits any type of retaliation against those who, in good faith, report any inappropriate activities described in this policy.
The False Claims Act protects qui tam relators against discharge, demotion, harassment or other discrimination by their employers as a result of the claims they made under the False Claims Act.
State and Federal laws also have protections for whistleblowers.

Applicable Standards and Regulations:

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-200: Restricting Use of PHI and Confidential Communications

Purpose:

This policy establishes guidelines for handling: (1) requests for a restriction on the use or disclosure of protected health information (PHI); and (2) requests to receive communications of PHI by alternative means.

Responsible for Implementation:

Chief Privacy Officer

Scope:

All workforce members, Elected Officials and volunteers are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

Policy:

Mahaska County recognizes an individual's right to request privacy protection for PHI, including a restriction of the uses or disclosures and/or a request to receive communications of PHI by an alternative means or at alternative locations. As described by and subject to the restrictions in this Policy, Mahaska County will permit and consider requests by individuals or their representatives for the restriction of the uses and disclosures of their PHI to carry out treatment, payment, and operations, or to an individual involved in the individual's care, such as a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual. Mahaska County will also accommodate reasonable requests by individuals to receive communications of PHI at an alternative address or by an alternative means as described below.

Procedures:

Mahaska County allows an individual to request that Mahaska County restrict:

1. Uses and disclosures of PHI about the individual to carry out treatment, payment and operations; and
2. Permitted uses and disclosures as outlined in relevant Mahaska County HIPAA policies.

Mahaska County may require the individual to make a request for restricting use of PHI in writing with Policy/Procedure AS-200a "Restriction Request for Use and Disclosure of PHI Form." Mahaska County is not required to agree to a restriction. If Mahaska County does agree to a restriction, Mahaska County may not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide emergency treatment. Mahaska County may use the restricted PHI itself or Mahaska County may disclose such restricted PHI to a health care provider to provide such treatment to the individual. If restricted PHI is disclosed to another health care provider for emergency treatment, as outlined above, Mahaska County must request that the health care provider not further use or disclose the PHI. A restriction agreed to by Mahaska County is not effective to prevent uses or disclosures from being made to the individual for:

1. Inspection and copying their own PHI;
2. The individual from obtaining an accounting of disclosures of PHI; or
3. For uses and disclosure for which consent, authorization or opportunity to agree or object is not required.

Terminating a Restriction:

Mahaska County may terminate its agreement to a restriction if:

1. The individual agrees to or requests the termination in writing,
2. The individual orally agrees to the termination and the oral agreement is documented, or
3. Mahaska County informs the individual that it is terminating the restriction. Any PHI created and received after the termination will not be restricted. However, any PHI created or received before the termination will be restricted.

Confidential Communications:

A request for restricting confidential communications can occur anytime and requires a change in the individual's designated address. Mahaska County must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from Mahaska County at alternative locations. It is up to the individual to change the address back to the original designated address. Mahaska County may require the individual to make a request for confidential communication in writing with Policy/Procedure PR-145b "Consent for Health Information to be Communicated by Alternative Means." Mahaska County may condition the provision of a reasonable accommodation on:

1. When appropriate, information as to how payment, if any, will be handled; and
2. Specifications of an alternative address or other method of contact.

Mahaska County may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

Process Documentation:

Mahaska County's CPO will:

1. Maintain an ongoing log of requests using the Policy/Procedure AS-200b "Log of Requests for Restricting Use and Disclosure of PHI."
2. Maintain an ongoing log of requests for confidential communications by alternative means using Policy/Procedure PR-145a "Request for Alternative Communications of PHI Log;"
3. Maintain documentation of all Restriction Request forms, Communication by Alternative Means forms, Log of Requests for Restricting Use and Disclosure of PHI and Request for Alternative Communications of PHI Log efforts for a minimum of six years.

Applicable Standards and Regulations:

45 C.F.R. §164.308(a)(3)(ii)(A)
45 C.F.R. §164.522

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

James Blomgren		

AS-210: Risk Analysis

Purpose:

This policy establishes the scope, objectives, and procedures of Mahaska County's information security risk management process. The risk management process is intended to support and protect the county and its ability to fulfill its mission.

Responsible for Implementation:

Chief Security Officer

Scope:

The scope of the information security risk management process covers the administrative, physical, and technical processes that enable and govern protected health information (PHI) and electronic protected health information (ePHI) that is received, created, maintained or transmitted.

Policy:

Mahaska County's Chief Security Officer (CSO) shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI/ePHI that Mahaska County holds.

ADDITIONAL

1. It is the policy of Mahaska County to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its ePHI, and other confidential and proprietary electronic information, and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's information security program.
2. Risk analysis and risk management are recognized as important components of Mahaska County's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8).
    A. Risk assessments are done throughout IT system life cycles:
        i. Before the purchase or integration of new technologies and changes are made to physical safeguards;
        ii. While integrating technology and making physical security changes; and
        iii. While sustaining and monitoring of appropriate security controls.
    B. Mahaska County performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.

3. Mahaska County implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all ePHI the organization creates, receives, maintains, and/or transmits;
   B. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
   C. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required; and
   D. Ensure compliance by workforce.
4. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the senior management, the organization's Risk Management Team, and business managers.
5. All Mahaska County workforce members, Elected Officials and volunteers are expected to fully cooperate with all persons charged with doing risk management work. Any workforce members, Elected Officials and volunteers that violates this policy will be subject to disciplinary action based on the severity of the violation according to Mahaska County's Policy/Procedure AS-130 "Disciplinary Actions for Breach of Confidentiality, Privacy or Security -Sanctions and Penalties."
6. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

Procedures:

A comprehensive analysis of security threats is conducted at least once every year, reviewed annually and updated as needed. The risk analysis comprehensively describes the provider's information system, including the following components:

ADDITIONAL

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Mahaska County's Information Security Officer (or other designated employee), and the identified Risk Management Team.
2. Risk Assessment: The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

   Step 1. System Characterization

   i. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). (See "Risk Analysis and Risk Management Toolkit – Network Diagram Example and Inventory Asset List" to assist with these efforts)

   ii. Output – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.

   Step 2. Threat Identification

   i. In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-

sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment. (See "Risk Analysis and Risk Management Toolkit –Threat Overview" for definitions and the "Threat Source List" in the Risk Assessment for examples of threat sources)

ii. Output – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

Step 3. Vulnerability Identification

i. The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. (See "Risk Analysis and Risk Management Toolkit – Risk Assessment Template – Security Questions and Threat Source List")

ii. Output – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

Step 4. Control Analysis

i. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability.

ii. Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

Step 5. Likelihood Determination

i. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls. (See "Risk Analysis and Risk Management Toolkit – Risk Likelihood, Risk Impact, and Risk Level Definitions")

ii. Output – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 6. Impact Analysis

i. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. (See "Risk Analysis and Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

ii. Output – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 7. Risk Determination

i. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree

or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level. (See "Risk Analysis and Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

ii. Output – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Step 8. Control Recommendations

i. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. (See "Risk Analysis and Risk Management Toolkit – NIST - Risk Mitigation Activities".)

ii. Output – Recommendation of control(s) and alternative solutions to mitigate risk.

Step 9. Results Documentation

i. Results of the risk assessment are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes. (See "Risk Analysis and Risk Management Toolkit –Risk Analysis Report Template")

ii. Output – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

3. Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

Step 1. Prioritize Actions

i. Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources

ii. Output – Actions ranked from high to low

Step 2. Evaluate Recommended Control Options

i. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.

ii. Output – list of feasible control

Step 3. Conduct Cost-Benefit Analysis

i. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of

controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

ii. Output – Documented cost- benefit analysis of either implementing or not implementing each specific control

Step 4. Select Control(s)

i. Taking into account the information and results from previous steps, the Mahaska County's mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

ii. Output – Selected control(s)

Step 5. Assign Responsibility

i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

ii. Output – List of resources, responsible persons and their assignments

Step 6. Develop Safeguard Implementation Plan

i. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
    a. Each risk or vulnerability/threat pair and risk level
    b. Prioritized actions
    c. The recommended feasible control(s) for each identified risk
    d. Required resources for implementation of selected controls
    e. Team member responsible for implementation of each control
    f. Start date for implementation
    g. Target date for completion of implementation
    h. Maintenance requirements

ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

iii. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.

iv. Output – Safeguard Implementation Plan

Step 7. Implement Selected Controls – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not

practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.

i. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.
ii. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
iii. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
iv. Output – Residual Risk

4. Risk Management Schedule: The two principal components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Mahaska County's information security program:
   A. Scheduled Basis – an overall risk assessment of Mahaska County's information system infrastructure will be conducted annually. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the county budgeting process.
   B. Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
   C. As Needed – the Security Officer (or other designated employee) or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Mahaska County's information systems.
5. Process Documentation: Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.

Applicable Standards and Regulations:

45 CFR §164.308(a)(1)(ii)(A)
45 CFR §164.308(a)(1)(ii)(B)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-215: Protection from Malicious Software

Purpose:

This policy reflects Mahaska County's commitment to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (ePHI) for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall utilize a combination of cost effective resources available to ensure that malicious software can neither be installed nor made operational on any county servers, work stations or mobile devices. Additionally, it shall be Mahaska County's policy that downloading information or software without specific permission is prohibited and will be subject to the county's disciplinary policy.

Procedures:

Mahaska County has implemented the following procedures:

1. Servers, workstations and network devices are protected by a combination of antivirus software, individual firewalls, prohibited network mapping and wireless stealth technology, inside the firewall.

2. Portable devices such as laptops, tablets and smart phones which might contain ePHI or propriety county data are equipped with software that permits remote location of each device and retrieval or destruction of sensitive data in each device should such devices be lost or compromised.

3. Antivirus software is internet-based, updated automatically on a nightly basis, monitors both inbound and outbound internet traffic, and automatically isolating or removing viruses and malware, including spyware.

4. Authorized disks and other removable media, including those containing newly released software, shall be scanned for viruses and other malware by Mahaska County's Chief Security Officer (CSO) before the media may be used.

5. If a virus or other malware is detected through protection software or other indicators, the workstation or server shall be taken off-line from the network and taken to the CSO for review and corrective action by the CSO or an IT Specialist that has been designated by the CSO/IT Director.

6. Only county owned servers, work stations, laptops, tablets, cellphones and storage media may be used when dealing with ePHI to protect ePHI from unauthorized access, modification, dissemination or deletion. Such device shall be clearly marked as approved for handling ePHI.

7. Devices that have been repaired shall be checked using the county's antivirus/anti-malware software before such units will be authorized for return to service.

8. Mahaska County workforce members, Elected Officials and volunteers will receive initial and recurrent training in the recognition and safe handling of malicious email and attachments, safe use of portable storage media, minimization of suspected infection, and the segregated use of devices to avoid the inadvertent spread of malware between them.

Applicable Standards and Regulations:

45 CFR § 164.308(a)(5)(ii)(B)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-220: Log in Monitoring

Purpose:

The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall monitor user login attempts, restrict users who attempt to login to the network and information system without using appropriate login procedures, and identify users who abuse the county's login policy and procedure.

ADDITIONAL

To ensure that access to servers, workstations, and other computer systems containing PHI is appropriately secured; Mahaska County will configure all critical components that process, store or transmit ePHI to record log-in attempts – both successful and unsuccessful – as well as automatic lock out and reporting after 3 failed attempts.

Procedures:

Mahaska County has implemented the following procedures:

1. Network login monitoring is included in the system's software such that it can capture all system login attempts.

2. Each system server, PC, laptop or tablet independently logs each login attempt and anomalies will be periodically reviewed by Mahaska County's Chief Security Officer (CSO), either upon notification of routine login reports, receipt of anomalous incidents/reports or the beginning of each calendar quarter, whichever comes first.

3. Systems that provide for remote notification of unauthorized login attempts will be enabled to alert the CSO or an IT specialist/service, as designated by the CSO.

4. Each system will be set to restrict additional login attempts by users who fail at least three times to employ the appropriate protocol(s) to access the network or information system.

5. If the user is locked out, the user must contact CSO or an IT specialist/service designated by the CSO for or reinstatement of the user's login authorization.

Applicable Standards and Regulations:

45 CFR § 164.308(a)(5)(ii)(C)
45 CFR § 164.308(a)(1)(ii)(D)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-225: Data Back-Up and Storage

Purpose:

The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to the confidentiality, integrity and availability of electronic protected health information (ePHI). This policy covers procedures that Mahaska County will develop for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Planning
- Emergency mode operation plan

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall implement appropriate procedures to create and maintain retrievable exact copies of electronic protected health information, including procedure to ensure that data at rest is secure from unauthorized acquisition, access, use or disclosure of electronic protected health information.

Procedures:

Mahaska County has implemented the following procedure for the back-up of locally maintained data:

1. The Chief Security Officer (CSO) and/or IT Director will oversee backup of all locally stored ePHI and business operating data essential to disaster recovery utilizing encrypted external storage devices solely designated for that purpose, as outlined here.
2. Data will be backed up using at least two devices in a father-grandfather manner at least twice a week which have been pre-scanned for malicious software and hardware faults.
3. Backup devices will be utilized on a rotating (generational) basis so that the oldest backup is overwritten first when conducting a scheduled data backup.

4. The newest (father) backup will be maintained under double lock and key in a fireproof, theft resistant safe offsite away from the Mahaska County's principal place of business.
5. The oldest (grandfather) backup will be maintained under double lock and key in a secure designated location at the county's principal place of business.
6. The integrity of each backup will be verified weekly and contemporaneously logged.

Applicable Standards and Regulations:

45 CFR § 164.308(a)(7)(ii)(A)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-230: Disaster Recovery Plan

Purpose:

The purpose of this policy is to comply with the HIPAA Security Rule's requirements pertaining to its response to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

The scope of this policy contains procedures regarding a contingency plan that shall be developed and implemented in the event of an emergency, disaster or other occurrence (i.e. fire, vandalism, system failure and natural disaster) when any system that contains ePHI is affected, including data backup, disaster recovery planning and emergency mode operation plan. This policy covers all ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use, or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall maintain back-up data sets that can be used to recreate lost data following a system failure or other disaster. The Chief Security Officer (CSO), along with the IT Director or her/his designee, shall make the determination when a backup data set should be used to recreate or restore lost data based upon a current assessment of the nature and circumstances of the data loss, as well as any other impairment of the county's information system.

Mahaska County may, at the discretion of the CSO, contract with a third party to provide the services outlined in the procedure(s) related to this policy. In the event a third party is engaged, the specific requirements of this policy will be included in either the" terms of service", or included in a Statement of Work ("SOW"), and made part of the agreement for the contracted services.

Procedures:

Workforce members, Elected Officials and volunteers who believe that a system failure or other disaster has resulted in the loss of information should promptly report the possible failure to the county CSO or on-duty workforce member responsible for operating the information system.

Workforce members responsible for preparing backup data sets shall test the backup copies to ensure that they contain an exact copy of the information they back up and can be used to restore data when needed.

Workforce members will be notified promptly of any data lost following restoration of the backup data set using Mahaska County's notification system specified in Policy and Procedure PS-155

"Contingency Operations." Data loss may indicate potential violation of county policy/procedure or federal/state regulations regarding the handling and safeguarding of such data and thus require diligent investigation. For example, a machine failure destroys information created since the last backup. Workforce members should be notified as soon as possible that these data have been lost; and backup copies should be made available to users within one working day of being requested and the CSO shall coordinate with the Chief Privacy Officer (CPO) to conduct an initial investigation and identify potential corrective action.

Note: Procedures for restoring data are documented in Policy and Procedure PS-155 "Contingency Operations."

Applicable Standards and Regulations:

45 CFR §164.308(a)(7)(ii)(B)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-235: Emergency Mode Operation Plan

Purpose:

The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to its response to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

The scope of this policy contains procedures regarding a contingency plan that shall be developed and implemented in the event of an emergency, disaster or other occurrence (i.e. fire, vandalism, system failure or natural disaster) when any system that contains ePHI is affected, including data backup, disaster recovery planning and emergency mode operation plan. This policy covers all ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers (including students, residents, interns and others) who collect, maintain, use, or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County has established procedures to safeguard the security of PHI during emergencies that impair normal security safeguards. The workforce members responsible for creating and implementing these procedures are specified in greater detail in Mahaska County's contingency plan.

Procedures:

The Chief Security Officer (CSO) develops detailed emergency-mode operating procedures as part of the comprehensive contingency plan. These procedures safeguard the provider's information resources and PHI during emergencies that disrupt normal security measures. During an emergency that disrupts power supplies, Mahaska County's information systems are shut down. Only the following are supported by back-up power supplies or alternative power sources:

- _____
- _____
- _____
- _____
- _____

Power interruptions and other disasters that disrupt even these essential services are sufficient reason to close Mahaska County's office until essential services have been restored.

During power disruptions, workforce members maintain paper records of information that would ordinarily be recorded electronically. After restoration of power, electronic databases are updated from these paper records.

When an emergency condition exposes components of the provider's information system to theft or unauthorized removal, the Chief Security Officer or a designated workforce member is present to prevent loss of information or essential system components.

A complete inventory of any damage to information system components is conducted after the emergency condition resolves.

Applicable Standards and Regulations:

45 C.F.R §164.308(a)(7)(ii)(C)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-240: Testing and Revision of Contingency Plans

Purpose:

Mahaska County shall establish procedures to review and test the county's contingency plans on an annual basis. In the event the review justifies a revision, the revision will be documented, tested, and implemented. Elected Officials, Department Heads and other workforce members responsible for creating and implementing these procedures are specified in greater detail in the county's contingency plan.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (ePHI) for any purposes. This policy covers all ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County requires testing procedures be developed for the data backup, disaster recovery, and emergency mode operations plan. These plans must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner, with or without the availability of the primary delivery method. Revisions to plans described based on changes due to systems design, policy changes (internal or external), or testing results will be documented and submitted.

Procedures:

On an annual basis the Chief Security Officer and/or IT DIrector shall conduct the following:

A. Test Mahaska County's contingency plans, evaluate the adequacy of such plans, revise them as necessary and retest them to verify the adequacy of the plans as revised;
B. Test the backup data sets to verify they contain exact copies of the information that they are intended to back up and that the backup data can successfully be restored;
C. Inspect and test emergency power supplies to confirm they will provide power for the amount of time specified in the contingency plan;
D. Test fire alarms and inspect any fire suppression equipment installed to confirm they will operate as intended and be available when needed;
E. Review contingency plans with the Elected Officials, Department Heads and workforce members responsible for implementing them;
F. Train and drill new Elected Officials, Department Heads and workforce members who will implement contingency plans; and

G. Document the review, any other steps not specified here to test the contingency plan, and any initial or recurrent training completed in the course of testing the contingency

Applicable Standards and Regulations:

45 CFR §164.308(a)(7)(ii)(D)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-250: Applications and Data Criticality Analysis

Purpose:

As part of the development of a comprehensive contingency plan, Mahaska County's Chief Security Officer (CSO) shall assesses the criticality of specific applications and data and shall oversee the development of a contingency plan addressing system malfunction and data loss.

Arrangements shall be made to ensure that critical applications and equipment are replaced within one work day in the event of failure and critical data shall be backed up as provided in the county's data backup plan.

Responsible for Implementation:

Chief Security Officer and/or IT Director

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (ePHI) for any purposes. This policy covers all ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

The purpose of this criticality analysis is to document the impact to services, processes, and operating objectives if a disaster or other emergency causes ePHI systems to become unavailable for a period of time. The criticality analysis will serve as the basis for the prioritization of restoration of ePHI and ePHI systems.

Procedures:

Every three (3) years, the CSO and/or Director of IT will analyze all applications, computer hardware and provider data in order to identify those applications, hardware components and data sets critical to Mahaska County's successful handling of ePHI and sensitive county data. The CSO will also review this three-year applications and criticality analysis annually, updating it as needed. Findings and recommendations developed from these analyses and updates shall be presented by the CSO and reviewed by the Chief Privacy Officer (CPO) and the Board of Supervisors.

The criterion for identifying critical components is whether rendering a component unusable or unavailable would significantly disrupt Mahaska County's ongoing operation or compromise the integrity or security of ePHI and essential business data.

To determine component criticality, the CSO will assess the options for replacing the affected component(s). The analysis shall identify components that must be quickly replaced or restored to operating condition during an emergency. It shall also identify the longest period of time that those

components judged critical can be unavailable and also identify the most cost-effective method of restoring function within the critical time period.

Applicable Standards and Regulations:

45 CFR §164.308(a)(7)(ii)(E)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-255: Device and Media Controls and Accountability

Purpose:

According to the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR 164.310(d)(2)(iii), relative to Mahaska County, departments that use, store, maintain, or are otherwise responsible for electronic protected health information (ePHI) must implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a department, and the movement of these items within the department, and to maintain records of that movement. Thus, this standard is mandatory for ePHI and recommended for all other electronic sensitive information.

Responsible for Implementation:

Chief Security Officer

Scope:

All personnel responsible for managing Departmental data processing equipment with ePHI or other sensitive information, especially data owners and data custodians. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

A record is maintained of any movement of computer equipment within the county and all removal of equipment and storage media from Mahaska County. This policy applies to the transfer of storage media to off-site storage locations. This policy does not apply to routine shifting of equipment during ordinary operation or maintenance.

Procedures:

The Chief Security Officer (CSO) maintains an inventory of all computer hardware installed in the county. The log includes:

- A description of the equipment
- The equipment serial number
- The date on which the equipment was installed
- The location of the equipment
- The name of the person responsible for installation

Log entries are made in the inventory of computer hardware for all equipment that is removed from county facilities. The log entry includes:

- The date on which the equipment was removed
- The destination of the equipment
- The reason for removal, such as repair or disposal
- The person responsible for preparing the equipment for removal, including any sanitizing of storage devices

When storage media are transferred to off-site storage facilities, a record is made of the date and time the media were removed from the facility and the date and time the media arrived at and were processed by the storage facility.

Applicable Standards and Regulations:

45 C.F.R §164.310(d)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): County Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

AS-260: Policies and Procedures for Conducting Business with Business Associate

Purpose:

Mahaska County shall protect the confidentiality and integrity of health information of its patients. This policy defines the guidelines and procedures that must be followed by Mahaska County's business associates that come into contact with protected health information (PHI).

Note: In short, any person or any organization (except a Mahaska County workforce members, Elected Official or volunteer) that receives, transmits, or uses PHI belonging to or managed by Mahaska County is considered a business associate, whether or not a business associate agreement has been signed. A sample business associate agreement can be found in Policy and Procedure AS-260a "Business Associate Agreement."

A business associate may receive PHI from the county, create PHI for the county, or transmit data on behalf of the county.PHI may be disclosed to business associates only if Mahaska County receives satisfactory assurances with the Business Assoiciate Agreement (BAA) that the business associate will safeguard the privacy of the PHI that it creates or receives.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

To establish guidelines for Mahaska County to identify those vendor/business relationships which meet the HIPAA definition of a "business associate" and provide direction in establishing formalized business associate agreements. Mahaska County shall implement the required procedures and ensure documentation to establish satisfactory assurance of compliance.

Procedures:

Written contracts or agreements must be negotiated between Mahaska County and any business associate that will handle protected health information it receives from or creates for the county. This contract or agreement must include provisions that:

1) Identify the uses and disclosures of protected health information permitted under the contract;

2) Permit the business associate to use or disclose the information only as permitted under the privacy standards;
3) Restrict use and disclosure of the protected health information the business associate creates or receives to those that are specified in the contract;
4) Call on the business associate to fully comply with the provisions of the HIPAA privacy and security regulations, not limited by specific references in the contract with Mahaska County;
5) Provide for reporting to Mahaska County any use or disclosure of protected health information that is not provided for under the terms of the business associate's contract;
6) Require the business associate to apply the same restrictions and conditions on use and disclosure of protected health information to the agents and subcontractors to whom it forwards the protected health information;
7) Make protected health information available to patients;
8) Amend any protected health information that it receives when asked to do so by Mahaska County;
9) Make available to Mahaska County the information it needs to account for uses and disclosures of protected health information;
10) Make internal countys, books, and records related to the use and disclosure of protected health information available to the U.S. Department of Health and Human Services (HHS) for the purposes of determining compliance with the privacy standards;
11) Return, if feasible, all protected health information to Mahaska County upon termination of the contract, and destroy any copies of such information;
12) When return and/or destruction of protected health information is not feasible, the business associate will extend contractual protections to the use and disclosure of the information for the purposes that make its return or destruction infeasible;
13) Notify Mahaska County in the event of an unauthorized disclosure of unsecured PHI/ePHI;
14) Provide for termination of the contract if the business associate violates these contractual provisions;
15) Require that the business associate comply with the privacy rule to the extent the business associate is carrying out Mahaska County's obligations under the privacy rule; and
16) Require that business associates enter into business associate agreements with their subcontractors, such agreements imposing the same obligations that apply to the business associates themselves.

Duty of Workforce Members, Elected Officials and Volunteers to Report Contractual Breaches by Business Associates

If workforce members, Elected Officials and volunteers become aware of activities or practices by the business associate that violate the Mahaska County's contractual obligations under HIPAA regulations, then the activities or practices must be reported to Mahaska County's Chief Security Officer (CSO) or Chief Privacy Officer (CPO). Additionally, any report of violations by the business associate received by the CSO shall be relayed promptly by the CSO to the CPO who will lead the investigation and correction of contractual violation and breaches with the assistance of the CSO, as needed, and in coordination with Mahaska County's Board of Supervisors.

Investigation and Correction of Contractual Breaches

When Mahaska County's CPO is notified that a business associate has violated a contractual provision related to the privacy of protected health information, he or she must implement the following procedure to correct the violation.

1) The CPO will contact the business associate and determine whether a contractual provision has been violated.
2) If a contract provision has been violated, the CPO will identify steps to be taken by the business associate that will enable it to comply with its contractual obligations.
3) The CPO will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If an agreement can be reached, the corrective measures will be summarized in writing and sent to the business associate.
4) The CPO will monitor the implementation of the corrective action measures by periodically contacting the business associate. The CPO may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future.
5) If it is not possible to develop an acceptable corrective action plan, CPO should implement the procedures established to terminate the contract.

Reporting of Contractual Breaches by Business Associates

When the CPO is not able to correct violations of contractual obligations by a business associate, he or she should implement the following procedure:

1) Identify an alternative source for the services provided by the business associate;
2) Refer the matter to the Mahaska County Attorney with a request that formal action be taken to terminate the contract;
3) Have Mahaska's County Attorney notify the business associate that action will be taken to terminate the contract if the violation of contract provisions is not immediately corrected; and
4) Monitor the status of the contract and arrange for replacing the business associate, in consultation with Mahaska County's Board of Supervisors when the contract is formally terminated. If the contract cannot be terminated, the facts of the contract violation as they are known will be reported by legal counsel to HHS, as required by federal regulations.

Applicable Standards and Regulations:

45 CFR §164.308(a)(8)(4)
45 CFR §164.314(a)(1)(ii)
45 CFR §164.314(a)(2)(i)(A)
45 CFR §164.314(a)(2)(i)(B)
45 CFR §164.314(a)(2)(i)(C)
45 CFR §164.314(a)(2)(i)(D)
45 CFR §164.502(e)
45 CFR §164.504(e)(1)
45 CFR §164.308
45 CFR §164.314(a)(i)
45 CFR §164.314(a)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS-261: Business Associate Due Diligence

Purpose:

With the passage and implementation of the Final Omnibus Rules in 2012 and 2013, the "Safe Harbor" exemption from liability for breached by business associates was removed. Now, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act and applicable rules issued by the Department of Health and Human Services (HHS) mandate that every business associates agrees to:

1. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
2. Protect against reasonably anticipated, impermissible uses or disclosures of PHI; and
3. Identify any "pattern of activity or practice by a business associate in violation of the business associate agreement and it fails to take reasonable steps to cure the breach and if unsuccessful, terminate the contract if feasible"

Given that business associates account for a significant number of HIPAA related breaches, in some studies, over 30%, complying with the requirement to conduct due diligence on business associates is a critical component of the Mahaska County's security and privacy program.

This policy outlines the steps that Mahaska County will go through to conduct sufficient due diligence on business associates, to both comply with the regulations and maintain the privacy and security of Mahaska County's protected health information (PHI).

Responsible for Implementation:

Chief Privacy Officer

Scope:

All Mahaska County business associates are required to participate in the Mahaska County's due diligence investigation.

Policy:

The Chief Privacy Officer (CPO), or their designate (the "investigator"), is required to conduct a due diligence investigation on each of the Mahaska County's business associates. Such investigations will be conducted before, or in a reasonable period of time following, the signing of a business associate agreement.

Additional due diligence will be conducted annually and/or as part of the remediation of a security incident or breach by the business associate.

In the event any due diligence investigation uncovers any "pattern of activity or practice by a business associate in violation of the business associate agreement and it fails to take reasonable steps to cure the breach and if unsuccessful, terminate the contract if feasible.

Procedures:

To ensure appropriate due diligence is conducted, Appendix A will be used. Upon completion of the due diligence document, the investigator is required to generate a report, Appendix B, indicating that the business associate is in compliance with or not in compliance with the requisite HIPAA Regulations, the business associate refused to participate with the due diligence investigation.

The report will be reviewed by the CPO, discussed with the Board of Supervisors, appropriate Elected Officials or Department Heads and made part of the file of the business associate. The Board of Supervisors will determine the course of action to be taken with the business associate, as determined by the resolution of the due diligence.

Applicable Standards and Regulations:

45 C.F.R. §164.308(a)(5)(ii)(A)
45 C.F.R. §164.502(a)
45 C.F.R. §164.502(b)
45 C.F.R. §164.514
45 C.F.R. §164.530

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

HIPAA Diagnostic - A Rubric for Compliance

Is our Business Associate HIPAA Compliant?

Under the Final Omnibus Rules governing HIPAA compliance we are required to conduct due diligence on your business associates. What follows are some questions to help us assess your compliance under the regulations:

1. Are your HIPAA policies and procedures up to date, effective and available?

☐YES ☐ NO

All business associates should have organizational policies and procedures that address each requirement in the HIPAA Privacy and Security regulations. These HIPAA policies also need to address the changes outlined in the HITECH Act, enacted as part of ARRA (the "Regulations"). Further, when the final HITECH Act regulations were published in January 2013, HIPAA policies and procedures needed updating.

Policies and Procedures need to follow the requirements outlined in the Regulations, and be maintained in a "Master Manual" and be available for all employees, on an as needed basis. Organizations should also be monitoring employee compliance with HIPAA regulations to ensure that the policies and procedures in place effectively guide employees to correctly follow required HIPAA practices.

2. Is your HIPAA training effective and up to date?

☐YES ☐NO

HIPAA requires all business associates to deliver HIPAA training to its employees. These training presentations should be updated on a regular basis to reflect regulatory or organizational changes.

Additionally, organizations should have a system in place that evidences training completion, as well as procedures to ensure that trainings are delivered and attended in accordance with internal policies and procedures. Further, organizations should have evidence to substantiate that the trainings delivered are effective in providing employees with the information necessary to comply with HIPAA.

3. **Has a risk assessment been conducted?**
    a) **Did you follow the NIST SP800-30 protocol?**
    b) **Did you generate a Remediation Plan?**
    c) **Are the assessment and remediation plans updated regularly?**

☐YES ☐NO

The HIPAA Security Rule Administrative Safeguards provisions require business associates to perform a risk assessment as part of their security management processes. When analyzing potential risks to the security of PHI, organizations should (1) evaluate each risk's likelihood and impact; (2) implement appropriate security measures to address identified risks; and (3) document the selected security measures, including an explanation of the reasoning for selection. Any corrective action taken by an organization as a result of the risk assessment findings should be monitored to completion and documented. While not part of the Privacy Regulations, best practice is to conduct the same risk assessment on privacy management processes.

Once the Risk Assessment is completed, a remediation plan is required. The remediation plan outlines a strategy to remediate the gaps in compliance identified during the Risk Assessment. For each identified threat, the plan should include the risk score for the threat, the action to be taken to mitigate the threat, the individual responsible in mitigating the threat, and a target date for the threat to be mitigated. Meaningful progress in implementing the mitigation plan is required for compliance.

Because risk assessment is an ongoing process, organizations should update their risk analysis, at least annually, to ensure that risks are appropriately identified, remediated and monitored. Additionally, internal controls and security measures used should be regularly monitored and evaluated to ensure that PHI is appropriately and effectively protected.

4. Do you have an ongoing auditing and monitoring programs for HIPAA Privacy and Security?

☐YES ☐NO

Organizations should be monitoring their HIPAA Privacy and Security compliance on an ongoing basis. Compliance Officers, in conjunction with the HIPAA Privacy and Security Officers, should be monitoring completion of HIPAA education, as well as detecting and investigating potential HIPAA compliance incidents occurring during daily operations. Additionally, there should be several HIPAA items included in the organization's annual audit plan, specifically focusing on ensuring that patient records are accessed and disclosed appropriately and that internal controls are effectively securing PHI.

5. Have you conducted due diligence on your sub-contractors?

☐**YES** ☐**NO**

With the publication of the Final Omnibus Rules in January 2013, your relationship with your sub-contractors has fundamentally changed. You, and the covered entity you are a business associate to can be held liable for breaches caused by your subcontractors.

You now have a requirement to investigate your sub-contractors to assure yourself that they are in fact complying with the same HIPAA requirements as you, and that there is not a pattern of behavior that has caused breaches in the past, or will likely cause a breach in the future.

6. Can you provide the following?

		YES	NO
a)	The signature pages of your most recent Security Risk Assessment	☐	☐
b)	The signature page of your most recent Remediation Plan	☐	☐
c)	The signature page of your HIPAA Master Policy and Procedure manual	☐	☐
d)	A copy of your most recent network vulnerability scan	☐	☐
e)	A sample of your most recent training materials and logs	☐	☐

Based on these results you are/are not satisfying the regulatory requirements of HIPAA

For: Date:

By:

Signature:

<Date>

To «Chief Privacy Officer»,

I have conducted the requisite due diligence on _____ our business associate, as per the process outlined in our Policy AS-261, see attached document (Appendix A of AS-261).

My due diligence consisted of reviewing:

- Their most recent Security Risk Assessment and Remediation Plan,
- Their HIPAA Master Policy and Procedure Manual, and
- Their most recent training logs

In my opinion _____

Pick one of the following:

- is complying with its obligations under HIPAA/HITECH. As such, we should have confidence we are not carrying any additional or unwarranted liabilities in the event of either a breach of your ePHI, or from an audit by CMS or OCR.

- is **not** compliant with its obligations under HIPAA/HITECH. As such, you should be aware that we may be carrying some additional and unwarranted liabilities, in the event of either a breach of ePHI or from an audit by CMS or OCR. As such I recommend you address this with _____.

- Has refused to cooperate with my attempts to conduct our required due diligence. As such, you should be aware that we may be carrying some additional and unwarranted liabilities, in the event of either a breach of ePHI or from an audit by CMS or OCR. As such I recommend you address this with _____.

Best regards,

Signature

Title

AS 265: Identifying Business Associates and Distributing BA Agreements

Purpose:

A business associate that creates, receives, maintains, or transmits electronic protected health information (ePHI) for Mahaska County must provide satisfactory assurances that it will appropriately safeguard the information. These assurances must be included in a written contract or other arrangement with the business associate.

It is Mahaska County's policy to comply with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) regulations requiring Mahaska County to contract with all such business associates in accordance with such regulations as they may be modified from time to time.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) or ePHI for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

It is the policy of Mahaska County to assure itself that its business associates are in compliance with all applicable regulations governing business associates and it shall conduct a due diligence review prior to sharing or transmitting PHI/ePHI to such entities. However, Mahaska County's Chief Privacy Officer (CPO) may exempt any organization from the requirement to submit information as part of this policy with the concurrence of Mahaska County's Board of Supervisors. In such an event, the CPO, understanding the risks associated with exempting an organization, shall provide a written documentation of the exemption. Such documentation shall include:

1. The term of the exemption; and
2. The reason(s) for granting the exemption.

Procedures:

1. Business Associate Agreements (BAA's)

Written contracts or agreements must be established with all business associates before the exchange or creation of PHI/ePHI with or by the associate.

All written contracts or agreements must contain the assurances identified in Mahaska County's policies for business associate agreements, including the required termination provisions.

2. Procedure for Identifying Business Associates

To identify all business associates, Mahaska County will undertake the following steps:

A. Review all vendors with whom Mahaska County has done business.

B. Eliminate all vendors that are healthcare or mental health contractors providing treatment services as not being business associates

C. Eliminate all vendors that do not, may not or likely will not have access to or transmit Mahaska County's PHI/ePHI.

See Policy and Procedure AS-260c "BA Decision Tree" for a tool to use when assessing in an entity is a Business Associate

3. Procedure for qualifying Business Associates

Each vendor/entity which qualifies as business associates will undergo a due diligence review conducted by Mahaska County's CPO and CSO, or a qualified designee and will be required to complete a business associate agreement with Mahaska County before accessing, creating or transmitting PHI/ePHI on behalf of Mahaska County. Such agreements must address the information listed in Policy and Procedure AS-260a "Business Associate Agreement" of Mahaska County's Master HIPAA manual before any PHI/ePHI from Mahaska County may be exchanged. Amendments to pre-existing business associate agreements will be offered and shall be executed in a timely manner in the event relevant/mandatory post-agreement regulatory changes are made.

Applicable Standards and Regulations:

45 CFR §164.314(a)(i)(2)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

AS 270: Education and Training

Purpose:

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act and its applicable rules issued by the Department of Health and Human Services (HHS) mandate that every covered entity provide training for all members of its workforce with respect to awareness of HIPAA regulations, patients' and individual's rights and Human Resource Management responsibilities with respect to "policies and procedures" on use and disclosure of Protected Health Information (PHI) as necessary and appropriate for Mahaska County workforce members, Elected Officials and volunteers to carry out their function within the county as a covered entity. It is the policy of Mahaska County to comply with training mandates.

Responsible for Implementation:

Chief Privacy Officer

Scope:

Mahaska County workforce members, Elected Officials and volunteers, whether salaried or non-salaried, are required to complete HIPAA privacy and information security training. This includes students, volunteers, Board Members and others who may have either direct or indirect access to PHI.

Policy:

Each person who handles PHI must be aware of the obligations imposed by HIPAA and the Privacy and Security Rules. Mahaska County has developed general HIPAA training which is required to be taken by every member of the workforce who comes in contact with PHI. Certain special training modules are required to be taken by those whose jobs require them to be in closer contact with PHI. Each department will determine the appropriate training modules to be taken by its workforce. Additional training on local procedures should be provided by each department in the covered entity.

Procedures:

The following procedures will be implemented to ensure appropriate training and education:

1. Every current Mahaska County workforce member, Elected Official and volunteer will be trained;
2. Each new Mahaska County workforce member, Elected Official and volunteer will receive similar training as part of the mandatory new employee orientation sessions;
3. Retraining will be provided for anyone "whose functions are affected by a material change in the policies or procedures… within a reasonable period of time after the material change:"
4. Post privacy/ security incident training on the policy and procedures related to the regulation(s) associated with the incident;

5. Mahaska County will document that such HIPAA Awareness and Privacy Training has been provided to all Mahaska County workforce members, Elected Officials and volunteers;
6. Mahaska County will modify its management and workforce training program to include the modified requirements as described by the ARRA/HITECH act and the subsequent HHS/OCR rules and regulations; and
7. Mahaska County will conduct a training program to update management and workforce on the updated rules, policies and procedures.

Applicable Standards and Regulations:

45 C.F.R. §164.308(a)(5)(ii)(A)
45 C.F.R. §164.502(a)
45 C.F.R. §164.502(b)
45 C.F.R. §164.514
45 C.F.R. §164.530

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

DR-105: Development and Maintenance of Security Policies and Procedures

Purpose:

This policy defines requirements for system security planning and management to improve protection of Mahaska County information system resources. Security has to be considered at all stages of the life cycle of an information system (i.e., feasibility, planning, development, implementation, maintenance, and retirement) in order to: a) ensure conformance with all appropriate security requirements, b) protect sensitive information throughout its life cycle, c) facilitate efficient implementation of security controls, d) prevent the introduction of new risks when the system is modified, and e) ensure proper removal of data when the system is retired.

This policy provides guidance to ensure that systems security is considered during the development and maintenance stages of an information system's life cycle.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy applies to all Mahaska County departments, administrative units, and affiliated organizations that use information technology resources to create, access, store or manage Mahaska County data to perform their business functions. The requirements apply to enterprise information systems or systems that require special attention to security due to the risk of harm resulting from loss, misuse, or unauthorized access to or modification of the information therein.

Policy:

Mahaska County is responsible for developing and maintaining written security policies and procedures pursuant to the Health Insurance Portability and Accountability Act (HIPAA) security standards.

Procedures:

The Chief Security Officer (CSO) will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for the protection of the security of health information. The CSO may delegate this responsibility, but such delegation must be reflected in that individual's job description, and the CSO will supervise the development of all security policies and procedures.

The CSO must:

- Monitor changes in federal and state law and regulations that may require changes in security policies and procedures;

- Notify Board of Supervisors, Elected Officials, and Department Heads of the issuance of new or revised federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented;

- Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations;

- Identify any revisions needed in the security orientation and training program to reflect revised policies and procedures. Before a revised policy or procedure is submitted for approval, the CSO will review the notice of security practices form and determine whether the notice must be revised to reflect the new security policies or procedures. The effective date of a revised policy or procedure must not be earlier than the date on which the revised notice of security practices is posted and made available to patients. All policies and procedures must be approved by the Board of Supervisors of Mahaska County before they can be implemented. New or revised policies and procedures are to be qqqq through the following:

    - An all-county memorandum from CSO will announce the adoption of the new or revised policies and indicate affected staff functions. This memorandum should describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for review;

    - CSO or a designated representative will announce the adoption of the new policies at appropriate county and/or department meetings and provide appropriate training. A memorandum from CSO to those staff members whose job responsibilities are directly affected by the new policies should indicate whether training or orientation meetings or programs will be held and whether background information on the new policies is available. A copy of the revised policy should be attached to the memorandum, or individuals should be directed to consult the updated policy and procedure manual; and

    - Copies of the revised policy will be distributed to Mahaska County Department Heads and Elected Officials for updating copies of the policy manual.

Applicable Standards and Regulations:

45 C.F.R §164.316(a)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

Darin Hite		

DR-100: Periodic Evaluation of Privacy and Security Policies

Purpose:

Mahaska County is committed to conducting business in compliance with all applicable laws, regulations and Mahaska County policies. Mahaska County has adopted this policy to ensure that its Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policies are up to date and effective in ensuring the confidentiality, integrity and availability of electronic Protected Health Information (ePHI) created, received, maintained and transmitted by Mahaska County.

Responsible for Implementation:

Chief Privacy Officer and Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce member, Elected Official and volunteer who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County will perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Privacy and Security regulations and subsequently, in response to environmental or operational changes affecting the privacy and security of ePHI, that establishes to the extent to which an entity's privacy and security policies and procedures are effective.

Procedures:

Mahaska County's Privacy and Security Procedures initially will be evaluated to determine their compliance with the HIPAA Privacy and Security Regulations. Once compliance with the Privacy and Security Regulations is established, the Mahaska County Privacy and Security Policies will be evaluated on a periodic basis to assure continued viability in light of technological, environmental or operational changes that could affect the security of ePHI.

1. Periodic Evaluation by Mahaska County Chief Privacy Officer (CPO) and Chief Security Officer (CSO)
    a. The CPO/CSO will review on an on-going basis the viability of Mahaska County's Privacy and Security Policies and general approaches taken by Mahaska County workforce member, Elected Official and volunteer in their Privacy and Security Procedures;
    b. The CPO/CSO will develop and recommend any necessary Policy or Procedure changes;
    c. The CPO/CSO evaluate, on an annual basis, the technical and nontechnical viability of Mahaska County Privacy and Security Policies;
    d. The CPO/CSO or any other person may suggest changes to the Security Policies or Procedures by submitting such suggestion to the CPO/CSO for consideration;

e. The CPO/CSO will review any suggested Privacy and Security Policy or Procedure change and make a preliminary recommendation;
f. If the CPO/CSO preliminarily recommends a new privacy and security standard or a change in Mahaska County's Privacy and Security Policies or Procedures, such new standard or change will be communicated to Mahaska County Elected Officials and Department Heads by the CPO/CSO, who will elicit feedback for a specific period of time and provide such feedback to the CPO/CSO;
g. The CPO/CSO will consider the feedback received and make a final recommendation on the suggested change to the CPO/CSO.
h. If the CPO/CSO approves the change, such change will be propagated to Mahaska County Departments through policy updates and reminders. Mahaska County will be required to update their Privacy and Security Procedure in a timely manner to incorporate the change.
i. The CPO/CSO will update Mahaska County's HIPAA Master Manual with the approved Privacy and Security Policy or Procedure and sign with the appropriate effective date.

2. Evaluation Upon Occurrence of Certain Events
   a. In the event that one or more of the following events occur, the policy evaluation process described in Paragraph 2 will be immediately triggered:
      i. Changes in the HIPAA Security or Privacy Regulations
      ii. New federal, state, or local laws or regulations affecting the privacy or security of ePHI
      iii. Changes in technology, environmental processes or business processes that may affect HIPAA Security Policies or Procedures
      iv. A serious security violation, breach, or other security incident occurs
   b. The CSO may begin evaluation if deemed necessary based on information received from, but not limited to, the CPO or an Internal Audit.
3. Evaluation of Mahaska County Procedures
   a. Mahaska County must periodically evaluate its HIPAA Privacy and Security Procedures to ensure that departments follow such procedures and that these procedures maintain their technical and non-technical viability and continue to comply with the HIPAA Privacy and Security Policies. The schedule for this periodic evaluation will be defined per paragraph 5 below.
4. Internal Audit of Privacy and Security Policies and Procedures
   a. All Mahaska County's Privacy and Security Policies and Mahaska County Department procedures are subject to periodic audits, as defined by Mahaska County's Internal Audit Program.
   b. The Internal Audit Program will be conducted by Mahaska County's management and/or the CPO/CSO, or a designated third party, as appropriate.

Applicable Standards and Regulations:

45 C.F.R. §164.316(b)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

DR-115: Documentation Review and Retention

Purpose:

It is the policy of Mahaska County to comply with assessment, remediation and documentation standards of the federal government to reasonably protect the security and privacy of protected health information (PHI) and electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI information for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce member, Elected Official and volunteer who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County will implement an electronic and written version of Health Insurance Portability and Accountability Act (HIPAA) HIPAA Policies and Procedures with respect to protected health information, which are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy and Security Rules. Mahaska County will maintain documentation, in written or electronic form, of these HIPAA Policies and Procedures, communications in writing, actions or activities required to be in writing, and other administrative documents for a period of at least six (6) years from the date of creation or the date when last in effect, whichever is later. Mahaska County will incorporate into its policies, procedures and other administrative documents any changes in the Privacy and Security Rules. Mahaska County will properly document and implement any changes to policies and procedures.

Procedures:

Mahaska County will:

- Maintain, make available to all workforce, and update written/electronic HIPAA policies and procedures implemented to comply with Code of Federal Regulations subpart §164.316(b)(1)(i) in written (which may be electronic) form; and
- If an action, activity or assessment is required by subpart §164.316(b)(1)(i) to be documented, maintain a written (which may be electronic) record of the action, activity or assessment; and
- Retain the documentation required by this paragraph (b)(1) of this section for 6 years from the date of creation or the date when last in effect, whichever is later;
- Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

- Review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of PHI/ePHI.

Applicable Standards and Regulations:

45 C.F.R §164.316 (b)(2)(ii)
45 C.F.R.§164.530(j)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

DR-120: Availability of Documented Policies and Procedures

Purpose:

Mahaska County shall make available all relevant policies and procedures to those persons and entities responsible for implementing applicable policies and procedures.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and/or electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

The Chief Security Officer (CSO) will maintain multiple copies of the Health Insurance Portability and Accountability Act (HIPAA) Master Manual, in paper and/or electronic format, in locations accessible to all Mahaska County workforce members, Elected Officials and volunteers responsible for implementing HIPAA Policies and Procedures.

Procedure:

When Mahaska County's HIPAA Master Manual is updated, the CSO will replace all copies of the HIPAA Master Manual, in paper and/or electronic format, in locations accessible to all Mahaska County Elected workforce members, Elected Officials and volunteers, retaining all prior versions of the manual for the required six-year document retention period.

Applicable Standards and Regulations:

45 C.F.R §164.316 (b)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PR-105: Notice of Privacy Practices

Purpose:

The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. The Notice of Privacy Practices provides a mechanism to convey that information to our patients (45 CFR §164.52).

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

The HIPAA Privacy Rule gives individuals the to be informed of the privacy practices health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Mahaska County is required to develop and distribute a notice that provides a clear explanation of these rights and practices. The notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health care providers and exercise their rights.

Procedures:

Mahaska County is required to provide a notice in plain language that describes:

- How Mahaska County may use and disclose protected health information about an individual.
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to Mahaska County.
- The covered Mahaska County's legal duties with respect to the information, including a statement that Mahaska County is required by law to maintain the privacy of protected health information.
- Whom individuals can contact for further information about Mahaska County's privacy policies.

The notice must include an effective date.

Providing the Notice.

- Mahaska County must make its notice available to any person who asks for it.
- Mahaska County must prominently post and make available its notice on our web site that provides information about our customer services or benefits.
- Mahaska County must provide the notice to the individual no later than the date of first service delivery (after the April 14, 2003 compliance date of the Privacy Rule) and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.
- When first service delivery to an individual is provided over the Internet, through e-mail, or otherwise electronically, Mahaska County must send an electronic notice automatically and contemporaneously in response to the individual's first request for service. Mahaska County must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.
- In an emergency treatment situation, Mahaska County must provide the notice as soon as it is reasonably practicable to do so after the emergency situation has ended. In these situations, providers are not required to make a good faith effort to obtain a written acknowledgment from individuals.
- Mahaska County must make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the provider's office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.
- Mahaska County may e-mail the notice to an individual if the individual agrees to receive an electronic notice.

Content of the Notice.

The required contents of the notice are described in Form PR-105.

Applicable Standards and Regulations:

45 CFR §164.520
45 CFR §164.520(b)
45 CFR §164.520(b)(3)
45 CFR §164.520(c)(2)(iv)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

PR-115: Use of Protected Health Information (PHI)

Purpose:

To provide an overview of permissible uses and disclosures of protected health information (PHI) and electronic protected health information (ePHI) to cross reference applicable Mahaska County privacy policies addressing uses and disclosures in these situations.

Responsible for Implementation:

Chief Security Officer

Scope:

All Mahaska County workforce members, Elected Officials and volunteers who have direct or indirect access to PHI/ePHI created, held or maintained by Mahaska County.

Policy:

PHI will not be used or disclosed by Mahaska County workforce members, Elected Officials and volunteers except as permitted or required by Health Insurance Portability and Accountability Act (HIPAA) and applicable state laws. Whenever required by the HIPAA Privacy Rule, Mahaska County workforce members, Elected Officials and volunteers will make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Mahaska County must reasonably safeguard PHI: (i) from any intentional or unintentional use or disclosure that violates HIPAA policies, and (ii) to limit incidental uses or disclosures.

Procedures:

This Policy discusses the use and disclosure of PHI, addressed in sections as follows:

- Permitted Uses and Disclosures
- Required disclosures
- Minimum necessary applies
- Safeguards
- Uses and disclosures subject to an agreed-upon restriction
- Uses and disclosures of de-identified PHI, and to create de-identified PHI
- Disclosure to business associates
- Deceased Individuals
- Personal representatives
- Confidential communications
- Uses and disclosures consistent with the Notice of Privacy Practices
- Disposal of PHI

Permitted Uses and Disclosures

PHI may not be used or disclosed except as permitted or required by HIPAA and applicable state law. PHI may be used or disclosed as follows:

1) To the patient (or their authorized personal representative, as applicable) (the "individual");
2) For treatment, payment, or health care operations;
3) Incidental uses or disclosures that occur as a byproduct of a permissible or required use or disclosure, as long as reasonable safeguards are applied and the minimum necessary standard are implemented, where applicable, for the primary use or disclosure;
4) Pursuant to and in compliance with a valid authorization from the individual;
5) Pursuant to an agreement under or as otherwise permitted-- including, uses and disclosures:
   - to persons involved in a patient's care or payment;
   - for notification;
   - for disaster relief; and
   - to a family member or other persons involved in the care or payment for care of a deceased patient prior to death (limited to the PHI of a deceased individual that is relevant to such person's involvement) unless the disclosure would be inconsistent with any prior expressed preference of the individual that is known to Mahaska County.
6) As permitted by and in compliance with Mahaska County Policies which include uses and disclosures:
   - for public health activities;
   - for health oversight activities;
   - required by law;
   - about immunizations of a student or prospective student;
   - about victims of abuse, neglect or domestic violence;
   - for judicial and administrative proceedings;
   - for law enforcement purposes;
   - to avert a serious threat to health and safety;
   - about decedents;
   - for cadaveric organ, eye or tissue donation;
   - for research purposes;
   - for specialized government functions; and
   - for workers compensation.

<u>Required Disclosures</u>

Mahaska County workforce members, Elected Officials and volunteers are required to disclose PHI:

- To an individual upon request and subject to Patient Requests to Access PHI;
- For an accounting of disclosures of PHI provided to an individual upon request;
- When required by the Secretary of Health and Human Services (HHS) to determine Mahaska County's HIPAA compliance.

<u>Minimum Necessary Applies</u>

When using or disclosing PHI or when requesting PHI from another covered entity or a business associate, Mahaska County must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, as described in the Mahaska County HIPAA Policy and Procedure As-110 "Minimum Necessary Use and Disclosure."

Safeguards

Mahaska County workforce members, Elected Officials and volunteers must reasonably safeguard PHI: (i) from any intentional or unintentional use or disclosure that violates Mahaska County HIPAA policies, and (ii) in order to limit incidental uses or disclosures.

Uses and Disclosures of PHI Subject to an Agreed-Upon Restriction

Mahaska County workforce members, Elected Officials and volunteers that have agreed to a restriction under Restriction Request for Use and Disclosure of PHI or for alternative Confidential Communications may not use or disclose the PHI covered by the restriction in any manner that would violate the restriction, unless an exception applies as addressed in the policy.

Uses and Disclosures of De-Identified PHI and to Create De-Identified PHI

Mahaska County workforce members, Elected Officials and volunteers may use PHI to create de-identified PHI or may disclose PHI only to a business associate for de-identification. Health information that meets the standard and implementation specifications for de-identification is not considered to be PHI and can therefore be used or disclosed for any lawful purpose, as long as:

- a code or other identification is used to enable re-identification or for any other purpose does not constitute PHI; and
- the de-identified information is not re-identified.

Disclosures to Business Associates

Mahaska County workforce members, Elected Officials and volunteers may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if Mahaska County obtains satisfactory assurance that the business associate will appropriately safeguard the information and enters into a business associate agreement.

Deceased Individuals

Mahaska County workforce members, Elected Officials and volunteers must comply with the same use and disclosure requirements described in this Policy with respect to the PHI of a deceased individual. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to PHI relevant to such personal representation.

Personal Representatives

Except for unemancipated minors and/or abuse, neglect, and endangerment situations, Mahaska County workforce members, Elected Officials and volunteers must treat an authorized personal representative as the patient with respect to PHI for purposes of HIPAA. An authorized personal representative is a person with authority under applicable law to act on behalf of a patient in making decisions related to health care.

Confidential Communications

If Mahaska County workforce members, Elected Officials and volunteers have granted a patient’s request that they receive communications of PHI from Mahaska Countyby alternative means or at

alternative locations, the Mahaska County workforce members, Elected Offcials and volunteers must comply with the applicable HIPAA policies and requirements in communicating the PHI.

Uses and Disclosures Consistent with Mahaska CountyNotice of Privacy Practices

Mahaska County workforce members, Elected Officials and volunteers may not use or disclose PHI in a manner that is inconsistent with their Notice of Privacy Practices.

Disposal of PHI

Mahaska County workforce members, Elected Officials and volunteers must implement reasonable safeguards, including appropriate workforce training on the Mahaska County 's disposal policies and procedures, to limit incidental and avoid prohibited uses and disclosures of PHI in connection with the disposal of the information. In determining what is reasonable, Mahaska Countyworkforce members, Elected Officials and volunteers should consider potential risks to patient privacy, as well as the form, type and amount of PHI to be disposed.

Although no particular disposal method is required by HIPAA, proper disposal methods may include, for example:

- Shredding, burning, pulping, or pulverizing paper records so PHI is rendered essentially unreadable, indecipherable and cannot be reconstructed;
- Maintaining labeled prescription bottles and other PHI-containing material in opaque bags in a secure area and shredding or using another mechanism to destroy the PHI;
- For electronic media: clearing, purging, destroying, and other sanitization methods;
- Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy PHI;
- Using a business associate to appropriately dispose of PHI on Mahaska County's behalf.

Workforce members, Elected Officials and volunteers may not dispose PHI in a dumpster or other containers accessible by the public without using proper methods of rendering PHI essentially unreadable.

Applicable Standards and Regulations:

45 C.F.R. § 164.501
45 C.F.R. § 164.502
45 C.F.R. § 164.504
45 C.F.R. § 164.506
45 C.F.R. § 164.506(a)
45 C.F.R. § 164.508
45 C.F.R. § 164.508(a)(2)
45 C.F.R. § 164.508(3)
45 C.F.R. § 164.510
45 C.F.R. § 164.512
45 C.F.R. § 164.530(c)

Distribution:

Policy Distribution:

Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PR-120: Acknowledgement of Receipt of Notice of Privacy Practices

Purpose:

A Notice of Privacy Practices, compliant with the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule, will be given to every individual/client. Copies of prior versions of the Notice must be retained for six (6) years.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) or electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

It is the policy of Mahaska County that all individuals know the possible uses and disclosures of their protected health information, their rights, and Mahaska County's legal duties. Protected health information (PHI) is any personally identifiable health information transmitted or maintained by Mahaska County, in any form or medium, including electronic, or in a data base that relates to past, present, or future physical or health services or payment.

The Notice of Privacy Practices promotes understanding of how Mahaska County will protect individuals' information, circumstances in which protected health information may be used and disclosed by Mahaska County, individuals' rights, and Mahaska County obligations. Individuals must be informed and, in writing, acknowledge receipt of this information at their first date of service on or after April 14, 2003.

Procedures:

1. The Notice of Privacy Practices is the official description of:
    - How the Covered Entity uses Protected Health Information (PHI);
    - When the Covered Entity may disclose PHI;
    - The rights of the individual/client with respect to PHI; and
    - The Covered Entity's legal duties with regard to PHI.

The Notice of Privacy Practices will reflect the requirements contained in the HIPAA Omnibus Final Rule, as well as other state and federal laws that impact the Covered Entity's privacy practices.

2. The Notice of Privacy Practices must contain a statement indicating that the following uses and disclosures will be made only with an individual's written authorization:
    - Uses and disclosures of psychotherapy notes that are not for permitted treatment, payment or health care operations;

- Uses and disclosures of PHI for marketing purposes, including subsidized treatment communications; and
- Disclosures that constitute a sale of PHI.

3. The Notice of Privacy Practices must contain a statement indicating that the Covered Entity is required to notify the individual/client of any breach of his or her unsecured PHI.
4. If the Covered Entity intends to send fundraising communications to the individual/client, the Notice of Privacy Practices must inform the individual/client of the same and that he/she has a right to opt out of such fundraising communications with each solicitation.
5. The Notice of Privacy Practices must provide that if an individual/client has paid for services out-of-pocket, the Covered Entity must accommodate the individual's/client's request that the Covered Entity not disclose PHI related solely to those services paid for out-of-pocket if the disclosure is to be made to a health plan for payment or health care operations.
6. The Notice of Privacy Practices is approved by the Chief Privacy Officer (CPO). The CPO is responsible for revising the Notice of Privacy Practices to reflect any changes in practices regarding PHI. The Notice shall be written in plain language.
7. The Notice of Privacy Practices, or a summary of the same, is posted in a prominent location accessible to individuals/clients. The complete Notice of Privacy Practices must be made readily available upon request to existing individuals. If the Covered Entity has a website, the Notice is also available electronically through the Covered Entity's website.
8. A copy of the Notice of Privacy Practices must be offered to the client/individual at the time of the first service delivery. EXCEPTION: If treatment is first rendered in an emergency, the Notice is given as soon as reasonably practicable after resolution of the emergency.
9. The workforce member giving the Notice shall ask the client/individual to sign a written acknowledgement of receipt. If the individual/client refuses or is unable to sign, the circumstances will be documented on the acknowledgement form. The acknowledgement form will be retained in the individual's/client's record for six (6) years.
10. The Notice will be promptly revised whenever there is a material change to uses or disclosures of information, the individual's rights, the Covered Entity's legal duties or other privacy practices stated in the Notice. The revised Notice will be made available at each service delivery site for continuing individuals to take with them upon request and will be posted on Mahaska County's website(s), if applicable.

Applicable Standards and Regulations:

45 C.F.R. § 164.520

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

James Blomgren		

PR-130: Access and Denial of Request for PHI

Purpose:

It is Mahaska County's policy to recognize the right of an individual (or their authorized personal representative, as applicable) to access their protected health information (PHI) and electronic protected health information (ePHI), subject to the exceptions described in this Policy, in accordance with the requirements of Health Insurance Portability and Accountability Act (HIPAA) and state law.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials or volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

The access and denial process is managed under the direction of the Chief Privacy Officer (CPO).

Individuals have a right to inspect and receive a copy of the PHI in their designated record set. With the exception of:

1. Psychotherapy notes;
2. Information compiled in anticipation of or use in a civil, criminal, or administration action or proceeding; or
3. PHI subject to the Clinical Laboratory Improvements Amendments (CLIA) of 1988.

Procedures:

All Mahaska County personnel must strictly observe the following standards:

1. A individual has the right to inspect, or receive copies of PHI about the individual in a designated record set for as long as the PHI is maintained in the designated record set.
2. If Mahaska County does not maintain the PHI that is the subject of the individual's request for access, and Mahaska County knows where the requested information is maintained, Mahaska County must inform the individual where to direct the request for access.
3. The individual must make the request in writing using the Authorization form, to Obtain or Release Protected Health Information to the workforce member assigned to this duty. The Chief Privacy Officer will approve such requests.
4. Based on Mahaska County policy, Mahaska County must act on the individual's request no later than the 30th business day after receipt and payment of the request. Mahaska County shall:
    a. make the information available, in full or in part, for examination; or

b. inform the authorized requestor if the information does not exist, cannot be found, or is not yet complete. Upon completion or location of the information, Mahaska County will notify the individual.

5. If the access is granted, in whole or in part, Mahaska County must comply with the following requirements:
   a. Mahaska County must provide the individual access to his/her PHI in the designated record set, including inspection or receiving a copy, or both. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, Mahaska County must make all PHI available for access.
6. Mahaska County must provide the individual with access to the PHI in the form or format requested by the individual, if it is reasonably producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by both parties.
7. Mahaska County may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if:
   a. The individual agrees in advance to such a summary or explanation; and
   b. The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.
8. Mahaska County must provide the access as requested by the individual in a timely manner, including arranging with the individual for a convenient time and place to inspect or receive a copy of the PHI, or mailing the copy of the PHI at the individual's request. Mahaska County may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.
9. If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, Mahaska County may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
   a. Copying, including the cost of supplies for and labor of copying, the PHI requested. The fee schedule for these services is set by the State of _____. The fee schedule is maintained in each department responsible for releasing copies of PHI;
   b. Postage, if the individual has requested the copy, summary, or the explanation is mailed. The fee schedule for postage is maintained in purchasing.

Denial of Access

1. Mahaska County must allow an individual to request access to inspect or receive a copy of PHI maintained in their designated record set. However, Mahaska County may deny an individual's request without providing an opportunity for review when:
   a. An exception detailed above in the policy statement exists;
   b. Mahaska County is acting under the direction of a correctional institution and the prisoner's request to obtain a copy of PHI would jeopardize the individual, other prisoners, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the prisoner;
   c. The individual agreed to temporary denial of access when consenting to participate in research that includes treatment, and the research is not yet complete;

d. The records are subject to the Privacy Act of 1974 and the denial of access meets the requirements of that law;
e. The PHI was obtained from someone other than Mahaska County under a promise of confidentiality and access would likely reveal the source of the information; or
f. The PHI requested is not allowed for disclosure because it includes psychotherapy notes.

2. Mahaska County may also deny an individual access for other reasons, provided that the individual is given a right to have such denials reviewed under the following circumstances:
   a. A healthcare provider and/or a licensed healthcare professional, designated or appointed by the committee, has determined that access is likely to cause substantial harm or endanger the life or physical safety of the individual or another person;
3. If access is denied on grounds permitted above, the individual has the right to have the denial reviewed by a licensed healthcare professional, designated or appointed by the committee to act as a reviewing official, and who did not participate in the original decision to deny. Mahaska County must provide or deny access in accordance with the determination of the reviewing official.
4. If Mahaska County denies access, in whole or in part, to PHI, Mahaska County must comply with the following requirements:
   a. Mahaska County must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which Mahaska County denied access.
   b. Mahaska County must provide a timely, written denial to the individual, in plain language and containing:
      i. The basis for the denial;
      ii. If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights; and
      iii. A description of how the individual may make a formal complaint to Mahaska County.
5. If the individual has requested a review of a denial, Mahaska County must:
   a. designate or appoint a licensed Mahaska County health care professional by the committee, who was not been directly involved in the decision to deny access.
   b. Mahaska County must promptly refer a request for review to a licensed health care professional who must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards discussed above.

Mahaska County must promptly provide written notice to the individual of the findings of the committee, and take other action as required by this section to carry out the licensed health care professional's determination.

Applicable Standards and Regulations:

45 C.F.R. §164.524

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version
Implementation Date:

Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-135: Amending Protected Health Information (PHI)

Purpose:

Individuals have a right to amend information collected and maintained about them in their designated record set.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and /or electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska Countyworkforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

1. Amendment of PHI

Mahaska County's workforce members, Elected Officials and volunteers shall strictly observe the following standards:

A. An individual has the right to have Mahaska County amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

B. Mahaska Countymay deny an individual's request for amendment, if it is determined that the PHI or record that is the subject of the request:

i. Was not created by Mahaska County, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

ii. Is not part of the designated record set;

iii. Would not be available for inspection under the Access and Denial of Individual Request for PHI Policy; or

iv. Is inaccurate and incomplete.

C. The individual must make the request to amend the PHI in writing with a reason to support a requested amendment. See Policy and Procedure PR-135a "Request to Amend PHI Form."

D. Mahaska County must accept all requests to amend PHI in the designated record set; however, is not required to act on the individual's request if it is in accordance with item 1(B) above.

E. Mahaska County must act on the individual's request for an amendment no later than 60 days after receipt of such a request. If Mahaska County is unable to act on the amendment within the required 60 day time limit, Mahaska County may extend the time for such action by no more than 30 days, provided that:

i. Mahaska County provides the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed; and

ii. Mahaska County may have only one such extension of time for action on a request for an amendment.

2. If the amendment is granted, in whole or in part:

A. Mahaska County must make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

B. Mahaska County must inform the individual in a timely manner that the amendment is accepted and obtain the individual's identification of an agreement to have Mahaska County notify the relevant persons with which the amendment needs to be shared.

C. Mahaska County must make reasonable efforts to inform and provide the amendment within a reasonable time, to:

i. Persons identified by the individual as having received PHI about the individual and needing the amendment; and

ii. Persons, including business associates, that Mahaska County knows have the PHI that is the subject of the amendment and that could have relied on (or could foreseeably rely on) such information to the detriment of the individual.

3. Denial of Amendment

A. If the requested amendment is denied, in whole or in part, Mahaska County must provide the individual with a timely, written denial (see Policyand Procedure PR-135c "Amendment Denial Form"). The denial must use plain language and contain:

i. The basis for the denial, in accordance with this policy;

ii. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

iii. A statement that, if the individual does not submit a statement of disagreement, the individual may request that Mahaska County provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

iv. A description of how the individual may complain to Mahaska Countyor the Secretary of the Department of Health and Human Services (HHS) in accordance with Mahaska County's Privacy Complaint Process.

B. Additionally for denials:

i. Mahaska County must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Mahaska County may reasonably limit the length of a statement of disagreement.

ii. Mahaska County may prepare a written rebuttal to the individual's statement of disagreement.

iii. Whenever such a rebuttal is prepared, a copy of the rebuttal must be provided to the individual who submitted the statement of disagreement.

iv. Mahaska County must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any, to the designated record set for future disclosures:

C. If a statement of disagreement has been submitted by the individual, Mahaska County must include the individual's request for an amendment, the denial of the request, the individual's

statement of disagreement and the rebuttal, if any, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
D. If the individual has not submitted a written statement of disagreement, Mahaska County must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.
E. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, Mahaska County may separately transmit the material required to the recipient of the standard transaction.

Procedures:

1. Amendment

   Individuals may request to have their PHI amended by submitting a "Request for Amendment of Protected Health Information" Form (Policy and Procedure PR-135a) to Mahaska County's Chief Privacy Officer (CPO).
   Administrative staff trained in these policies and procedures, in collaboration with the CPO, as necessary, have the authority to amend or correct any PHI that is determined to be a routine revision and would not require a review from a Mahaska County clinician (i.e. individual's name is spelled incorrectly on a psychosocial test or public health record).
   If an amendment request requires further investigation from a clinical staff member, the request shall be forwarded by the CPO, after his/her review, to the Elected Official or Department Head who will then consult the treating clinician (if still employed with Mahaska County).
   If still available, the treating clinician will review the record and the request and render a decision to modify or not. If the treating clinician is no longer serving with Mahaska County the Elected Official or Department Head will review the matter and make a decision to amend the record as requested by the individual in whole, in part or not at all, and notify the CPO. The CPO will document the decision and send a letter outlining the decision to the individual.

2. Amendments Received from Other Entities

   If Mahaska County is informed by another provider or payer of an amendment made to an individual's PHI within the outside entities' designated record set, Mahaska County must amend the PHI in designated record sets that have been received from those outside entities. However, Mahaska County does not have to amend the PHI in the designated record set based upon an outside determination, unless Mahaska County has relied on the outside entities' findings.

3. Enforcement

   Each person who serves as a county HIPAA Chief Privacy Officer, Chief Security Officer, Elected Official, Department Head or similar responsibilty is responsible for enforcing this policy. Individuals who violate this policy will be subject to county discipline, including termination of employment or internship.

Applicable Standards and Regulations:

45 C.F.R. §164.526

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-140: Accounting of Disclosures

Purpose:

One of the rights granted to individuals under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the right of the individual to request and receive an accounting of the disclosures of the individual's Protected Health Information (PHI) and electronic protected health information (ePHI).

The individual's right to request and receive an Accounting of Disclosures is described within Mahaska County's Notice of Privacy Practices. This policy describes what Mahaska County must to be able to provide the individual with an accurate Accounting of Disclosures.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County. This applies to any PHI that is obtained, handled, learned, heard or viewed, while in the course of work or association with Mahaska County.

All Mahaska County workforce members, Elected Officials, volunteers and persons associated with Mahaska County are responsible to be trained in Mahaska County's privacy policies and procedures for protecting the security and confidentiality of all PHI whether oral, written or electronic format.

Policy:

Mahaska County will respond appropriately to requests from individuals for an Accounting of Disclosures listing the disclosure made of their PHI by Mahaska County.

Procedures:

Individuals have the right to receive an accounting of non-electronic medical record PHI disclosures made by Mahaska County in the six years prior to the request. Mahaska County is not required to account for any disclosures that occurred prior to the compliance date of April 14, 2003. Individuals have the right to request electronic medical record PHI disclosures made by Mahaska County in the three years prior to the request.

Mahaska County must account for all disclosures of non-electronic medical record PHI, except for disclosures made for Treatment, Payment or Health Care Operations (TPHCO), pursuant to an individual authorization or as allowed without authorization under the HIPAA regulations. Mahaska County must provide the individual with a written accounting that except as otherwise provided,

must include disclosures of PHI that occurred during the six years (or shorter time period if requested) prior to the date of the request. This includes disclosures to and by business associates for purposes other than Treatment, Payment or Operations (TPO).

Mahaska County has adopted an electronic medical record as the media for capturing individual medical information. Consistent with the Health Information Technology for Economic and Clinical Health (HITECH) Act, it is Mahaska County policy to capture an audit of all events including adding or creating, editing, deleting and viewing of the electronic medical record data for a period of three years. Mahaska County will provide the accounting on the Mahaska County site for the individual. It is not the policy of Mahaska County to allow the individual to take the accounting of the disclosures from the Mahaska County facility.

Standards

1. The accounting for each non-electronic medical record disclosure must include:
    a) The date of the disclosure;
    b) The name of the entity or person who received the PHI and, if known, the address of such entity or person;
    c) A brief description of the PHI disclosed; and
    d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement a copy of a written request for a disclosure if any.
2. If Mahaska County has made multiple disclosures of non-electronic medical record PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide:
    a) The information required above;
    b) The frequency, periodicity, or number of the disclosures made during the accounting period; and
    c) The date of the last such disclosure during the accounting period.
3. For electronic medical record PHI, Mahaska County will provide the accounting as the Audit Trail data as provided in the electronic medical record system. The individual can view the Audit Trail information on the Mahaska County site. The individual will not be provided the data to take away from the Mahaska County facility.

Content for Research Disclosures (> 50 individuals)

Disclosures for research purposes must be accounted for unless an authorization has been obtained from the individual. For research disclosures involving less than 50 individuals Mahaska County must account for the disclosure in accordance with the above requirements. However, for larger research disclosures (more than 50 individuals) Mahaska County may provide a summary list of all protocols for which the individual's PHI may have been disclosed for research pursuant to a waiver of authorization.

The summary list must provide:

1. The name of the protocol or other research activity;
2. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
3. A brief description of the type of PHI that was disclosed;

4. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
5. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
6. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity. If Mahaska County provides a summary accounting for research disclosures, and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, Mahaska County shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Compliance Standards

Mahaska County must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows: i. Provide the individual with the accounting requested; or ii. If Mahaska County is unable to provide the accounting within the time required above, Mahaska County may extend the time to provide the accounting by no more than 30 days, provided that:

1. Mahaska County, within the time limit of 60 days, provides the individual with a written statement of the reasons for the delay and the date by which Mahaska County will provide the accounting; and
2. Mahaska County may have only one such extension of time for action on a request for an accounting.

Mahaska County will provide the first accounting to an individual in any 12-month period without charge. Mahaska County may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that Mahaska County informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. The fee schedule for these services is set by the State of Iowa. The fee schedule is maintained by each Department responsible for releasing PHI and/or Accounting of Disclosures.

Mahaska County personnel need to account for disclosures of non-electronic medical record PHI by documenting any such disclosures. Each Department responsible for releasing PHI will account for disclosures in release of information. Each Department responsible for releasing PHI will be responsible for receiving and processing requests for an accounting of disclosures.

Each Department responsible for releasing PHI must document and maintain a copy of the following:

1. The required information to be included in an accounting of disclosures, as outlined in the earlier section "Content Standards for the Accounting of Disclosure of PHI."
2. The written accounting that is provided to the individual requesting an accounting of disclosures.

Exceptions to the Right of Accounting of Disclosures

1. In accounting for disclosures of PHI:
    a) Mahaska County will temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official if such agency or official provides Mahaska County with a written statement that such an accounting to the

individual would be reasonably likely to impede the agency's activities. The written statement must specify the time for which such a suspension is required; and

b) If the agency or official suspends an individual's right to receive an accounting of disclosures and the statement is made orally, Mahaska County must document the statement, including the identity of the agency or official making the statement.

2. Mahaska County is not required to account for the following disclosures of non-electronic medical record PHI:
   a) To carry out TPO;
   b) To individuals requesting their own PHI;
   c) Incidental use or disclosure made during an otherwise permitted or required disclosure;
   d) Pursuant to an authorization;
   e) For persons involved in the individual's care or other notification purposes; or
   f) Disclosures not requiring an authorization as allowed by the HIPAA regulations.

Applicable Standards and Regulations:

45 C.F.R. §164.528

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-145: Communication by Alternate Means

Purpose:

The purpose of this policy is to provide guidance on how to accommodate an individual's reasonable request to have their PHI that is created or maintained within Mahaska County communicated to an alternate location or by an alternate means.

DEFINITIONS

A. Alternative Communication: A communication from provider to patient by an alternative means or at an alternative location. Examples may include using an alternate mailing address or phone number; or using an alternate communication vehicle (phone, mail or email) rather than the provider's standard method of communication.

B. Protected Health Information (PHI): Health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy applies to all Mahaska County departments that create or maintain PHI.

Policy:

Mahaska County must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from their Mahaska County by alternative means or at alternative locations.

Mahaska County may require the individual to make a request for a confidential communication in writing using the "Patient Consent for Health Information to be Communication by Alternative Means" form (see Policy and Procedure PR-145b.)

Conditions on Providing Confidential Communications:

1. Mahaska County may require the individual to make a request for a confidential communication described in paragraph (1) of this policy in writing.
2. Mahaska County may condition the provision of a reasonable accommodation on:
    - A. When appropriate, information as to how payment, if any, will be handled; and
    - B. Specification of an alternative address or other method of contact.
3. Mahaska County may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

Mahaska County may condition the provision of a reasonable accommodation on:

1. When appropriate, information as to how payment, if any, will be handled.

Procedure:

Patients may request that they receive communications of PHI by alternative means or at alternative locations at the time of visit, or at any time during the course of their care.

Patient requests to receive communications of PHI by alternative means or at alternative locations must be made in writing using the "Patient Consent for Health Information to be Communication by Alternative Means" form. The Chief Privacy Officer (CPO) or their designee will make decisions about reasonableness of the request.

A. All patient requests should be forwarded to the CPO at Mahaska County for a decision. The CPO may deny a request for alternative confidential communications only if:
    1. The request is unreasonable from an administrative standpoint and/or;
    2. The patient does not provide an alternative address or other method of contact.
B. Reasonableness of a request from an administrative standpoint may vary. Mahaska County may not require that the patient provide a reason for their request.
C. Mahaska County will not deny requests based on its perception of whether the patient has a good reason for making the request. A patient's reason for making a request cannot be used to determine whether the request is reasonable.
D. If Mahaska County grants a patient's request, it will inform appropriate staff of the alternative communication requirements and will require staff to adhere to them.
E. An alternative communication request that is implemented remains in place until it is revoked by the patient or until such time as Mahaska County determines that it no longer meets the administrative reasonableness criteria. Revocation or denial of an implemented request will be communicated to provider and patient and documented in the patient record.
F. Each patient will be informed in writing whether his/her request has been approved or denied and, if approved, that all future communications initiated by Mahaska County will be made in this manner. (Exception: if it is necessary to communicate urgently with the patient, staff may use any available address or phone number.)
G. An alternative communication request that is implemented remains in place until it is revoked by the patient or until such time as Mahaska County determines that it no longer meets the administrative reasonableness criteria. Revocation or denial of an implemented request will be communicated to provider and patient and documented in the patient record.
H. Each patient will be informed in writing whether his/her request has been approved or denied and, if approved, that all future communications initiated by Mahaska County will be made in this manner. (Exception: if it is necessary to communicate urgently with the patient, staff may use any available address or phone number.)

DOCUMENTATION REQUIREMENTS

If Mahaska County grants a patient's request, the decision will be documented by maintaining a written or electronic record of the actions taken for a period of six (6) years.

A contemporaneous log of Requests for Confidential Communications via Alternate Forms will be maintained (see Policy and Procedure PR-145a). Patient written request for alternative communication, and the organization's response will be maintained in the medical record.

Applicable Standards and Regulations:

45 CFR 164.522(b) (HIPAA Privacy Rule)
45 CFR 164.510 (HIPAA Privacy Rule)
45 CFR 164.502(h) (HIPAA Privacy Rule)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-150: Breach Notification Policy and Procedures

Purpose:

To provide guidance for breach notification by covered entities when impermissible or unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

It is Mahaska County's policy to ensure that electronic and hardcopy PHI is secured from unauthorized disclosure. In the event that a possible unauthorized notification has occurred (as defined in Policy/Procedure AS-180 "What Constitutes a Breach of PHI") Mahaska County will provide the proper notification to the required parties. It is the policy, wherever practical, for any one communication of ePHI to be for less than 500 individuals at any one transfer of data.

Procedures:

Mahaska County will perform the procedure below:

1. Mahaska County will gather and document the following information for each disclosure:
   - A brief description of the breach including what occurred, the date of the breach and the date of discovering the breach;
   - A description of the types of unsecured PHI involved in the breach;
   - A description of the steps that Mahaska County is taking to investigate the breach:
   - A description of the steps that the individuals subject to the breach can take to protect themselves from potential harm; and

- Contact procedures for individuals to contact Mahaska County to ask questions or learn additional information. Mahaska County will establish a toll-free telephone number, an email address, a page on its web site and its postal address for individuals to contact Mahaska County.

2. Mahaska County will promptly, but no more than 60 days from discovery of the breach, notify each affected individual of the breach:
   - Mahaska County will notify all affected individuals using first class mail at their last known address or through email if the individual has agreed to receive electronic notice via email;
   - If the individual is deceased, Mahaska County will notify the individual's next of kin or personal representative;
   - In the event the individual does not have sufficient contact information, Mahaska County will provide substitute notice, such substitute notice be comprised of other written notice or telephone notification;
   - In the event there are more than 10 individuals for whom there is insufficient contact information, notification will be prominently posted on the Mahaska County web site or in print or broadcast media. If the notification is posted on the Mahaska County website, the posting will reside on the website for no less than 90 days.

3. For breaches of less than 500 individuals, Mahaska County will maintain a log of these breaches and submit this log to the Secretary of Health and Human Services on an annual basis;

4. For breaches of more than 500 individuals, Mahaska County will immediately notify the Secretary of Health and Human Services; and

5. For breaches affecting more than 500 individuals residing on any one state, Mahaska County will notify prominent media outlets serving the state.

Applicable Standards and Regulations:

45 C.F.R. §164.400

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-155: Patient Authorization

Purpose:

To outline the required content of a patient authorization for use or disclosure of protected health information (PHI).

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

To ensure the privacy of patient health information, Mahaska County obtains a valid patient authorization for uses and disclosures of health information that are not otherwise required or permitted by law.

In general, any use or disclosure of PHI/ePHI will be limited to the minimum amount of information necessary to carry out the purpose of the use or disclosure.

Procedures:

A. Requirements of a valid authorization (see Policy and Procedure PR-155a "Authorization for Use or Disclosure of Health Information"). To be valid, an authorization must be written in plain language and contain:

1. A meaningful description of the health information to be used or disclosed;
2. A description of each purpose of the use or disclosure in question;
3. The name or specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
4. The name or specific identification of the person(s) or class of persons to whom the use or disclosure may be made;
5. An expiration date or event;
6. A statement of the patient's right to revoke the authorization in writing and the limitations on that right;
7. A description of how the patient may revoke the authorization;
8. A statement acknowledging that the health information disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer protected by Mahaska County's privacy practices;

9. A statement of Mahaska County's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and
10. Signature of the patient or the patient's legal representative and the date signed. The signature of a legal representative must be accompanied by a description of the representative's authority to act for the patient.

B. Invalid authorizations. An authorization is invalid if any of the following occur:
1. The expiration date or event has passed;
2. The authorization lacks any of the required elements; See section A above.
3. The authorization contains missing required information;
4. The authorization contains information that Mahaska County knows to be false;
5. The authorization is known by Mahaska County to have been revoked; or
6. The authorization is of a type prohibited by law.

C. Documentation requirements
1. If the organization obtains the authorization, Mahaska County must provide the patient with a copy of the signed authorization.
2. Mahaska County must document and maintain all patient authorizations for a period of at least six years, or in accordance with state law, whichever is longer.

Applicable Standards and Regulations:

45 CFR §164.312(c)(2)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-160: Uses and Disclosures of PHI to Family and Friends

Purpose:

Mahaska County is committed to protecting individual privacy and to disclosing individual PHI in accordance with the individual's desires. However, when the individual's desires are not known or have not been expressed, it may be necessary to disclose an individual's PHI to a member of the individual's family, a friend of the individual, or someone else who is directly involved in the individual's care. It may also be necessary to disclose a limited amount of the individual's PHI in order to locate the individual (for example, in case the individual elopes) or to locate or notify a member of the individual's family or a friend of the individual. This Policy describes the procedures for releasing and limitations surrounding the release of an individual's PHI to someone directly involved in the individual's care or for location or notification purposes.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County. Violation of this policy may result in disciplinary action up to and including termination for employees; a termination of employment relationship in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals may be subject to loss of access privileges and civil and/or criminal prosecution.

Policy:

Mahaska County may disclose an individual's PHI to a member of the individual's family, a friend of the individual, or to another individual if the family member, friend, or other individual is directly involved in the individual's care and the disclosure is necessary for the individual's welfare.

Mahaska County will limit the PHI disclosed to the family member, friend, or other individual to health-related signs and symptoms and to information designed to help the individual deal with his/her illness or treatment, including setting and changing appointments, receiving instructions for post-visit care, or picking up treatment-related items.

Mahaska County may also disclose a limited amount of the individual's PHI in order to locate the individual or to locate or notify the individual's family member or friend.

Procedures:

Mahaska County requires individual authorization to disclose PHI to the individual's family or friends. However, Mahaska County may use and disclose certain PHI to the individual's family and/or friends without written individual authorization, under certain circumstances. When possible, the individual must be informed in advance of the use or disclosure and have the opportunity to agree, prohibit, or restrict the disclosure. Mahaska County may orally inform the individual of the permitted uses and disclosures and obtain the individual's agreement or objection to a use or disclosure permitted by this policy. Mahaska County staff responsible for releasing PHI must document the agreement, prohibition, or restriction in the medical record.

Uses and Disclosures to Family or Friends without Authorization for Involvement in the Individual's Care and Notification Purposes:

Mahaska County may disclose to a family member, other relative, a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. Mahaska County may use or disclose PHI to notify or to assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Mahaska County can also use and disclose PHI in these circumstances for identifying or locating the types of persons mentioned above. In order for Mahaska County to use or disclose PHI for these purposes, the individual's presence is a determining factor.

The following processes outline how Mahaska County may use and disclose PHI for these purposes.

Uses and Disclosures with the Individual Present:

If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, Mahaska County may use or disclose the PHI if Mahaska County:

1. Obtains the individual's verbal consent, reflected by documentation in the medical record;
2. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to such disclosure.

Limited Uses and Disclosures when the Individual is not present:

If the individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, Mahaska County may exercise professional judgment to determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. Mahaska County may use professional judgment in

allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies or other healthcare items containing PHI.

Applicable Standards and Regulations:

45 C.F.R. §164.510(b)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-165: Use and Disclosure of PHI for Fundraising

Purpose:

The purpose of the policy is to ensure that any fundraising activities that occur under the auspices of Mahaska County comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the fundraising procedures and guidelines created by Mahaska County.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy includes all fundraising activities that take place within any department of Mahaska County and applies to all Mahaska County and Business Associates engaged in fundraising activities on behalf of Mahaska County. Compliance with this policy is the responsibility of all Mahaska County workforce members, Elected Officials and volunteers.

Policy:

In general, an individual's PHI may not be used for fundraising purposes without specific authorization from the individual or representative. Any fundraising efforts will be communicated in clear and concise wording allowing potential recipients to opt out of receiving the fundraising communication regardless of any prior authorizations.

Procedures:

Fundraising personnel may only use and disclose dates of treatment and demographic information in connection with fundraising activities unless they obtain specific authorization from an individual granting more expansive use of the individual's PHI. Demographic information generally includes name, address, other contact information, age, gender and insurance status.

Information about the department in which an individual received services, also cannot be used for fundraising purposes without the individual's prior authorization, if that information would reveal or could reveal the nature of the diagnosis, services or treatment that the individual received.

With individual's prior authorization, Mahaska County personnel and affiliated fundraising associates may:

1. Use an individual's basic demographic information to solicit gifts;
2. Access individuals' dates of care;
3. Use public information outside its internal database to send fundraising requests, without fear of violating this policy; and
4. Mahaska County personnel and affiliated fundraising associates MUST:
    a. Provide a "Notice of Privacy Practices" to any individuals they may be planning to contact. Individuals may receive a Notice of Privacy Practices (NPP) while at Mahaska County, by

visiting the Mahaska County website, or by calling Mahaska County and requesting to mail the information to the member;

b. Include an opt-out provision along with the initial fundraising letter sent describing how individuals may opt out of receiving further fundraising materials;
c. Exclude information about diagnosis, nature of services, or treatment in any solicitation;
d. Remove that individual's information immediately from the mailing list upon receipt of an opt out clause;
e. Sign an appropriate business associate contract before disclosing individual information to consultants or outside entities for fundraising activities. This contract is not necessary should Mahaska County employees or an institutionally related foundation perform the fundraising, which includes nonprofit foundations that raise only a portion of funds for Mahaska County.

After Notice of Privacy Practices is sent, information that CAN be used for fundraising without authorization or consent includes:

Name
Address
Other contact information (such as email, phone etc.)
Age
Gender
Insurance status
Date of service

Information that CANNOT be used without authorization:

Diagnosis
Nature of services
Treatment
Place within hospital where individual receives treatment that specifically identifies that treatment, such as:

- Department of Psychiatry
- Department of Obstetrics
- Department of Radiation Oncology

Information about a part of Mahaska County where treatment occurred may be used to filter names for fundraising as long as the department does not identify the type or nature of treatment. Caution should be used when divulging the matter of hospital area treatment.

When a prospective contributor voluntarily discloses information about diagnosis and treatment to a member of Mahaska County's fundraising staff, that information can then be used for other fundraising purposes.

Applicable Standards and Regulations:

45 C.F.R. §164.514(f)(1)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-180: Use and Disclosure of PHI for Research

Purpose:

There may be instances where a Mahaska County is involved with research. This policy is to ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's personal health information (PHI) or electronic protected health information (ePHI) in relation to research.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County protects the confidentiality and integrity of PHI as required by law. The use and disclosure of PHI in research must have the appropriate authorizations and safeguards in place. The review process shall make all determinations regarding the applicable federal and state privacy standards as it applies to the use and disclosure of PHI for research. As a result, all personnel must strictly observe the following standards relating to the use and disclosure of PHI for research.

Procedures:

Approval of Research:

In order to provide for the adequate discharge of the responsibility, no research activity may be undertaken by any Mahaska County staff unless approved by the Chief Privacy Officer (CPO).

Use of De-Identified Information and Limited Data Sets:

Whenever possible, de-identified PHI should be used. De-identified PHI is rendered anonymous when identifying characteristics are completely removed with reasonable expectation that the data can be used to re-identify the individual. De-identified PHI may only be used and disclosed in accordance with the appropriate Mahaska County policy. If PHI cannot be de-identified the next step should be to use a limited data set in accordance with Use and Disclosure of Limited Data Sets. Only when both de-identified PHI and a limited data set are inadequate can PHI be used for research.

Applicable Standards and Regulations:

45 C.F.R. §164.512(i)

Distribution:

Policy Distribution
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-185: Use and Disclosure of Psychotherapy Notes

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to requests for psychotherapy notes.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County may not release psychotherapy notes, except in specific situations or as required by law.

Authorization for the disclosure of psychotherapy notes is not required in the following circumstances:

1. For purposes of the Department of Health and Human Services in determining compliance with the privacy rule;
2. By a health oversight agency for a lawful purpose related to oversight of a psychotherapist;
3. To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law;
4. To law enforcement in instances of permissible disclosure related to a serious or imminent threat to the health or safety of a person or the public; or
5. As otherwise required by law.

Procedures:

Psychotherapy notes (i.e., process notes) shall be maintained separately from the medical record. An individual does not have a right to inspect or obtain a copy of psychotherapy notes. An individual may not request a review of an originator's denial of access to psychotherapy notes. However, an individual may be provided access to a summary of the treatment.

Applicable Standards and Regulations:

45 C.F.R.§164.508

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-190: Use and Disclosure of PHI for Judicial or Administrative Proceedings

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to judicial and administrative proceedings.

There may be instances where an individual is involved with a legal proceeding, either conducted by a court of law (such as a state trial court or federal district court) or a government agency of the State of Iowa Department of Health and Family Services, the State of Iowa Department of Workforce Development, or the federal Centers for Medicare and Medicaid Services.

In these legal proceedings, lawyers, judges and others involved with the proceeding may contact Mahaska County to access the individual's PHI. Examples of health information these proceedings may require include information about a certain medical procedure the individual underwent to determine whether the procedure is covered under a health plan or the outcome of that procedure, results of blood or genetic tests in child custody or similar proceedings, medical records that document disabling conditions in discrimination cases, or health information that documents serious illnesses for conflicts pertaining to medical leave.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the individual or a valid authorization has been obtained. However, PHI may be used or disclosed for judicial or administrative proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request or other lawful process. Each department can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Definitions

Disclosure**:** the release, transfer, provision of access to or divulgence in any other manner of information to any organization external to Mahaska County.

Use**:** with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Mahaska County.
Qualified protective order: with respect to PHI requested under this section, an order of court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceedings that:

1. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
2. Requires the return to Mahaska County or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Procedures:

Permitted disclosures

Mahaska County may use or disclose PHI in the course of any judicial or administrative proceedings if:

1) The disclosure is in response to an order of a court or administrative tribunal, provided that Mahaska County discloses only the PHI expressly authorized by such order; or
2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal (such as a subpoena from the Iowa Department of Health and Human Services), if:
   A. Mahaska County receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request (with an affidavit from the requesting party); or
   B. Mahaska County receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of this section (in Definitions above).
3) Mahaska County receives satisfactory assurances from a party seeking PHI along with a written statement and accompanying documentation demonstrating that:
   A. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
   B. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
   C. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objections were filed; or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
4) Mahaska County receives satisfactory assurances from a party seeking PHI including a written statement and accompanying documentation demonstrating that:
   A. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

B. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

Notwithstanding this section, Mahaska County has the option to disclose PHI in response to lawful process without receiving full satisfactory assurance, if Mahaska County of its own accord makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this section or to seek a qualified protective order.

Mahaska County may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

Applicable Standards and Regulations:

45 C.F.R. §164.512(e)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-195: Use and Disclosure of PHI for Specialized Government Functions

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to specialized government functions.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County workforce members, Elected Officials and volunteers may not disseminate PHI/ePHI without authorization, unless requested by the individual or a valid authorization has been obtained. However, PHI/ePHI may be used or disclosed without authorization for specialized government functions.

Mahaska County's Chief Privacy Officer (CPO) should be contacted for verification of individuals representing a specialized government agency. Each department can handle these releases of information with approval of the CPO. All requests of this type should be routed to the CPO. These specialized government functions include:

1. Armed Forces personnel, the Red Cross, or other authorized agents of the Armed Forces, if deemed necessary by appropriate military command;
2. Authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities;
3. Authorized federal officials for the provision of protecting the President or foreign heads of state;
4. The Department of State to make medical suitability determinations;
5. A correctional institution or a law enforcement official with lawful custody of an inmate if necessary for the health and safety of such individual, other inmates, officers or other employees at the correctional institution; and
6. Governmental programs providing public health benefits and governmental agencies administering such programs. For example: the testing of an individual for communicable diseases, as authorized by state criminal law, and by state agencies; or intervention programs administered by state agencies.

Procedures:

Military and veteran's activities

1. Mahaska County may use and disclose the PHI of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command.

2. Mahaska County may use and disclose the PHI of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the same guidelines that apply to US Armed Forces.

National security and intelligence activities

Mahaska County may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by law.

Correctional institutions and other law enforcement custodial situations

1. Mahaska County may disclose PHI to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual PHI, if the institution or official represents that such PHI is necessary for:
   A. The provision of health care to such individuals;
   B. The health and safety of such individual or other inmates;
   C. The health and safety of the officers or employees of or others at correctional institution;
   D. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
   E. Law enforcement on the premises of the correctional institution; and
   F. The administration and maintenance of the safety, security, and good order of the correctional institution.
2. Any component of Mahaska County that is affiliated with a correctional institution may use PHI of individuals who are inmates for any purpose for which such PHI may be disclosed.
3. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

Departments or components of Mahaska County that are or may become government programs providing public benefits

1. Any Mahaska County health plan that is a government program providing public benefits may disclose PHI to another agency either to enroll or determine individual eligibility. Such health plan may do so if the sharing of PHI information is required or authorized by statute.
2. Any Mahaska County department administering a government (state or federal) program providing public benefits may disclose PHI to another covered entity that is a like agency as long as the programs serve the same or similar populations and the disclosure of PHI is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

Applicable Standards and Regulations:

45 C.F.R. §164.512(k)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

James Blomgren		

PR-200: Use and Disclosure for Disaster Relief Purposes

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose a patient's protected health information (PHI) and electronic protected health information (ePHI) in relation to requests for disaster relief purposes.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purposes of coordinating with such entities. Each department can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Procedures:

Mahaska County may use or disclose PHI for disaster relief if the CPO considers the need for the use or disclosure to be critical to supporting the disaster relief effort.

Applicable Standards and Regulations:

45 C.F.R. §164.512(k)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-205: Use and Disclosure of PHI for Health Oversight Reporting

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose a member's protected health information (PHI) and electronic protected health information (ePHI) in relation to Health Oversight Reporting activities.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the member or a valid authorization has been obtained. However, Mahaska County may disclose PHI without an authorization to a health oversight agency for oversight activities authorized by law, including audits, civil, administrative or criminal investigations, inspections, licensure or disciplinary actions, civil, administrative, or criminal proceedings or actions, or other activities necessary for appropriate oversight of:

1. The health care system;
2. Government benefit programs for which health information is relevant to beneficiary eligibility;
3. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
4. Entities subject to civil rights laws for which health information is necessary for determining compliance.

Each department can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Procedures:

Disclosures to Department of Health and Human Services

PHI may be disclosed to the Secretary of the Department of Health and Human Services in their role of enforcing the Privacy Rules.

Joint activities or investigations

If a health oversight activity or investigation is related to a claim for public benefits not related to health, the joint activity or investigation shall be considered a health oversight activity for purposes of this policy.

Disclosures by whistleblowers

All Mahaska County personnel are strongly encouraged to report conduct that is unlawful or otherwise violates professional or clinical standard to the CPO. Mahaska County is not considered to have violated the requirements of this policy if a member of its workforce or a business associate discloses PHI, provided that:

1. The workforce member or business associate believes in good faith that Mahaska County has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or

that the care, services, or conditions provided by Mahaska County potentially endangers one or more members, workers, or the public; and

2. The disclosure is to:
   A. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Mahaska County;
   B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Mahaska County; or
   C. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

Disclosures by Mahaska County personnel who are victims of a crime

Mahaska County is not considered to have violated the requirements of this policy, with just cause, if a member of its workforce who is the victim of a criminal act discloses PHI of the suspected perpetrator to a law enforcement official, provided that:

1. The PHI disclosed is about the suspected perpetrator of the criminal act; and
2. The PHI disclosed is limited to:
   a. Name and address;
   b. Date and place of birth;
   c. Social security number;
   d. ABO blood type and Rh factor;
   e. Type of injury;
   f. Date and time of treatment;
   g. Date and time of death, if applicable; and
   h. Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

Exception to health oversight activities

The following scenario is NOT to be considered health oversight activity:

1. The individual is the subject of the investigation or activity and the investigation or other activity is not directly related to:
   a) The receipt of health care;
   b) A claim for public benefits related to health (e.g. claims for Food Stamps); or
   c) Qualification for, or receipt of, public benefits or services when a member's health is integral to the claim for public benefits or services.

Applicable Standards and Regulations:

45 C.F.R. §164.512(d)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

James Blomgren		

PR-220: Use and Disclosure of PHI for Law Enforcement Agencies

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) or electronic protected health information (ePHI) in relation to requests from law enforcement agencies.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the member or a valid authorization has been obtained. However, PHI may be used or disclosed for law enforcement agencies if the use or disclosure is made in response to a lawful process. Each department will handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Definitions

Disclosure**:** the release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to Mahaska County.

Use**:** with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within Mahaska County.

Procedures:

Permitted disclosures

Mahaska County will disclose PHI to authorized law enforcement agencies under the following conditions:

1. The information requested is relevant, material, specific and limited to the amount reasonably necessary and de-identified information is not sufficient;
2. The information is needed to identify or locate a suspect, fugitive or material witness or missing person only as approved by the person authorized to act on behalf of the individual;
3. The information is about a suspected victim of a crime if the individual agrees to the disclosure;

4. The information is about a deceased individual if Mahaska County has reason to suspect that the death resulted from criminal conduct and the disclosure is approved by individuals authorized to act on behalf of the deceased individual;
5. The information that Mahaska County reasonably believes constitutes evidence of criminal conduct occurring on Mahaska County's premises;
6. The information relates to an emergency situation as required by law such as test results on those involved in an automobile accident; or
7. The information is critical to Mahaska County's reasonable assessment of the safety of the individual.

Applicable Standards and Regulations:

45 C.F.R. §164.512(c)
45 C.F.R. §164.512(f)
45 C.F.R. §164.512(j)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-225: Permitted Use and Disclosure for Emergency Treatment

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to emergency treatment.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the individual or a valid authorization has been obtained or it is disclosed without authorization for public Health or safety. Each can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO. Mahaska County may disclose PHI for the purposes of emergency treatment without authorization:

1. For reporting child abuse, or neglect;
2. To avert a serious and imminent threat to the health or safety of a person or the public; or
3. To law enforcement officials for law enforcement purposes and when allowed by law.

Procedures:

Required by Law

Mahaska County personnel may use or disclose PHI to the extent that such use or disclosure that meets the "minimum necessary" requirement to provide emergency medical treatment.

Permitted Disclosures for Abuse or Neglect

1. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
2. If the individual agrees to the disclosure; or
3. To the extent the disclosure is expressly authorized by statute or regulation and:
   A. Mahaska County, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
   B. If the individual is unable to agree because of incapacity, a law enforcement or other public official may authorize to receive the report if:
      i. the PHI sought is not intended to be used against the individual; and

ii. an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Informing the individual

In making a permitted disclosure, Mahaska County personnel must promptly inform the individual that such a report has been or will be made, except if:

1. Mahaska County believes informing the individual would place the individual at risk of serious harm; or
2. Mahaska County would be informing a personal representative, and Mahaska County reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by Mahaska County.

Serious Threat to the Health or Safety of the Public Permitted disclosures

Mahaska County may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if Mahaska County, in good faith believes the use or disclosure:

1. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
2. In the course of treatment which is designed to alter or change the desire to commit the criminal conduct which would be the basis for making a disclosure, or when an individual initiates or is referred to Mahaska County for treatment, counseling, or therapy: or
3. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

Limitations and Good Faith related to the Serious Threat

Mahaska County may only release the statement relating to the serious threat and the PHI related to the serious threat. If Mahaska County acts in good faith upon its belief, then Mahaska County will be protected for disclosures related to the serious threat.

Victims of a Crime

Mahaska County may disclose PHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to this section, if:

1. The individual agrees to the disclosure; or
2. Mahaska County is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

   A. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

   B. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

C. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Reporting Crime in Emergencies

A Mahaska County health care provider providing emergency health care in response to a medical emergency, other than such emergency on Mahaska County premises, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

1. The commission and nature of a crime;
2. The location of such crime or of the victim(s) of such crime; and
3. The identity, description, and location of the perpetrator of such crime.

If a Mahaska County health care provider believes that the medical emergency described in the above paragraph of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph above of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to the section on abuse, neglect, or domestic violence at the beginning of this policy.

Applicable Standards and Regulations:

45 C.F.R. §164.501
45 C.F.R. §164.512(b)
45 C.F.R. §164.512(c)
45 C.F.R. §164.512(f)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-230: Use and Disclosure of PHI for Deceased Individuals

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to requests about deceased individuals.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the patient or a valid authorization has been obtained. However, two exceptions to the general policy exist after a patient has expired. These exceptions are:

1. PHI may be used or disclosed to coroners, medical examiners, or funeral directors, and
2. PHI may also be used or disclosed for organ procurement purposes, to organ procurement organizations or similar entities. Although no authorization is required, these disclosures must be tracked.

Each Department responsible for these releases can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Procedures:

Coroners and medical examiners

Mahaska County may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

Funeral directors

Mahaska County may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, Mahaska County may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

Organ Procurement

Mahaska County may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Applicable Standards and Regulations:

45 C.F.R. §164.512(g)
45 C.F.R. §164.512(h)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-235: Use and Disclosure of PHI for Worker's Compensation

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) or electronic protected health information (ePHI) related to Workers' Compensation.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI which is available currently or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process.

Policy:

As a general rule, Mahaska County workforce members, Elected Officials and volunteers may not disseminate PHI without authorization, unless requested by the member or a valid authorization has been obtained. However, PHI may be used or disclosed for Worker's Compensation proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request, or other lawful process. Each department can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Definitions

Disclosure**:** the release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to Mahaska County.

Use: with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within Mahaska County.

Qualified protective order**:** with respect to PHI requested under this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceedings that:

3. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
4. Requires the return to Mahaska County or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

Procedures:

Permitted disclosures

Mahaska County may use or disclose PHI/ePHI in the course of any Workers' Compensation proceeding if:

1. The disclosure is in response to an order of a court or administrative tribunal, provided that Mahaska County discloses only the PHI/ePHI expressly authorized by such order.

2. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal (such as a subpoena from the State of Iowa's Department of Health), if:
   A. Mahaska County receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request (with an affidavit from the requesting party); or
   B. Mahaska County receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of this section (in Definitions above).
3. Mahaska County receives satisfactory assurances from a party seeking PHI along with a written statement and documentation demonstrating that:
   A. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
   B. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
   C. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
      1. No objections were filed; or
      2. All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
4. Mahaska County receives satisfactory assurances from a party seeking PHI/ePHI including a written statement and documentation demonstrating that the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
5. Notwithstanding this section, Mahaska County has the option to disclose PHI/ePHI in response to lawful process without receiving full satisfactory assurance, if Mahaska County of its own accord makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this section or to seek a qualified protective order
6. Mahaska County may disclose PHI/ePHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

Applicable Standards and Regulations:

45 CFR §164.512(l)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

James Blomgren		

PR-240: Use and Disclosure of PHI for Public Health and Safety

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose a patient's protected health information (PHI) and electronic protected health information (ePHI) in relation to requests for Public Health and Safety.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is available currently or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County. All Department Heads and Elected Officials are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process.

Policy:

As a general rule, Mahaska County workforce members, Elected Officials and volunteers may not disseminate PHI/ePHI, without authorization, unless requested by the patient or a valid authorization has been obtained. Mahaska County may disclose PHI/ePHI without authorization for Public Health or Safety. Each department can handle these releases of information with approval of the Chief Privacy Officer (CPO). All requests of this type should be routed to the CPO.

Mahaska County may disclose PHI for public health or safety without a patient authorization:

4. For reporting child abuse, or neglect;
5. To avert a serious and imminent threat to the health or safety of a person or the public; or
6. For law enforcement purposes to law enforcement officials and when allowed by law.

Procedures:

Required by Law

Mahaska County workforce members, Elected Officials and volunteers may use or disclose PHI/ePHI to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

Mahaska County workforce members, Elected Officials and volunteers must meet the requirements pertaining to disclosures relating to victims of abuse or neglect, disclosures for judicial and administrative proceedings and disclosures for law enforcement purposes.

Permitted Disclosures for Abuse or Neglect

1. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
2. If the individual agrees to the disclosure; or

3. To the extent the disclosure is expressly authorized by statute or regulation and:
   A. Mahaska County, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
   B. If the individual is unable to agree because of incapacity, a law enforcement or other public official may authorize to receive the report if:
      i. Mahaska County the PHI sought is not intended to be used against the individual; and
      ii. Mahaska County an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

Informing the individual

In making a permitted disclosure, Mahaska County workforce members, Elected Officials and volunteers must promptly inform the individual that such a report has been or will be made, except if:

3. Mahaska County believes informing the individual would place the individual at risk of serious harm; or
   Mahaska County would be informing a personal representative, and Mahaska County reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by Mahaska County.

Serious Threat to the Health or Safety of the Public Permitted disclosures

Mahaska County may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if:

1. Mahaska County, in good faith believes the use or disclosure:
   4. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; except a use and disclosure may not be made if the information is learned by Mahaska County;
   5. In the course of treatment which is designed to alter or change the desire to commit the criminal conduct which would be the basis for making a disclosure, or when an individual initiates or is referred to Mahaska County for treatment, counseling, or therapy; or
   6. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
2. It is necessary for law enforcement authorities to identify or apprehend an individual:
   A. Mahaska County Because of a statement by an individual admitting participation in a violent crime; or
   B. Mahaska County Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

Limitations and Good Faith related to the Serious Threat

Mahaska County may only release the statement relating to the serious threat and the PHI related to the serious threat. If Mahaska County acts in good faith upon its belief, then Mahaska County will be protected for disclosures related to the serious threat.

Law Enforcement Purposes

Mahaska County may disclose PHI/ePHI pursuant to a court order or subpoena with the approval of the CPO the disclosure complies with and is limited to the relevant requirements:

1. As required by law, including laws that require the reporting of certain types of wounds or other physical injuries, except for laws pertaining to public health;
2. In compliance with and as limited by the relevant requirements of:
   A. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
   B. A grand jury subpoena; or
   C. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
      i. The information sought is relevant and material to a legitimate law enforcement inquiry;
      ii. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
      iii. De-identified information could not reasonably be used.

Identification and Location Purposes

Mahaska County may disclose PHI in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that Mahaska County only discloses the following information:

A. Name and address;
B. Date and place of birth;
C. Social security number;
D. ABO blood type and Rh factor;
E. Type of injury;
F. Date and time of treatment;
G. Date and time of death, if applicable; and
H. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

Except as permitted in the paragraph above, Mahaska County may not disclose for the purposes of identification or location under that paragraph of this section any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

Victims of a Crime

Mahaska County may disclose PHI/ePHI in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to this section, if:

1. The individual agrees to the disclosure; or
2. Mahaska County is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

A. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
B. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
C. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Deceased Individuals
Mahaska County will disclose PHI/ePHI about a deceased individual to law enforcement officials for the purpose of alerting law enforcement of the death of the individual if Mahaska County has a suspicion that such death may have resulted from criminal conduct.

Crime on Premises
Mahaska County may disclose to a law enforcement official PHI/ePHI that Mahaska County believes in good faith constitutes evidence of criminal conduct that occurred on Mahaska County premises.

Reporting Crime in Emergencies
1. A Mahaska County health care provider providing emergency health care in response to a medical emergency, other than such emergency on Mahaska County premises, may disclose PHI/ePHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
   A. The commission and nature of a crime;
   B. The location of such crime or of the victim(s) of such crime; and
   C. The identity, description, and location of the perpetrator of such crime.
2. If a Mahaska County health care provider believes that the medical emergency described in the above paragraph of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph above of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to the policy on abuse, neglect or domestic violence at the beginning of this policy.

Applicable Standards and Regulations:

45 CFR §164.501
45 CFR §164.512(f)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version

Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-245: Use and Disclosure of PHI to Coroners, Funeral Directors and Organ Procurement Organizations

Purpose:

To ensure that Mahaska County workforce members, Elected Officials and volunteers understand when and how to disclose an individual's protected health information (PHI) and electronic protected health information (ePHI) in relation to requests for organ procurement.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all Mahaska County workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

As a general rule, Mahaska County personnel may not disseminate PHI without authorization, unless requested by the individual or a valid authorization has been obtained. However, two exceptions to the general policy exist after a member has expired. These exceptions are:

3. PHI may be used or disclosed to coroners, medical examiners, or funeral directors, and
4. PHI may also be used or disclosed for organ procurement purposes, to organ procurement organizations or similar entities. Although no authorization is required, these disclosures must be tracked and directed to the Chief Privacy Officer (CPO).

Each Department can handle these releases of information with approval of the CPO. All requests of this type should be routed to the CPO.

Procedures:

Coroners and medical examiners

Mahaska County may disclose PHI/ePHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

Funeral directors

Mahaska County may disclose PHI/ePHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, Mahaska County may disclose the PHI/ePHI prior to, and in reasonable anticipation of, the individual's death.

Organ Procurement

Mahaska County may use or disclose PHI/ePHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Applicable Standards and Regulations:

45 C.F.R. §164.512(g)
45 C.F.R. §164.512(h)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-250: De-Identification of Protected Health Information (PHI)

Purpose:

Mahaska County has adopted this procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations as well as acknowledge our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All workforce members, Elected Officials, and volunteers of Mahaska County must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every workforce member's responsibilities.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) or electronic protected health information (ePHI) for any purpose. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials, and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County. All Department Heads and Elected Officials are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process.

Policy:

Mahaska County has a duty to protect the confidentiality and integrity of PHI as required by law, professional ethics, and accreditation requirements. Whenever possible, de-identified PHI should be used. De-identified PHI is rendered anonymous when identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. This policy defines the guidelines and procedures that must be followed for the de-identification of PHI/ePHI.

Procedures:

All workforce members, Elected Officials, and volunteers must strictly observe the following standards relating to the de-identification of PHI:
De-identification requires the elimination not only of primary or obvious identifiers, such as the member's name, address, date of birth (DOB), and treating physician, but also of secondary identifiers through which a user could deduce the member's identity. For information to be de-identified the following identifiers of the individual (or of relatives, employers, or household member of the individual) must be removed:

1. Names
2. Address information
3. Names of relatives and employers
4. All elements of dates (except year), including DOB, admission date, discharge date, date of death
5. Telephone numbers
6. Fax numbers
7. Email addresses

8. Social Security Number (SSN)
9. Medical Record Number
10. Health beneficiary plan number
11. Account numbers
12. Certificate/License Number
13. Vehicle identifiers, including license plate numbers
14. Device ID and serial number
15. Uniform Resource Locator (URL)
16. Identifier Protocol (IP) addresses
17. Biometric identifiers
18. Full face photographic images and other comparable images, any other unique identifying number characteristic, or code

Whenever possible, de-identified PHI should be used for quality, peer review monitoring, utilization reporting and committee activities. If de-identified PHI cannot be used, a limited data set should be used whenever possible.

PHI used for research, including public health research, should be de-identified at the point of data collection for research protocols approved by the Chief Privacy Officer (CPO), unless the participant voluntarily and expressly consents to the use of his/her personally identifiable information or a waiver of authorization is obtained. If de-identified PHI cannot be used, a limited data set should be used whenever possible.

If an authorized user wishes to encrypt PHI when creating de-identified information, the authorized user must ensure that:

1. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
2. Anyone involved in the research project does not use or disclose the code or other means of record identification and does not disclose the mechanism to accomplish re-identification.

If removal of any identifiers is not practical or does not meet Mahaska County's needs, approval from the CPO must be obtained if the PHI is used.

Applicable Standards and Regulations:

45 C.F.R. §164.502(d)
45 C.F.R. §164.514(b)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-255: Employee Use of Social Media

Purpose:

Mahaska County accepts the value of social media (defined in this policy) in maintaining communications with members, other providers and vendors. However, Mahaska County also understands that there are significant risks associated with the use of social media. Based on this, it is the policy of Mahaska County to restrict the use of social media using Mahaska County servers and internet access by employees and contractors to only those approved by Mahaska County management.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

It is also the policy of Mahaska County for workforce members, Elected Officials, volunteers and contractors not to disclose any information regarding Mahaska County, its management and employees, policies and operations, or health care processes through their personal use of social media outside Mahaska County without prior approval of Mahaska County management.

Mahaska County will undertake training programs for all employees to ensure that workforce members, Elected Officials, volunteers and contractors be trained in the Mahaska County social media policies and the risks of using social media to Mahaska County and the workforce members, Elected Officials, volunteers or contractors.

Mahaska County discourages Mahaska County workforce members, Elected Officials, volunteers or contractors from using social media tools as a means for communicating with individuals.

Mahaska County reserves the right to monitor, prohibit, restrict, block, suspend, terminate or discontinue the use of any Mahaska County social media activity without notice and for any reason at its sole discretion.

Any social media content representing or referring to Mahaska County, workforce members, Elected Officials, volunteers, vendors and/or its contractors, its operations and practices, its policies and procedures, its members is the property of Mahaska County.

Mahaska County does not endorse people, products, services or organizations on social media web sites.

Definitions of Social Media

Social media platforms are comprised of the technology tools and online spaces for integrating and sharing user-generated content to engage constituencies in conversations and allow them to participate in content and community creation. Examples are Facebook, Twitter, LinkedIn and YouTube. If there are any questions as to whether the service the employee or contractor is using is social media, please refer to the Mahaska County Chief Security Officer for approval.

Content Owners are those assigned the responsibility of creating, maintaining, monitoring and moderating any social media content regarding Mahaska County, its management and employees, its policies and operations, its health care processes and individuals, whether using the Mahaska County platform or a personal platform.

Procedures:

1. Content Owner responsibilities:
    a. Before a workforce member, Elected Official, volunteer or contractor can create, maintain, monitor or moderate social media content regarding Mahaska County, using either the Mahaska County platform or their personal platform, the employee or contractor must obtain approval for the social media posting from the Mahaska County Chief Security Officer (CSO).
    b. To receive approval, the Content Owner must provide to the Chief Security Officer the following information: the social media tools to be used, the purpose of the social media effort, how it will help Mahaska County, how the Content Owner will mitigate risks to Mahaska County and the Content Owner, a draft of the content and how the content will be maintained and monitored to ensure the social media use conforms to Mahaska County policies and procedures.

2. Social media content will not include any reference to Mahaska County workforce members, Elected Officials, volunteers or contractor information, any Mahaska County client or client information or any information in conflict with Mahaska County HIPAA privacy and security policies, and will not constitute a conflict of interest, violate any copyrights, reveal any proprietary financial, intellectual property or other similar data.

3. Social media content will not violate local, state or federal laws or regulations nor include any content that is unlawful, disruptive, threatening, profane, abusive, harassing, embarrassing, tortuous, defamatory, ethnically or racially hateful, obscene, transmit any information that Mahaska County does not have the right to transmit, promote any “junk mail,” “spam,” “chain letters,” “pyramid schemes” or any other form of solicitation, libel or an invasion of another’s privacy.

4. Social media content related to Mahaska County will be respectful of individuals and their rights and will positively present the Mahaska County professional image and reputation.

5. Mahaska County employees or contractors will not participate in online forums where any Mahaska County proprietary information as described in this policy is discussed without prior approval from the Mahaska County Chief Security Officer (CSO).

6. The Content Owner should take care not to endorse people, products, services or organizations with regard to the Content Owner's affiliation with Mahaska County in the social media postings.

7. Workforce members, Elected Officials, volunteers or contractors will immediately contact the Mahaska County Chief Privacy Officer (CPO) if the workforce member, Elected Official, volunteer or contractor is made aware of social media content that violates this policy, whether posted by an employee or contractor or other party.

8. Whether on the Mahaska County or personal platform, when creating, maintaining monitoring or moderating a social media posting in which Mahaska County, or its employees, management, contractors or members are mentioned, the Content Owner must identify his/her affiliation with Mahaska County and be clear as who the Content Owner is speaking.

9. Violation of these policies is inappropriate and may result in applicable disciplinary action as described in the Mahaska County policies and procedures.

Applicable Standards and Regulations:

45 C.F.R. §164.502(a)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-260: Use of Mobile Devices

Purpose:

This policy establishes guidelines for secure use of mobile devices and protection of any electronic protected health information (ePHI) stored on mobile devices.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

This Policy applies to the use of all types of mobile devices that may be used to store ePHI. Mobile devices may include, but are not limited to, laptops, smartphones, other types of wireless handheld devices, USB flash drives, memory sticks, and any other portable devices used to store or transport data.

Procedures:

It is Mahaska County policy, where possible, to not store ePHI on mobile devices.

If it is necessary to store ePHI on mobile devices:

1. Password protect the device using a complex password;
2. Encrypt the ePHI stored on the device, using county provided encryption software; and
3. Store only the minimum necessary ePHI if the purpose of storing the ePHI is not for treatment, payment or healthcare operations.

When it is no longer necessary to store the ePHI on the device:

1. If the device will continue in use, delete the ePHI and empty the recycle bin or trashcan;
2. If the device will continue in use, but none of the data stored on the device will be needed again, use a disk wiping tool to remove all traces of all data stored on the device; or
3. If neither the device nor the data stored on the device will be used again, the device must be disposed of according to Mahaska County policy.

Authorization to Use Mobile Devices:

No Mobile Device may be used for any purpose or activity involving information subject to this Policy without prior registration of the device and written authorization by the Chief Security Officer (CSO).

Authorization will be given only for use of mobile devices which the CSO has confirmed have been configured so that it complies with this policy. Authorization must be requested in writing.

Access to, obtaining, use and disclosure of information subject to this policy by a mobile device, and any use of a mobile device in any Mahaska County facility or office, including an authorized home office or remote site, must be in compliance with all Mahaska County policies at all times.

Authorization to use a Mobile Device may be suspended at any time:

1. If the User fails or refuses to comply with this Policy;
2. In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
3. In connection with the investigation of a possible or proven security breach, security incident, or violation of Mahaska County's policies;
4. In order to protect individual life, health, privacy, reputational or financial interests;
5. In order to protect any assets, information, reputational or financial interests of Mahaska County; or
6. Upon the direction of the supervising staff and/or department management or CSO.

Authorization to use a Mobile Device terminates:

1. Automatically upon the termination of a User's status as a member of Mahaska County's workforce;
2. Upon a change in the User's role as a member of the Mahaska County's workforce, unless continued authorization is requested by the supervising staff and/or department management; or
3. If it is determined that the User violated this or any other Mahaska County policy, in accordance with Mahaska County's policies.

The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.

Audit of Mobile Devices:

Upon request by the Chief Security Officer, at its sole discretion at any time, any Mobile Device may be subject to audit to ensure compliance with this and other Mahaska County policies. Any User receiving such a request shall transfer possession of the Mobile Device to the Chief Security Officer at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.

Mobile Device User Responsibilities:

Information subject to this Policy which is stored on the Mobile Device must be encrypted as provided in Mahaska County's policies. Information subject to this Policy should not be stored on the Mobile Device for any period longer than necessary for the purpose for which it is stored.

In addition to other requirements and prohibitions of this and other Mahaska County policies, Mobile Device Users have the following responsibilities:

1. A Mobile Device may not be shared at any time when unencrypted information subject to this Policy is stored on the device.
2. A Mobile Device which does not have unencrypted information subject to this Policy stored on it may be shared temporarily, provided that:
    a. The User may not share the password or PIN number used to access the Mobile Device, but must open access for shared use him- or herself.
    b. The configuration of the device to comply with this Policy must not be changed.
    c. The individual using the device must not further share it; must protect it against being misplaced, lost or stolen, and must immediately report to the User if it is; and must return it promptly to the authorized user when finished with the temporary use.
    d. The individual using the device must not use it to process, use or disclose information subject to this Policy.
3. Access to each Mobile Device must be controlled by a password or PIN number consistent with Mahaska County's policy. Password or PINs must be changed periodically as provided in Mahaska County's policy. The Mobile Device must provide for a maximum of three (3) attempts to enter the password or PIN correctly.
4. The timeout for access to the Mobile Devices must be a maximum of two (2) minutes.
5. Information subject to this Policy which is transmitted wirelessly by the Mobile Device must be encrypted unless an exception is authorized. Exceptions must be authorized by the Chief Security Officer.
6. If possible, Mobile Devices must have antivirus software. Mobile Devices which cannot support antivirus software may be subject to limitations on use at the discretion of the Chief Security Officer, as specified in writing by the Chief Security Officer.
7. Physical protection for Mobile Devices must be provided as required by Mahaska County's policy.
8. If the Mobile Device is misplaced, stolen or believed to be compromised this must be immediately reported to Chief Security Officer.
9. Applications and services installed on the Mobile Device must be approved by the Chief Security Officer.
10. Bluetooth and infrared (IR) services must be configured as approved by the Chief Security Officer or turned off.
11. Mobile Devices must be disposed of according to Mahaska County policy.

<u>Personal Use of Mobile Devices:</u>
Personal Use of Mobile Devices owned or leased and provided by Mahaska County are subject to the Mahaska County Acceptable Use Policy.

Personal use of personally-owned Mobile Devices must at all times be consistent with this Policy.

All information on a Mobile Device, including personal information about or entered by the User, may be subject to audit or evidentiary review as provided in this Policy. Any such personal information may be used or disclosed by Mahaska County to the extent it deems reasonably necessary:

1. In order to avoid, prevent or mitigate the consequences of a violation of this Policy;

2. In connection with the investigation of a possible or proven security breach, security incident, or violation of Mahaska County policies;
3. In order to protect the life, health, privacy, reputational or financial interests of any individual;
4. To protect any assets, information, reputational or financial interests of Mahaska County;
5. For purposes of determining sanctions against the User or any other member of the Mahaska County Workforce;
6. If Required by Law.

Prohibited Uses of Mobile Devices:

The following uses of Mobile Devices are prohibited:

1. The storage of information subject to this Policy, including voice messages, voice notes, email, instant messages, web pages and electronic documents, photographs, images and videos, unless they are encrypted.
2. The Internet or wireless transmission or upload of information subject to this Policy, including voice messages, voice notes, email, instant messages, web pages and electronic documents, photographs, images and videos, without encryption, unless previously authorized in writing by the Chief Security Officer.
3. The creation of any photograph, image, video, voice or other recording of any individual who is a patient or member of the Workforce of Mahaska County, except in compliance with Mahaska County policy.
4. The creation of any photograph, image, video, voice or other recording of any document, record, computer or device screen which includes information subject to this Policy, except in compliance with Mahaska County policy.

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PR-265: Consent for Treatment, Payment and Healthcare Operations

Purpose:

This policy establishes guidelines for the use and disclosure of health information by Mahaska County Covered Entities, in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and State law.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is available currently, or which may be created, used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

As a provider with a Direct Treatment Relationship with our patients, Mahaska County has the option of requesting a patient to sign a consent form to use their Protected Health Information (PHI) for treatment, payment or Mahaska County health care operations. As a matter of Mahaska County policy, the Mahaska County HIPAA Committee has set as Mahaska County policy that Mahaska County will not request the consent. In addition, as a matter of Mahaska County HIPAA policy and in consideration to the wide range of cultures that we serve, Mahaska County is advising our patients in the Mahaska County Notice of Privacy Practices that Mahaska County may find it necessary to use interpreters to ensure the best medical care Mahaska County can provide to our patients.
It is also Mahaska County' policy that Mahaska County will not require individuals to waive their rights under the HIPAA laws and regulations as a condition of the provision of treatment, payment or eligibility for benefits.

Procedures:

Applicable Standards and Regulations:

45 C.F.R. §164.512(e)
45 C.F.R. §164.530(h)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

PR-270: Monitoring of PHI Disclosures by Business Associates

Purpose:

Consistent with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) laws and rules, Mahaska County requires that all business associates promptly notify Mahaska County if there are any unauthorized disclosures of protected health information (PHI) and electronic protected health information (ePHI).

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purpose. This policy covers all PHI/ePHI which is a person's identifiable health information. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall treat any breaches of the disclosure rules by a business associate to be the same as a breach of disclosure by Mahaska County with the applicable tracking of breaches. In the event of a breach of disclosure rules by a business associate, Mahaska County will notify the business associate of its responsibilities to mitigate any damages resulting from the breach disclosure and will monitor the business associate's activities to ensure the cause of the breach is remedied.

Procedures:

Chief Security Officer (CSO) will:

Make an initial entry noting the current date, the date of notification, the nature of the suspected breach, current status of the suspected breach, and steps reportedly taken to deal with the breach into the spreadsheet provided in Mahaska County's Policy/Procedure AS-185a "Tracking Breach Incident Log" (or enter into HIPAA Suite Incident Tracking section of software).

With the business associate, Mahaska County's CSO will conduct a breach assessment, as described in Mahaska County's Policy/Procedure AS-180 "What Constitutes a Breach of PHI?" to determine if a breach has actually occurred;

If the assessment concludes that a breach has not occurred, Mahaska County's CSO will make a closing entry in Mahaska County's Tracking Breach Incident Log noting the current date and an attestation that no such breach actually occurred;

If the assessment concludes that a breach has occurred, the CSO and its business associate will conduct the breach tracking and resolution process, as described in Policy/Procedure AS-180 “What Constitutes a Breach of PHI?”

Applicable Standards and Regulations:

45 CFR § 164.410

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

Physical Standards

PS-105: Disposal of ePHI and/or Hardware

Purpose:

Mahaska County will ensure the privacy and security of protected health information (PHI) in the maintenance, retention and eventual destruction and disposal of such media. Destruction and disposal of protected health information will be carried out in accordance with federal and state law, and as defined in the Mahaska County disposal policy. The schedule for destruction and disposal shall be suspended for records involved in any open investigation, audit or litigation.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

All electronic devices (including computers, cell phones, printers, cameras, routers, etc.), and all electronic storage devices and storage media (including fixed and removable disk drives, hard drives, optical storage disks, flash drives, etc.) used to store ePHI or information enabling county security features or access to the county's information center shall be assessed by the Mahaska County's Chief Security Officer (CSO) and/or designated IT personnel and sanitized of such data to the extent necessary to render its recovery infeasible prior to the donation, sale, disposal or destruction of such devices or media. The CSO shall also oversee the removal of such information as well as subsequent testing of the devices or media to ensure and certify in a contemporaneous log that no ePHI can feasibly be recovered before each item is sold, donated, disposed of or destroyed.

Procedures:

All storage devices and media are to be given to Mahaska County's CSO for disposal. Storage devices and media may be disposed of only by the CSO or workforce member authorized by the CSO. Prior to donation, sale or disposal, the criticality of ePHI contained in electronic devices or storage media will be assessed by the CSO and/or designated IT personnel and then sanitized using methods informed by current guidance provided by the National Institute of Standards and Technology (NIST).

The CSO will refer to NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1 (December 2014) or later, as contained in Mahaska County's HIPAA Master Manual.
Additional precautions will be taken when donating, selling or disposing of electronic devices or media such as computers, cell phones and storage drives including removal of all data and software

installed or maintained in addition to ePHI or security programs and information used to access the system.

Devices or media that have been sanitized and are intended for donation, sale or disposal shall be quarantined and tagged “DO NOT USE” to preclude inadvertent reintroduction of ePHI.
The CSO will maintain a contemporaneous log of all computer equipment and storage media that have been disposed of. A certificate suitable for this purpose may be found in Appendix G of NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1 (December 2014) or later, as contained in Mahaska County’s HIPAA Master Manual. At a minimum, log entries will include the description of equipment or storage media, the CSO’s risk assessment for each item, sanitization method used, the name and address of any vendor used to accomplish sanitization or destruction of such items, the results of any verification test, and the dates of withdrawal from service and donation, sale or disposal.

The log will be maintained for inspection and reference a minimum of six years from the last date of entry.

Applicable Standards and Regulations:

45 C.F.R §164.310(d)(2)(i)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-115: Receipt and Removal of Hardware Containing ePHI

Purpose:

This policy reflects Mahaska County's commitment to appropriately control information systems and electronic media containing electronic protected health information (ePHI) moving into, out of and within its facilities.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (ePHI) for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County will assure the appropriate receipt and removal of hardware and ePHI into and out of a facility, and the movement of these items within a facility.

Procedures:

Mahaska County has implemented the following procedure:

1. The Mahaska County IT department maintains and keeps current an electronic record of the movements of hardware and electronic media and any person responsible therefore:
   - The IT department maintains an Excel Spreadsheet of all computers, monitors, scanners and printers and where they are located in all Mahaska County facilities
   - The IT department has recorded corresponding serial numbers on all computers, monitors, scanners and printers to match the Excel Spreadsheet documentation
   - The IT department is the only department authorized to move computers, monitors, scanners and printers from one department/location to another
   - When computers, monitors, scanners or printers are moved from one location to another, the IT Department appropriately updates the Excel Spreadsheet

2. The Mahaska County IT department creates a retrievable, exact copy of ePHI, when needed, before the movement of equipment;
   - The IT department utilizes the daily Data Backup and Storage procedures to ensure that an exact copy of ePHI is made before the movement of equipment

3. The IT department records the final disposition of ePHI and/or the hardware or electronic media on which it is stored;

- The IT department records the final disposition of ePHI on the Excel Spreadsheet
- Outdated equipment is disposed of by the maintenance department and media (hard-drives, floppy disks) are drilled or smashed to not be used again

4. The IT department has procedures for removal of electronic protected health information from electronic media before the media are made available for re-use
   - The IT department deletes any and all data on a media storage prior to reusing the media
   - The media is completely reformatted for reuse

Applicable Standards and Regulations:

45 C.F.R §164.310(d)(2)(i)

Distribution:

Policy Distribution:
Specific Location(s): County Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-120: Facility Access Controls

Purpose:

It is the policy of Mahaska County to establish and maintain facility access controls as a security standard for all work locations. This can be accomplished through the implementation of policies and procedures for granting, denying and monitoring the physical access of workforce members, Elected Officials, volunteers, business associates, vendors and other individuals to facilities where confidential or protected health information (PHI) and/or electronic protected health information (ePHI) may be accessed.

Responsible for Implementation:

Chief Security Officer

Scope:

All Elected Officials and Department Heads are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable Mahaska County disciplinary process.

Policy:

Mahaska County will implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.

Mahaska County will implement policies and procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Mahaska County will implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).

Procedures:

Mahaska County has implemented the following procedure:

1. Distribution of keys to the facilities is limited to those workforce members, Elected Officials and volunteers that require such access.
2. The CSO will designate the individual/department that will document repairs to the facilities and note how these repairs impact the security plan and operations and ensure repairs are documented.

Applicable Standards and Regulations:

45 C.F.R.§164.310(a)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-125: Access Controls and Validation Procedures - Facilities

Purpose:

It is the policy of Mahaska County to establish and maintain facility access controls as a security standard for all work locations. This can be accomplished through the implementation of policies and procedures for granting, denying and monitoring the physical access of workforce members, business associates and other individuals to facilities where confidential or sensitive electronic information, including protected health information (PHI) and electronic protected health information (ePHI), may be accessed.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose PHI/ePHI for any purposes. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

All components of Mahaska County's information system are housed in secure locations. Visitors to Mahaska County's office are accompanied by a workforce member when in a position to access the county's information resources. Consultants and contractors responsible for installing, maintaining, or testing computer equipment and software are authorized to access Mahaska County's information systems as if they were staff members authorized to perform similar tasks or functions.

Procedures:

Components of Mahaska County's information system other than workstations are located in secure, locked areas or cabinets. Only designated individuals authorized to use or service that equipment have keys to secure areas.

Visitors to the county are not left alone except in public waiting areas. Visitors should not be left alone in areas in which they may be able to access the county's information system. Contractors and maintenance personnel who are not county employees sign the visitor's log but need not be accompanied by a staff member at all times when performing work covered by a business associate or other service agreement containing a confidentiality and non-disclosure clause.

Contractors and maintenance personnel are given a unique user ID and password so that Mahaska County can monitor their access to the county's information resources. Before a user ID is activated, the CSO or IT Director reviews with the contractor the county's security policies and procedures and the provisions of the business associate agreement related to security.

Applicable Standards and Regulations:

45 C.F.R §164.310(a)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): County Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-130: Facility Security Plan

Purpose:

To safeguard the confidentiality, integrity, and availability of protected health information (PHI) and/or electronic protected health information (ePHI), business, and proprietary information within Mahaska County's information systems/applications by controlling access to the physical buildings/facilities that house these systems/applications in accordance to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule 45 CFR §164.310(a)(2)(ii) and its implementation specifications.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes.. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

It is Mahaska County's policy that all computer equipment and devices that are used to access, transmit or store hard copy protected health information PHI/ePHI shall be protected from unauthorized physical access, tampering and theft. Physical access to all of Mahaska County's facilities is limited to only those authorized in this policy. In an effort to safeguard PHI, facilities and systems/applications from unauthorized access, tampering, and theft, access is allowed to designated areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members, Elected Officials and volunteers are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Mahaska County's facilities to areas containing information systems/applications.

Procedures:

1. Security of County Information Systems and Storage Devices

Network servers and central storage devices, if any, will be housed in a secure location that cannot be accessed by visitors to the practice. Computers and workstations shall be secured with theft-deterrent hardware. Displays will be positioned or blocked to preclude casual unauthorized viewing by visitors and those without a need to know.

When not in use, laptops and tablets, and storage devices should be secured in a locked storage unit designated for such purposes. Equipment closets, offices or vehicles (in the case of devices used during off-site) shall be locked at all times when such locations or devices are not occupied or in use.

Backup storage devices and media will be rotated through the practice facility and an off-site location on a father-grandfather basis to maximize the potential for timely recovery of PHI and essential

business data. On-site backup storage devices and media (1st generation grandfather data) will be maintained in a locked designated storage unit when not in use and off-site backup devices and media (2nd generation father data) will be maintained in an off-site fire and water resistant combination vault when not in use. Additionally, Mahaska County's information system and back up storage devices containing ePHI and hardcopy records containing ePHI shall be maintained under double lock and key when not attended to preclude unauthorized access and to guard against total data loss in the event of a system failure or natural disaster.

Technology advancements and increased availability of technologies to the public will be periodically assessed to determine whether they pose a threat to data security.

The Chief Security Officer (CSO) will implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft, and to control and validate a person's access to facilities based on their role or function, including visitor control. Policies and procedures will be implemented to document repairs and modifications to the physical components of county facilities that are related to security (for example, hardware, walls, doors and locks).

2. Security of Office Facilities
Mahaska County's offices, file cabinets, information system components, backup storage devices and storage units containing hard copy PHI or ePHI will be maintained in a locked manner at any time access is not required and otherwise not attended by authorized staff.
Mahaska County's office locks will be changed when staff members who have been issued keys subsequently leave the county and anytime issued keys are lost.
Mahaska County's CSO will monitor repairs and changes to the facility(s) for any impact on the security plan and operations and will advise the county's senior most management accordingly.

A workforce member shall be immediately present anytime a vendor or business associate is permitted access to Mahaska County's facilities, information systems or data storage devices and an alternate procedure has not been established by the CSO and included as an Appendix in of Mahaska County's HIPAA Master Manual.

Applicable Standards and Regulations:

45 CFR §164.310(a)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

Darin Hite		

PS-135: Workstation Use and Security

Purpose:

All Mahaska County workforce members, Elected Officials, volunteers and associates utilizing Mahaska County's information system must follow workstation use guidelines established to maintain the security of its workstations, information system and the protected health information (PHI) and electronic protected health information (ePHI) created and/or stored or transmitted by Mahaska County.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

It is the objective of Mahaska County to assure that all workstations are used and secured in a consistent manner. This document delineates the workstation functions to be performed and the manner in which a workstation is to be secured. These policies and procedures are required so that all workforce members, Elected Officials and volunteers will understand the manner in which workstations are to be used to maximize the security of confidential or sensitive electronic information, including ePHI.

Procedures:

Mahaska County's guidelines on workstation use are as follows:

1. All Workstations

Each user must log off all workstations rather than leaving them unattended. This includes workstations in private offices. Screens should be positioned within workstations so that they are visible only to the persons who use them. View limiting devices such as polarized screens that limit the useful view of a screen display to a narrow forward view should be used when the screen cannot be turned away from unauthorized individuals to maintain privacy.

2. Workstations Located in Private Offices

A workstation in a case management or public health office is an example of this type of workstation. These workstations may be used to access all individual information, including both clinical and billing information. Administrative functions related to computer security may also be performed at these workstations. However, workforce members should not access individual information when unauthorized individuals can view the information displayed on a screen.

3. Workstations Located in Common but Non-Public Areas

A workstation, laptop or tablet temporarily located at an off-site workstation or client's home during a case management session are examples of this type of workstation. These workstations may be used to access all individual information, including both clinical information and billing information. Workforce members should not access individual information when unauthorized individuals can

view the information displayed on a screen. Workstations in these settings should not be used to perform administrative functions related to security, such as adjusting settings to enable access to programs or data.

4. System Management Workstations

A workstation in an office housing a network server or storage is an example of this type of workstation. These workstations may be used to access all individual information, including both clinical information and billing information. However, individual information should be accessed from these workstations only when necessary to perform maintenance on, or to troubleshoot, the information system.

5. Workstation Anti-Theft and Recovery

Portable workstations, including laptops, tablets, and smart phones must remain in close physical proximity of the user within eyesight, or be stored out of view in a secure location such as one's automobile until workforce can continuously monitor the status of the device.

All county devices, containing private non-public or ePHI, will be encrypted and protected by complex passwords. Additionally, each computer, laptop, tablet and smart phone will be equipped with software that permits the remote location of lost or stolen devices and also allows for the remote retrieval or destruction of critical data.

Workforce members who become aware that a device is misplaced, lost or stolen shall report such information immediately to the county's Chief Security Officer (CSO) or designated Supervisor at once. Once notified of the theft, misplacement, or loss of a county device, the Supervisor will become personally responsible to notify the CSO of the occurrence or suspected occurrence without delay. Failure to report such information without delay may result in disciplinary action, including termination.

6. Personal Devices

Workforce members, Elected Officials or volunteers may not utilize personal workstations, laptops, tablet or cell phones to create, modify, store, retrieve or disseminate either individual ePHI (including individual schedule information) or proprietary county data. In the event that a personal device which might contain ePHI or propriety county data is determined to be misplaced, lost, or stolen the reporting and retrieval process shall be the same as specified above regarding Workstation Anti-theft and Recovery.

Applicable Standards and Regulations:

45 CFR §164.310(b)

45 C.F.R §164.310(c)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-140: Access Control and Validation

Purpose:

All components of Mahaska County's information system shall be housed in secure locations. Visitors shall be accompanied by a staff member when in a position to access the Mahaska County's information system and backup storage devices or hardcopy files. Consultants and contractors responsible for installing, maintaining, or testing computer equipment and software may by authorized to access the county's information systems as if they were staff members without the requirement for a Mahaska County workforce member to be present provided a written agreement specifying the nature of the authorization has been completed prior to such work. Otherwise, a Mahaska County workforce member shall be present during periods when such individuals are allowed within the facility in areas where access to Mahaska County's information system, data storage devices, protected health information (PHI), electronic protected health information (ePHI) and sensitive county data may be gained.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County must control and validate physical access to its areas that have information systems containing ePHI or software programs that can access ePHI. All physical access rights to such areas must be clearly defined and documented, with access provided only to Mahaska County workforce members who have a need for specific access of the ePHI in order to accomplish a legitimate task. Additionally, such access rights must define specific roles or functions and the physical access rights associated with each. All physical access to Mahaska County areas that have information systems containing ePHI or software programs that can access ePHI must be tracked and logged.

Procedures:

Components of Mahaska County's information system other than workstations will be located in secure, locked areas or cabinets. Only workforce members, Elected Officials and volunteers authorized to access or service such equipment will be issued keys to secure areas where information system components are stored or are in use.

Visitors to the county should not be left alone in areas where PHI may be accessed via Mahaska County's information system. IT contractors and facility maintenance personnel who are not staff

members will sign a visitor's log but need not be accompanied by a workforce member except when entering or exiting the facility when performing work covered by a business associate or other service agreement.

IT contractors will be given a unique user ID and password so that Mahaska County's Chief Security Officer (CSO) can monitor their access to Mahaska County's information resources. Before a user ID is activated, the CSO will review with the contractor the individual's security policies and procedures and the provisions of the business associate agreement related to security and exposure to PHI or essential business data. This review shall be logged, including the date of training, topic(s) reviewed, results of any tests, signatures of the person(s) serving as instructor/reviewer and the person(s) receiving the instruction/review, and a statement by the instructor/reviewer indicating that the review was satisfactorily completed and the person receiving the instruction/review is authorized to access Mahaska Countys information resources.

If the instruction/review is deemed less than satisfactory, the instruction/review shall merely be logged as such and no statement authorizing access shall be made. Any authorization made will be limited to a maximum of six (6) months without completing a relevant summary review, considering how often the IT contractor will have an occasion to engage Mahaska County's HIPAA and HITECH processes regarding identification of PHI/ePHI and other sensitive county data, the requirement for confidentiality, proper reporting of confirmed or suspected breaches of rules disclosure, and steps to mitigate the risk of additional breach of rules of disclosure. Access shall only be provided for a maximum of six (6) months at a time but may be of a shorter duration, if the CSO or trainer/reviewer deems otherwise.

A contemporaneous summary list of persons granted or denied access shall be maintained by the CSO. The list shall also provide for tracking the rescission or expiration of access granted for any reason (e.g., routine expiration, resignation, end of internship, end of business associate agreement, dismissal from employment, disciplinary sanction, etc.)
Both the training log and access summary list shall be maintained for six (6) years from the latest closing entry in the case of training/reviews and the latest date of entry summarizing access status in the case of managing current access status.

Applicable Standards and Regulations:

45 CFR §164.310(a)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

Darin Hite		

PS-143: Remote Access Policy

Purpose:

The purpose of this policy is to establish uniform security requirements for all authorized users who require remote electronic access to Mahaska County's network and information assets. The guidelines set forth in this policy are designed to minimize exposure to damages that may result from unauthorized use of Mahaska County's resources and confidential information.

Responsible for Implementation:

Chief Security Officer

Scope:

All users who work outside of the county's environment, who connect to the county's network systems, applications and data, including but not limited to applications that contain electronic protected health information (ePHI), from a remote location.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

This policy applies to all authorized system users, including workforce members, Elected Officials, volunteers, business associates, and vendors, desiring remote connectivity to Mahaska County's networks, systems, applications, and data. Users are frequently categorized in one of these user groups:

1. Workforce members with permanent remote access. These users may include Information Services (IS), executive, or specific administrative staff, business staff, or workers who may require 24-hour system availability or are called upon to work remotely. Their remote access offers the same level of file, folder and application access as their on-site access.
2. Workforce members with temporary remote access. These users typically request short-term remote access due to an extended time away from the office most frequently as a result of a short-term medical or family leave. Access for these users will be restricted to only that which is necessary for task completion during time away from the office and may be limited.
3. Contractors and Vendors offering product support with no access to PHI. These users have varied access depending upon the systems needed for application or system support, but do not have access to any PHI in the applications or systems. These users access the system on an as needed, or as called upon basis for system troubleshooting.
4. Contractors and Vendors offering product support and other Business Associates with access to PHI. These users have varied access to PHI depending on the application or system supported and/or accessed. Appropriate Business Associate Agreements must be on file prior to allowing access, and all such access must be audited on a regular basis.

Policy:

To establish guidelines and define standards for remote access to Mahaska County's information resources (networks, systems, applications, and data including but not limited to, ePHI received, created, maintained or transmitted by the county). Remote access is a privilege, and is granted only to remote users who have a defined need for such access, and who demonstrate compliance with Mahaska County's established safeguards which protect the confidentiality, integrity, and availability of information resources.

Procedures:

1. Gaining Remote Access

A. Workforce members shall apply for remote access connections through their immediate manager. Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member's manager, and with approval by the Chief Security Officer (CSO).

B. The workforce member is responsible for adhering to all of Mahaska County's policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Mahaska County.

C. Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with Mahaska County which clearly defines the type of remote access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors with a defined business need, at the discretion of and approval by the CSO.

D. It is the remote access user's responsibility to ensure that the remote worksite meets security and configuration standards established by Mahaska County. This includes configuration of personal routers and wireless networks

2. Equipment, Software, and Hardware

A. The county will not provide all equipment or supplies necessary to ensure proper protection of information to which the user has access. The following assists in defining the equipment and environment required.

(i) User Provided:
(a) Broadband connection and fees
(b) Paper shredder
(c) Secure office environment isolated from visitors and family
(d) A lockable file cabinet or safe to secure documents when unattended

B. Remote users will be allowed access through the use of equipment owned by or leased to the entity, or through the use of the workforce member's personal computer system provided it meets the minimum standards developed by Mahaska County, as indicated above.

C. Remote users utilizing personal equipment, software, and hardware are:

(i) Responsible for remote access. Mahaska County will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
(ii) Responsible for remote access used to connect to the network and meeting Mahaska County requirements for remote access
(iii) Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to Mahaska County.

D. Continued service and support of Mahaska County owned equipment is completed by IT workforce members. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Mahaska County to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Mahaska County.
E. The ability to print a document to a remote printer is not supported without the county's approval. Documents that contain confidential business or ePHI shall be managed in accordance with the Mahaska County's confidentiality and information security practices.

3. Security and Privacy

A. Only authorized remote access users are permitted remote access to any of Mahaska County's computer systems, computer networks, and/or information, and must adhere to all of Mahaska County's policies.
B. It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Mahaska County's network when access is no longer needed to perform job responsibilities.
C. Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or the county's confidential and/or sensitive information.
D. Remote access users are automatically disconnected from the Mahaska County's network when there is no recognized activity for 15 minutes.
E. It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.
F. Remote access users must take necessary precautions to secure all of Mahaska County's equipment and proprietary information in their possession.
G. Virus Protection software is installed on all Mahaska County's computers and is set to update the virus pattern routinely. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may not stop the update process for Virus Protection, on county's or the remote user's workstation.
H. Copying of confidential information, including ePHI, to personal media (hard drive, USB, CD/DVD, etc.) is strictly prohibited, unless the county has granted prior approval in writing.
I. Mahaska County maintains logs of all activities performed by remote access users while connected to Mahaska County's network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 30 days will be disabled.
J. Electronic Data Security

i) Backup procedures have been established that moves data to external media. If there is not a backup procedure established or if Mahaska County has external media that is not encrypted, contact the IS Department or Security Officer for assistance.
(ii) Transferring data to the Mahaska County network requires the use of an encrypted connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to the Mahaska County's network.

K. Paper document security
(i) Remote users are discouraged from using or printing paper documents that contain PHI.
(ii) Documents containing PHI must be shredded before disposal consistent with the policy and procedure "Use of PHI" (PR-115).

4. Enforcement
A. Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with Mahaska County's termination policy.
B. Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Mahaska County's network, and liability for any damage to property and equipment.

Applicable Standards and Regulations:

45 CFR §164.312(a)(2)(iii)
45 CFR §164.308(a)(3)(ii)(B)
45 CFR §164.308(a)(3)(ii)(C)
45 CFR §164.308(a)(4)(ii)(B)
45 CFR §164.308(a)(4)(ii)(C)

Distribution:

Policy Distribution:
Specific Location(s): County Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-150: Media Reuse

Purpose:

To implement policies and procedures governing the receipt, movement, and removal of hardware, software, and electronic media that contain electronic Protected Health Information (ePHI) into, out of, and within Mahaska County's facilities. This policy relates to disposition and reuse of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of media and storage devices.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Data storage devices, such as hard drives, and storage media containing, including removable disks, rewritable CD-ROMs, and back-up tapes, shall be "sanitized" before reuse.

Procedures:

Data storage media (e.g. solid state drives, CD's, etc.) or storage devices (e.g., hard drives) may be reused provided:

A. The data contained can be transferred, does not serve a backup function, or is deemed obsolete;

B. The data sectors of such media or devices in question are sanitized utilizing the guidance provided in by NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1 (December2014); and

C. The media or devices are thoroughly scanned for damage and malware, no such damage or malware exists and the media or devices are operationally checked utilizing a suitable device completely isolated from Mahaska County's information system so as to preclude any risk a damaged or infected media or devices might pose to the county's information system, PHI/ePHI or essential business and disaster recovery data.

Media or devices that cannot be sanitized, scanned for damage and malware, and cannot be operationally checked shall be tagged unusable and must quarantined from all useable media and devices until such time as such deficiencies are corrected or the media and devices are destroyed or

disposed of utilizing the guidance provided in by NIST Special Publication 800-88, Guidelines for Media Sanitization, Revision 1 (December2014).

The CSO or his/her IT designee shall tag unusable data storage media or devices and maintain a contemporaneous log of each event. Log entries must include:

A. The date and time of determination;
B. The name of the person making the determination;
C. A description of the item, including make, model and serial number or other distinguishing county marks/identification;
D. The nature of the problem;
E. The disposition of the data storage media or device (e.g., to repair/repaired, to destroy/destroyed, to dispose of/disposed of, etc.); and
F. The location of the media or device (e.g., on site, repair vendor, licensed disposal service, etc.).

Note:
If the media or device has been repaired or cleared of malware and operationally checked using dummy data to assure functionality and data integrity refer to PS-165 "Accountability for Movement of Equipment and Media" for further guidance regarding documentation.

Applicable Standards and Regulations:

45 CFR §164.310(d)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): County Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-155: Contingency Operations

Purpose:

The purpose of this policy is to comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to the confidentiality, integrity and availability of electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer and Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose ePHI for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall maintain backup data both on and offsite that can be used to recreate data lost as a result of machine failure or other disaster and operate from a secure alternate facility, if necessary.

Procedures:

1. Mitigating Loss of Information

   Workforce members, Elected Officials and volunteers who believe that a system failure or other disaster has resulted in the loss of information should immediately report the suspected failure to Mahaska County's Chief Security Officer (CSO) and/or IT Director. If the CSO or IT Director are unavailable, the user shall promptly contact the county's Chief Privacy Officer (CPO), Board of Supervisors or senior most manager, whichever responds first, to advise them of the suspected problem.

   The first responding personnel listed above shall activate Mahaska County's back up data plan to preserve any available data and inform all county information system users of the potential loss of data and advise them to promptly save essential data using a contingency data backup device assigned to the user solely for such purposes.

   The personnel responding to the user notification of a possible loss of data, if other than the CSO or IT Director, shall cause the CSO or IT Director to be notified of the event at the earliest opportunity. Upon notification of the CSO or IT Director, the CSO or IT Director shall assume responsibility for overseeing the emergency backup of data, data preservation, and assessment of Mahaska County's information system utilizing the following procedures:

A. If possible, isolate affected machines from the county's information system by means of blocking traffic in and out of the machine utilizing a firewall control, physically disconnecting the machine from any hardwired connection to the system, or depowering the county wireless router if the machine is connected to the information system via wireless connection;
B. If possible, initiate a malware scan of each device and quarantine or render inert any malware detected. (See also Policy and Procedure AS-215 "Protection from Malicious Software"); and
C. Locate the master data file on each affected machine or potentially affected machine and, using the user's dedicated contingency backup device for that machine to backup all data in the master data file held on the paired machine. (See also Policy and Procedure AS-225 "Data Backup and Storage");

(Note: The dedicated contingency backup device is usually a sealed thumb drive so labeled and that has been wiped of all previously stored data, scanned for malware, and operationally tested with standard dummy data to assure the integrity of stored data.)

D. Complete a diagnostic scan of the machine's operating software utilizing comprehensive maintenance software and thoughtfully assess any findings or recommendations before taking any corrective action; and
E. Once it has been assured that the machine's hardware and software are in good operating order, verify the integrity of any backup data to be uploaded, using standard backup or contingency backup data as appropriate;

(Note: This step should be taken in consultation with qualified IT personnel following a thoughtful assessment of the nature of the original problem and any subsequent actions taken. If necessary a copy of the backup data or contingency data should be made to preclude inadvertent loss of data during the restoration process.)

F. Following restoration of the backup of contingency back up data, conduct a complete system scan for malware and operational check for system function and data integrity;
G. During the period that the machine is offline for emergency backup, diagnosis, repair, testing or offline storage, the device must be tagged as out of service; and
H. Once the machine has passed a return-to-service check, the device may be tagged as operable and returned to service or serviceable storage.

(Note: The county's HIPAA Master Manual specifies multiple log entries, as indicated by Policy and Procedure AS-255 "Device and Media Controls – Accountability.")

2. Operating from an Alternate Facility

Contingency plans to establish a secure backup location have been developed for use in the event that circumstances preclude operating from Mahaska County's usual location, such as may occur as the result of a natural disaster. Mahaska County's CSO and CPO shall be responsible for assessing the adequacy of such plans annually, in consultation with the Board of Supervisors or senior most management.

Contingency plans for an alternate location contemplate disaster recovery and are as follows:

A. An alternate location must provide for the security of any information system and storage of essential business records, including onsite PHI/ePHI;
B. An alternate location must provide for the secure electronic transmission of data between Mahaska County and its electronic health record (EHR) vendor or Community Services Network (CSN);
C. No county local area network (whether hardwired or wireless) may be shared with any non-county local area network;
D. Areas containing workstations shall provide for the privacy and security of PHI/ePHI by preventing viewing by onlookers and controlled access to areas containing information system components (whether installed, serviceable storage or inoperable storage), onsite PHI/ePHI, and back up data storage; and
E. Areas used by county staff and patients shall meet local zoning ordinances, building codes, and Occupational Safety and Health Administration (OSHA) requirements.

3. Alternate Operating Facility Considerations
   A. Zoning;
   B. Location;
   C. Facility Type;
   D. Exits;
   E. Lavatories;
   F. Parking;
   G. Safety;
   H. Patient Area;
   I. Workstations;
   J. Storage; and
   K. Data Source.

Applicable Standards and Regulations:

45 CFR §164.310(a)(2)(i)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-160: Maintenance Records

Purpose:

Distributed systems administrators will identify the physical components that are essential to security. These systems administrators must oversee any security-relevant physical modifications. A maintenance record must be created for each modification made to the physical site, facility or building. Such information must be securely stored.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) or electronic protected health information (ePHI) for any purpose. This policy covers all PHI/ePHI which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

All repairs and modifications to the physical components of Mahaska County's facilities that affect office, information system, or data security (e.g., hardware, walls, doors, locks, wiring, etc.) shall be reviewed and accounted for in Mahaska County's risk assessment and risk management plan.

Procedures:

Mahaska County's Chief Security Officer (CSO), assisted by the county's Chief Privacy Officer (CPO) and Risk Manager, will review in advance the potential impact of any modifications to the physical facilities upon county workstations, Mahaska County's information system, PHI/ePHI and any data essential to disaster recovery and present his/her findings to the county's CPO and Board of Supervisors for consideration and action, as necessary. This may involve altering modifications to the county's facilities. However, where alteration of repairs or modifications are not practicable, within the control of the county, or is otherwise not possible, then the CSO will revise security procedures as necessary and in consideration of a total risk management approach that maximizes workplace safety, minimizes the possibility of security and privacy breaches, and maintains the integrity of the county's information system, PHI/ePHI and all disaster recovery elements.

Applicable Standards and Regulations:

45 CFR §164.310(a)(2)(iv)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

PS-165: Accountability for Movement of Equipment and Media

Purpose:

To establish a standard for achieving accountability in protecting or tracking the movement of electronic sensitive information in to and out of Mahaska County departments and offices, as well as the movement of these items within Mahaska County departments and offices, and to encourage the encryption of sensitive information whenever possible.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (PHI) for any purposes. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

A log shall be maintained of any movements of computer equipment within the county and all removal of equipment and storage media from Mahaska County's facilities. This policy applies to the transfer of equipment and storage media to off-site storage locations or transfers that are not routine. This policy does not apply to routine shifting of equipment during ordinary operation or maintenance.

Procedures:

1. Computer Hardware Storage, Installation, and Placement In Service

Mahaska County's Chief Security Officer (CSO) will maintain a contemporaneous inventory of all operational computer hardware stored (including router, printers and modems), installed or placed in service by the county. Log entries must include:

A. A description of the equipment stored, installed or placed in service;
B. The equipment serial number;
C. The date and time on which the equipment is placed in operational storage, installed or placed in service;
D. The location of the equipment (e.g. stored or installed location);
E. The means used to determine/verify that the equipment is operational;
F. The name of the person making the determination that the equipment is operational;
G. The name of the person for placing operational equipment in storage, installing operational equipment or placing it in service; and
H. The date the equipment is operationally checked using dummy test data to assure data and system integrity and functionality prior to return to service;
I. The date and time approval for return to service is granted; and

J. The name of the person approving the installed component and associated system for return to service.

2. Computer Hardware Removal from Service

Contemporaneous log entries will also be made to reflect removal of all computer equipment (including routers, printers and modems) removed from service or the control of the county. Log entries must include:

A. A description of the equipment removed;
B. The equipment serial number;
C. The date and time that the equipment is removed from service or control of the county;
D. The destination of the equipment;
E. The reason for removal, such as operational rotation, equipment repair, sanitization, destruction or disposal;
F. The name of the person performing required sanitization, tests, or operational checks of equipment necessary to maintain data security or integrity or the need for repair, destruction or disposal;
G. If the equipment is repaired, destroyed or disposed of offsite, the name of the person transporting the equipment, as well as the date, time, and location to which it is transported;
H. If the equipment is repaired, the name of the person or vendor accepting the equipment from Mahaska County;
I. If the equipment is being accepted from the person or vendor completing the repair, the date, time and the name of the person accepting the equipment on behalf of Mahaska County;
J. If the equipment is being accepted following repair, the name of Mahaska County's CSO or his/her authorized designee reviewing the repair documents or completing tests or operational checks that indicate the equipment is in a condition acceptable for return to service; and
K. If the equipment is to be destroyed or disposed of, the date, time and name of the person or vendor accepting the equipment for destruction.

3. Movement and Disposition of Data Storage Media and Data Storage Devices

Contemporaneous log entries will be made to track the movement of data storage media or data storage devices to and from off-site storage facilities. These log entries must include:

For Offsite Storage

A. The date and time that the storage media or storage device was removed from Mahaska County's operations facility for placement in offsite storage;
B. The location of the storage facility;
C. The date and time that the media were secured at the offsite location;
D. The name of the person responsible for removal from Mahaska County's operations facility and transport to the offsite storage facility; and
E. The name of the person securing the storage media or storage device at the offsite storage facility.

For Return to Onsite Storage or Return to Service at Mahaska County's Operational Facility

A. The date and time that the storage media or storage device was removed from the offsite storage facility for return to Mahaska County's operational facility;
B. The location of Mahaska County's operational facility;
C. The date and time that the media were secured at Mahaska County's operational facility;
D. The name of the person responsible for removal from Mahaska County's offsite storage facility and transport to the county's operational facility; and
E. The name of the person testing the storage media or storage device for potential malware, data integrity, and functionality;
F. The specific tests and results obtained;
G. The name of the person authorizing return to service, sanitizing, repair or destruction and disposal;
H. When sanitization, repair; destruction or disposal is deemed appropriate, the name of the person or vendor making the determination;
I. When approved, for return to service following testing, sanitizing or repair, the date of the approval for return to service by the CSO or his/her authorized IT designee; and
J. Disposition following approval for return to service (e.g., onsite storage or installation in another device or information system by make, model and serial number).

Applicable Standards and Regulations:

45 CFR §164.310(d)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

Technical Standards

TS-105: Password Management

Purpose:

Passwords/Pass Phrases are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password/pass phrase may result in the compromise of Mahaska County's entire network. As such, all Mahaska County individuals are responsible for taking the appropriate steps, as outlined below, to select and to secure their passwords/pass phrases.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose protected health information (PHI) and electronic protected health information (ePHI) for any purposes. This policy covers all PHI/ePHI, which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

It is the Policy of Mahaska County that all users must select a password conforming to Mahaska County guidelines specified below.

Password Guidelines:

- Passwords should be a minimum of 8 characters.
- Passwords must contain two of the following three: Capital letter, number or special character (such as &, %, $)
- Passwords should not be the name of a pet, spouse, child, or parent. Date of birth, anniversary, phone number, social security number
- Passwords should be a word or sequence of letters and numbers that the user can remember but could not be easily guessed by even a close friend of the user.
- Passwords should never be written down.
- Passwords should never be given to other staff members.
- A new password should be selected every six months, and current or previous passwords should not be re-used.

Procedures:

1. The CSO, or designee, reviews password policies when a user first receives his or her user ID.
2. The CSO, or designee, monitors password usage and identifies any patterns that suggest password policies and guidelines are not being followed.

3. The CSO, or designee, requires workforce members, Elected Officials and volunteers who frequently lose or forget their passwords to complete retraining on the correct use of passwords

Applicable Standards and Regulations:

45 C.F.R.§ 164.312(a)(2)(i)
45 C.F.R.§ 164.308(a)(5)(ii)(D)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

TS-110: Automatic Logoff

Purpose:

To require that reasonable and appropriate steps are taken to ensure that hardware, software and/or procedural mechanisms will be implemented to automatically log off users after a predetermined time of inactivity on systems containing confidential information.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information (ePHI) for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall adopt electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Procedures:

All workstations, laptops, or tablets shall be configured to log users off after 10 minutes of inactivity. After being automatically logged off, a user must re-enter his or her user name and password to resume the interrupted activity.

All county cell phones that could be used collect, develop, transmit or store PHI or county data essential to disaster recovery shall be configured to log users off after 5 minutes of inactivity. After being automatically logged off, a user must re-enter a complex password to resume use of the device. Users may neither alter nor disable automatic logoff features established for county devices.

Applicable Standards and Regulations:

45 CFR § 164.312(a)(2)(iii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

TS-115: Encryption and Decryption of Electronically Transmitted Data

Purpose:

This policy reflects Mahaska County's commitment to appropriately use encryption to protect the confidentiality, integrity and availability of protected health information (PHI) and electronic health protected information (ePHI) contained on Mahaska County information systems.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy applies to all electronic data stored on any media or system(s) throughout Mahaska County and applies to all individuals storing, accessing, or working with the data, in any way, including all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

When determined necessary by the either the Chief Security Officer (CSO) and/or IT Director, information that is either stored internally or transmitted externally by Mahaska County shall be encrypted to prevent use of PHI/ePHI by unauthorized individuals.

Procedures:

Electronic private health information (ePHI) will be encrypted when at rest and when transmitted over a network that might be accessible by unauthorized individuals. Information that can be used to alter or defeat the county's security measures will also be encrypted.

The technical methods used to implement encryption and decryption will be determined by Mahaska County's CSO.

Applicable Standards and Regulations:

45 CFR § 164.312(a)(2)(iv)
45 CFR § 164.312(e)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

TS-120: Integrity Controls and Data Transmission

Purpose:

To comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information (ePHI).

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County shall implement technical measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. This shall include appropriate integrity controls for electronic transmissions.

Procedures:

Applications that transmit information electronically must include technical capabilities to ensure that the information received is the information that was transmitted by the sender through the use of measures including use of:

1. Transport layer security (TLS) and secure sockets layer (SSL); and
2. Current data encryption/decryption systems using automated key generation and recognition;

Integral data integrity checking such as mirroring or check-summing is a function of data handling systems and is not within Mahaska County's expertise to manage. However, Mahaska County's CSO will check the transmission of dummy data to verify that the processes of encryption, transmission and decryption leave the original test data (i.e., dummy data) both functional and unaltered.

Applicable Standards and Regulations:

45 CFR §164.312(e)(2)(i)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

TS-125: Protecting Integrity of ePHI from Improper Alteration or Destruction

Purpose:

To appropriately protect the integrity of all electronic protected health information (ePHI) contained on all Mahaska County information systems.

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose ePHI for any purposes. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County's Chief Security Officer (CSO) shall implement procedures and technical measures to guard ePHI from improper alteration or destruction. Workforce members, Elected Officials and volunteers must follow these procedures and may not take any action to evade the technical measures.

Procedures:

The technical measures established by Mahaska County's CSO should permit ePHI to be modified only by workforce members with appropriate authorization.

Applications used to create and modify ePHI should support tracking of changes to records, including the identity of the staff member making the change, the nature of the change being made, and the date on which the change was made.

In the event a record is modified to accurately reflect events, diagnoses, assessments and treatment plans and relevant county information, and an electronic record cannot be made, then a contemporaneous log detailing such changes shall be maintained, including the date and time of the change and signature of the workforce member making the change. Such logs will be electronically appended to ePHI documents or added to archival hard copies of the affected case file.

Applicable Standards and Regulations:

45 CFR §164.312(c)(1)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:

Darin Hite		

TS-130: Audit Controls

Purpose:

It is the policy of Mahaska County to safeguard the confidentiality, integrity, and availability of individual health information applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, Mahaska County shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusios.
- Breaches in confidentiality and security of individual protected health information.
- Performance problems and flaws in applications.
- Improper alteration or destruction of electronic protected health information (ePHI) - information integrity.

This policy applies to organizational information applications, systems, networks, and any computing devices, regardless of ownership [e.g., owned, leased, contracted, and/or stand-alone).

Responsible for Implementation:

Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose ePHI for any purposes. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County's Chief Security Officer (CSO) shall implement technical measures to create a record of information system activity, including user logon/logoff and startup/shutdown of technical security measures.

Procedures:

The CSO will periodically review records of system activity, including review of network and component access logs, anti-malware logs, software update status, random testing of applications and data retrieval, as well as a review of current licenses agreements to identify actual or potential system and security problems.

Applicable Standards and Regulations:

45 CFR §164.312(b)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

TS-135: Data Backup and Storage

Purpose:

To appropriately protect the integrity of all electronic protected health information (ePHI) contained on all Mahaska County information systems.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy is applicable to all departments that use or disclose ePHI for any purposes. This policy covers all ePHI, which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Before computer equipment is relocated within or removed from Mahaska County's facilities, a back-up copy is created of any information that is contained on storage devices that are integral parts of a piece of computer equipment.

Procedures:

Workforce members, Elected Officials and volunteers, IT vendors and others responsible for maintaining county computer equipment will ensure that a complete back-up data set of any information contained on that equipment is made before the equipment is relocated within or removed from Mahaska County's facilities.

Note: This policy and procedure applies to other than mobile devices that do not transport irreplaceable county or client data and for which backup is routinely accomplished and mobile security measures are in place to protect ePHI.

Applicable Standards and Regulations:

45 C.F.R §164.310(d)(2)(iv)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

TS-140: Emergency Access Procedure

Purpose:

To appropriately protect the integrity of all ePHI contained on all Mahaska County information systems.

Responsible for Implementation:

Chief Privacy Officer and Chief Security Officer

Scope:

This policy is applicable to all departments that use or disclose electronic protected health information for any purposes. This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit ePHI in connection with activities at Mahaska County.

Policy:

Mahaska County's computer equipment shall be configured to allow only those workforce members, Elected Officials and volunteers with appropriate authorization access to information stored on its computer(s) and to configure software installed on the equipment.

IT vendors and workforce members, Elected Officials and volunteers who implement contingency plans must authorization from the Chief Security Officer (CSO) that permits them to repair equipment and implement emergency procedures. If user accounts must be deleted or disabled to repair equipment failures or restore functions during an emergency, the affected users shall be notified and new user names and passwords shall be established.

Procedures:

The CSO will maintain a contemporaneous written record of so-called "administrator" user account names and passwords the names of those persons authorized by the CSO to exercise administrator privileges in a secure, locked file. An administrator user account has full authorization to configure equipment and software.

Applicable Standards and Regulations:

45 C.F.R §164.312(a)(2)(ii)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

TS-145: Person or Entity Authentication

Purpose:

Mahaska County is committed to conducting business in compliance with all applicable laws, regulations and Mahaska County policies. This Policy covers the procedures to be implemented by each Mahaska County Department that is a HIPAA health care component to verify that a person or entity seeking access to electronic Personal Health Information (ePHI) is the person or entity claimed.

Responsible for Implementation:

Chief Privacy Officer

Scope:

This policy covers all protected health information (PHI) and all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all PHI/ePHI, which is available currently, or which may be created and/or used in the future. This policy applies to all workforce members, Elected Officials and volunteers who collect, maintain, use or transmit PHI/ePHI in connection with activities at Mahaska County.

Policy:

Each user of Mahaska County's information system shall, at all times, follow the various guidelines described in this manual for person or entity authentication to maintain the security and integrity of the system.

Procedures:

Every workforce member, Elected Official and volunteer authorized to use Mahaska County's information systems will be given a unique user name and select a password known only to the individual. Workforce members, Elected Officials and volunteers must use their user name and password to use the information system and access ePHI.

Each user shall select a unique password and employ it when logging on to the county's information system. No workforce members, Elected Officials and volunteers may use another individual's user name and password to access Mahaska County's information system.

Passwords should comply with the following guidelines:

1) Passwords used to access Mahaska County's information system shall not be used for other purposes (e.g., to sign on to a cell phone or to access one's personal bank account).
2) Passwords shall be complex utilizing a combination of letters, numbers and special characters, be between six and 10 characters or more that the user can recall but that cannot easily be guessed, even by a close acquaintance of the user.
3) Passwords shall not be the name of a pet, spouse, child, or parent.
4) Passwords should never be written down.
5) Passwords shall not be given to other staff members.

A new password will be selected at least every six months or whenever the password becomes known to others; and current or previous passwords shall not be reused.

Applicable Standards and Regulations:

45 CFR §164.312(d)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
James Blomgren		

TS-150: Mechanism to Authenticate

Purpose:

This standard reflects Mahaska County 's commitment to implement appropriate electronic mechanisms to confirm that electronic protected health information (ePHI) contained on Mahaska County healthcare computing systems or other systems containing private information (the "Systems") has not been altered or destroyed in an unauthorized manner.

Responsible for Implementation:

Chief Security Officer

Scope:

This standard is applicable to all workforce members who are responsible for or otherwise administer a System. A System is defined as a device or group of devices that store ePHI, or other private information which is shared across the network and accessed by county workers.

Policy:

Mahaska County must implement appropriate electronic mechanisms to confirm that ePHI contained on Mahaska County Systems has not been altered or destroyed in an unauthorized way.

Procedures:

Electronic mechanisms used to protect the integrity of data contained on Mahaska County Systems must ensure that the value and state of the data is maintained, and it is protected from unauthorized modification and destruction. Such mechanisms must also be capable of detecting unauthorized alteration or destruction of data. Such mechanisms might include:

1. System memory, hard drives, and other data storage devices with error-detection capabilities
2. File and data checksums
3. Encryption

Applicable Standards and Regulations:

45 C.F.R. §164.312(c)(2)

Distribution:

Policy Distribution:
Specific Location(s): Organization Wide

Version History:

Current Version		
Implementation Date:		
Prepared By:	Reviewed and Approved By:	Content Changed:
Darin Hite		

Appendix A

Acronyms and Definition of Terms

A

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Accounting for Disclosures: Upon request, a covered entity must provide the individual with an accounting of each disclosure by date, the Protected Health Information (PHI) disclosed, the identity of the recipient of the PHI, and the disclosure. However, where the covered entity has, during the accounting period, made multiple disclosures to the same recipient for the same purpose, the Privacy rule provides for a simplified means of accounting. In such cases, the covered entity need only identify the recipient of such repetitive disclosures, the purpose of the disclosure, and describe the PHI routinely disclosed. The date of each disclosure need not be tracked. Rather, the accounting may include the date of the first and last such disclosure during the accounting period, and a description of the frequency of such disclosures.
A covered entity is not required to account for all disclosures of PHI. An accounting is **not required** for disclosures made:

- Prior to the covered entity's compliance date;
- For Treatment, Payment and Healthcare Operation (TPO) purposes;
- To the individual or pursuant to the individuals written authorization; or
- As part of a limited data set.

American Recovery and Reinvestment Act of 2009 (ARRA): requires HHS to audit covered entity and business associate compliance with the HIPAA privacy and security standards and the breach notification rule.

B

Breach: The term 'breach' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Business Associate (BA): A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right. Also see Part II, 45 CFR 160.103.

Business Associate Agreement (BAA): The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate.

C

Chief Privacy Officer (CPO): HIPAA regulations state that *a covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.*

Chief Security Officer (CSO): HIPAA regulations state that covered entities and business associates must formally designate a Security Officer *who is responsible for the development and implementation of the policies and procedures required by the Security Rule for the entity.*

Covered Entity (CE): Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction. Also see Part II, 45 CFR 160.103.

Covered Function: Functions that make an entity a health plan, a health care provider, or a health care clearinghouse. Also see Part II, 45 CFR 164.501.

D

Data Element: Under HIPAA, this is the smallest named unit of information in a transaction. Also see Part II, 45 CFR 162.103.

Disclosure: Release or divulgence of information by an entity to persons or organizations outside of that entity. Also see Part II, 45 CFR 164.501.

E

Electronic Health Record (EHR) or Electronic Medical Record (EMR): An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Electronic Storage Device: Any medium that can be used to record information electronically. Examples include hard discs, compact discs, magnetic tapes, flash drives, USB.

H

Healthcare Operations: Any of the following activities of the covered entity to the extent that the activities are related to covered functions: 1) conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment; 2) reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health-care providers, training of nonhealth-care professionals, accreditation, certification, licensing, or credentialing activities, 3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits; 4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5) business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and 6) business management and general administrative activities of the entity.[45 CFR 164.501]

Health and Human Services (HHS): The U.S. Department of Health and Human Services (HHS) is an agency of the federal government responsible for administrating programs that deal with health, welfare and health information technology (health IT), including the authority to mandate safeguards to protect the security and privacy of personally identifiable health care information.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law that makes a number of changes that have the goal of allowing persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives DHHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.

Hybrid Entity: A covered entity whose covered functions are not its primary functions. Also see Part II, 45 CFR 164.504.

I

Institutional Review Board (IRB): A group of peers in a clinical setting that examines a research proposal to insure patient safety and addresses the ethics of the proposed study.

M

Minimum Necessary: The Privacy Rule stipulates that covered entities limit the amount of information disclosed to the minimum necessary to achieve the specified goal [45 CFR 164.514(d)(1)]. This requirement would not apply if the disclosure were required by law, authorized by the individual, or for treatment purposes.

N

Non-Retaliation: Covered Entities are mandated by HIPAA regulations to have non-retaliation policies enforced for reports of HIPAA violations

O

Office for Civil Rights (OCR): Through the federal civil rights laws and the HIPAA Privacy Rule, OCR protects fundamental nondiscrimination and health information privacy rights by: 1) Teaching health and social service workers about civil rights, health information privacy, and patient safety confidentiality laws; 2) Educating communities about civil rights and health information privacy rights; and 3) Investigating civil rights, health information privacy, and patient confidentiality complaints to identify discrimination or violation of the law and take action to correct problems. OCR can investigate complaints against covered entities (health plans, health care clearinghouses, or health care providers that conduct certain transactions electronically) and their business associates.

P

Payment: 1) The activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a health-care provider or health plan to obtain or provide reimbursement for the provision of health care; and 2) the activities relate to the individual to whom health care is provided and include, but are not limited to (i) determinations of eligibility or coverage and adjudication or subrogation of health benefit claims, (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance) and related health-care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (a) name and address; (b) date of birth; (c) social security number; (d) payment history; (e) account number; and (f) name and address of the health-care provider or health plan.

Protected Health Information (PHI): PHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information. See Part II, 45 CFR 164.501.

Public Health Authority: A public health authority is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501, 65 F.R. p. 82805

S

Sanctions: Covered Entities and Business Associates are mandated by HIPAA regulations to have disciplinary/sanction policies enforced for HIPAA violations

T

Tracking disclosures: see Accounting for Disclosures

Treatment: is the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

W

Workforce: Under HIPAA, this means employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity. Also see Part II, 45 CFR 160.103.

Facsimile Cover Sheet

Mahaska County

To: **From:**

Company: **Department:**

Fax#: **Pages including cover sheet:**

Phone: **Date:**

Re: **CC:**

ڤ **Urgent** ڤ **For Review** ڤ **Please Comment** ڤ **Please Reply** ڤ **Please File**

Comments:

Confidentiality Notice: The information contained with this cover letter is privileged and confidential patient information, intended only for the use of the addressee named above. **Disclosure of protected health information to any other party is prohibited by Law, under Federal Privacy Regulations, Public Law 104-191, Health Insurance Portability & Accountability Act (HIPAA).** Additionally, other restrictive information under this coversheet, is intended to be used only by the identified recipient, for business purposes. If the reader of this message is not the intended recipient or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that dissemination, distribution or copying of this information is prohibited. If you have received this communication in error, please notify us immediately by telephone @ 641-673-9819.

Thank You.

Form AS-155a

Privacy Concern or Security Breach Investigation Form

(place on Mahaska County letterhead)

Person Reporting Concern _____Date:_____

(If reporting anonymously, specify "unknown".)

Please ***circle*** one of the following:

I am a patient/client
I am an employee or elected official
I am a consultant or business associate
"Other" than above
If "other", please identify. _____

Please Identify Privacy Concern or Security Breach_____

_____

_____

_____

Please attach any available documents that may assist in this investigation.

If you would like to be contacted regarding this concern, please document your name address and phone number below.

_____

Name (First) (M.I.) (Last)

_____

Address City State Zip Code

(_____)_____

Telephone Number

OFFICE USE ONLY, BELOW THIS LINE

Investigation Conducted by: _____

Name (First) (M.I.) (Last)

Individuals Interviewed: _____

Name (First) (M.I.) (Last) Phone

Individuals Interviewed: _____

Name (First) (M.I.) (Last) Phone

Individuals Interviewed: _____

Name (First) (M.I.) (Last) Phone

Findings_____

_____

_____

Corrective Action_____

_____

_____

Privacy/Security Officer Signature Date:

Restriction Request for Use and Disclosure of Protected Health Information (PHI)

In completing this form, you are requesting the following restrictions as limitations to Mahaska County's use and disclosure of your PHI. You will be notified in writing of Mahaska County's decision to accept or deny your restriction request. Until a decision is reached, your request for restriction will not be honored.

Patient Name:	
Date of Birth:	
Contact Information:	
Record Number:	
Requested Restrictions:	
Reason for Request of Restriction:	

Select Type of Restriction

Permanent Restriction			
		(Initial)	

Temporary Restriction			
		(Initial)	Expiration Date for Temporary Restriction

Signature of Patient or Representative: _____

Date: _____ Relationship to Patient: _____

FOR MAHASKA COUNTY USE ONLY	
_____*Accepted*	
_____ *Denied (If denied document reason below and submit a copy to Patient.)*	
Reason for Denial	
Signature:	
Title:	
Date:	

Form AS-200a

Business Associate Agreement (sample)

This Business Associate Agreement (this "Addendum") amends, and is made a part of, that certain Engagement Letter, by and between _____ ("Business Associate"), and Mahaska County ("Covered Entity"), dated _____, 2017 ("Underlying Agreement").

We typically have the BA signed at the time an agreement is signed, and prefer to make it an addendum to the main agreement because that agreement typically specifies the specific services to be delivered.

WHEREAS, Business Associate and Covered Entity are parties to the Underlying Agreement, pursuant to which Business Associate provides the Services (as defined in the Underlying Agreement) to Covered Entity, which include the use and disclosure of Protected Health Information;

This section is required

WHEREAS, Business Associate and Covered Entity wish to set forth their understandings with regard to the use and disclosure of Protected Health Information in compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations set forth at 45 C.F.R. Part 160 and Part 164, Subparts A and E (the "Privacy Rule"), and 45 C.F.R. Part 160, Part 162 and Part 164, Subparts A and C (the "Security Rule) (collectively, "HIPAA") and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("HITECH").

Sake of good order

WHEREAS, this Addendum shall replace in its entirety and supersede any other business associate addendum or agreement between Business Associate and Covered Entity.

Standard boiler plate

NOW THEREFORE, for and in consideration of the mutual promises and covenants contained herein and in order to assure compliance with HIPAA and HITECH, the parties agree as follows:

This section is required

SECTION I. DEFINITIONS

Capitalized terms used herein shall have the meanings assigned to such terms under HIPAA or HITECH, which definitions are incorporated herein by reference.

This section is the core of the agreement; it covers all the obligations and activities of the BA and permitted uses of PHI

SECTION II. DUTIES AND RESPONSIBILITIES OF BUSINESS ASSOCIATE

A. Use and Disclosure of Protected Health Information. Business Associate agrees not to use or further disclose Protected Health Information other than as permitted or required by this Addendum or the Underlying Agreement or as Required by Law.

B. Minimum Necessary. In connection with its performance of services under the Underlying Agreement, Business Associate's use, disclosure or request of Protected Health Information shall utilize information making up a Limited Data Set, if practicable. Otherwise, Business Associate will, in its performance of these services, make reasonable efforts to use, disclose, and request of Covered Entity only the minimum amount of Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, in accordance with 45 C.F.R. Section 164.502(b) and Section 13405(b) of the HITECH Act.

C. Specific Use or Disclosure Provisions. Unless otherwise limited by this Addendum, Business Associate may:

1. Use the Protected Health Information in its possession for the proper management and administration of Business Associate's operations or to carry out its legal responsibilities.

2. Disclose to subcontractors and agents the Protected Health Information in its possession for the proper management and administration of Business Associate's operations or to carry out its legal responsibilities, if such disclosure is Required by Law or where Business Associate obtains reasonable assurance from any person or entity to which Business Associate will disclose Protected Health Information that the person or entity will:

   a. Hold the Protected Health Information in confidence and use or further disclose the Protected Health Information only for the purpose for which Business Associate disclosed the Protected Health Information to the person or entity or as Required by Law; and

   b. Promptly notify Business Associate (who will in turn notify Covered Entity) of any instance of which the person or entity becomes aware in which the confidentiality of the Protected Health Information has been breached.

3. Use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. Section 164.504(e)(2)(i)(B).

D. Electronic PHI. To the extent Business Associate creates, receives, maintains or transmits Electronic PHI, Business Associate shall:

1. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity in accordance with 45 C.F.R. Sections 164.308, 164.310 and 164.312. Further, Business Associate shall comply with the policies and procedures and documentation requirements of HIPAA's security standards as set forth in 45 C.F.R. Section 164.316.

2. Ensure that any agent or subcontractor to whom it provides such Electronic PHI agrees to implement reasonable and appropriate safeguards to protect it; and

3. Report to Covered Entity any Security Incident of which it becomes aware.

E. PHI Safeguards. Business Associate shall use appropriate safeguards to prevent uses or disclosures of Protected Health Information other than as provided for by this Addendum.

F. Breach Notification. Subject to the law enforcement delay exception contained in 45 C.F.R. Section 164.412, Business Associate shall report to Covered Entity, following discovery and without unreasonable delay, but in no event later than sixty (60) calendar days from the date of discovery, any Breach of Unsecured Protected Health Information maintained by Business Associate or its subcontractors. Such report shall include the identification, if known, of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used or disclosed during such Breach. Business Associate shall provide such other available information as may be requested by Covered Entity to enable Covered Entity to comply with its notification requirements to Individuals, the Secretary and the media, in accordance with Section 13402 of the HITECH Act.

G. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Addendum or the Underlying Agreement.

H. Impermissible Uses and Disclosures. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided by this Addendum of which it becomes aware.

I. Subcontractors and Agents. Business Associate shall ensure that its agents, including subcontractors, to whom it provides Protected Health Information under this Addendum, agree to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

J. Access to PHI. Business Associate shall provide access, at the written request of Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual to meet the requirements under 45 C.F.R. Section 164.524 and to meet the electronic transmission requirements for access to Electronic Health Records by Individuals in accordance with Section 13405(e) of HITECH.

K. Amending PHI. Upon receipt of a written request by Covered Entity, Business Associate shall make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to, pursuant to 45 C.F.R. Section 164.526.

L. Accounting of Disclosures of PHI. Business Associate shall document all disclosures of PHI, including, as applicable, any disclosures of PHI through Electronic Health Records, and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. Section 164.528 and Section 13405(c) of HITECH. Business Associate agrees to provide to Covered Entity the information regarding such disclosures of Protected Health Information to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. Section 164.528 and Section 13405(c) of HITECH.

M. Availability of Books and Records. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of the U.S. Department of Health and Human Services or his or her designee in a time and manner directed by the Secretary, for purposes of the Secretary determining Covered Entity's or Business Associate's compliance with the Privacy Rule.

N. Sale of PHI. Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI without an authorization from each affected Individual, unless an exception under Section 13405(d) of HITECH applies.

O. Confidential Communications. Business Associate shall accommodate reasonable requests by Individuals for confidential communications in accordance with 45 C.F.R. Section 164.522(b).

P. Marketing. Business Associate shall comply with the prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of Marketing under 45 C.F.R. Section 164.501, unless permitted by this Addendum and Section 13406 of HITECH.

Q. Requests for Restriction. Business Associate shall comply with requests for restrictions on disclosures of PHI about an Individual if the disclosure is to a health plan for purposes of carrying out payment or health care operations, and the PHI pertains solely to a health care item or service for which the service involved was paid in full out-of-pocket, in accordance with Section 13405(a) of HITECH.

R. Standard Transactions. To the extent that Business Associate conducts any Standard Transaction for or on behalf of Covered Entity, Business Associate shall comply with each applicable requirement of 45 C.F.R. Part 162.

This section is optional, but we recommend it.

SECTION III. OBLIGATIONS OF COVERED ENTITY

A. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. Section 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. Section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

D. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if such use or disclosure were made by Covered Entity, except to the extent that Business Associate will use or disclose PHI for Data Aggregation or management and administrative activities of Business Associate.

This section is required, may be a bit wordy, but you know how attorneys can be!

SECTION IV. TERMINATION

A. The term of this Addendum shall be effective as of the Effective Date, unless a separate compliance date is specified by law or this Addendum for a particular requirement, in which case the separate compliance date shall be the Effective Date for that particular requirement. This Addendum shall terminate upon the final expiration or termination of the Underlying Agreement, unless earlier terminated in accordance with paragraph (B) of this Section.

B. Notwithstanding any other provision of this Addendum, if either Party ("Non-Breaching Party") becomes aware of a material breach of this Addendum by the other Party ("Breaching Party"), then the Non-Breaching Party may:

1. Provide an opportunity for the Breaching Party to cure the breach or end the violation, and terminate this Addendum and the Underlying Agreement if the Breaching Party does not cure the breach or end the violation within thirty (30) days of notice of a material breach; or
2. Immediately terminate this Addendum and the Underlying Agreement.

C. 1. Except as provided in subparagraph 2 below, upon termination of this Addendum for any reason, Business Associate shall cease and desist all uses and disclosures of Covered Entity's PHI and shall immediately return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

2. In the event that Business Associate determines that returning or destroying PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Business Associate shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes

that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

Everything below this, are optional. Two sections AMENDMENT and INTERPERATION are mentioned in the guidance provided by HHS. The rest is boiler plate for a "standard" agreement, but could be deleted. It's more a "legal question" which I can't answer for you, but I will say none of it is included in the guidance given by HHS.

This section is optional

SECTION V. AMENDMENT

This Addendum may not be modified, nor shall any provisions hereof be waived or amended, except in a writing duly signed by authorized representatives of the parties. The parties agree to take such action as is necessary to amend this Addendum from time to time to comply with the requirements of HIPAA, HITECH or other applicable laws relating to the privacy or security of Protected Health Information. Notwithstanding the foregoing, to the extent that any provision of this Addendum is in conflict with any law, regulation, rule, or administrative policy of any governmental entity, this Addendum will have been deemed to have been amended in order to bring it into conformity with these provisions

SECTION VI. GOVERNING LAW

This Addendum will be executed, delivered, integrated, construed and enforced pursuant to and in accordance with the laws of the State of Iowa. **THE PARTIES SUBMIT TO THE EXCLUSIVE JURISDICTION OF ANY STATE OR FEDERAL COURT SITTING IN MAHASKA COUNTY, IOWA AND ITS APPELLATE COURTS IN ANY ACTION OR PROCEEDING ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.**

SECTION VII. ASSIGNMENT

This Addendum may not be assigned by either party without the prior written consent of the other party. Except for the prohibition on assignment contained in the preceding sentence, this Addendum shall be binding upon and inure to the benefits of the heirs, successors, and assigns of the parties hereto.

Nothing stated or implied in this Addendum is intended to confer, nor shall it be construed to confer, any rights or remedies, upon any person other than the parties and their respective successors or assigns.

SECTION VIII. WAIVER OF BREACH

The waiver by either party of a breach or a violation of this Addendum shall not operate as, or be construed to be, a waiver of any subsequent breach of the same or other provision hereof. No waiver shall be effective against any party hereto unless in writing signed by that party.

SECTION IX. SEVERABILITY

If any provision of this Addendum is held invalid, the remainder of this Addendum shall not be affected unless the invalid provision substantially impairs the benefits of the remaining provisions of this Addendum.

SECTION X. INDEMNIFICATION

Each Party ("Indemnifying Party") shall indemnify, defend and hold harmless the other Party, its affiliates and each of their respective directors, officers, employees or assigns ("Indemnified Party") from and against any and all causes of action, claims, suits and demands whatsoever, and from all damages, liabilities, costs, charges, debts and expenses whatsoever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims) (collectively, "Liabilities"), which may be asserted or for which the Indemnified Party may now or hereafter become subject arising from or in connection with the Indemnifying Party's material breach of this Addendum, gross negligence or willful misconduct, except to the extent such Liabilities were caused by the Indemnified Party.

SECTION XI. SURVIVAL

The responsibilities of Business Associate under the provisions of Section IV, paragraph C of this Addendum shall survive termination of this Addendum indefinitely.

This section is optional

SECTION XII. INTERPRETATION

This Addendum shall be construed as broadly as necessary to implement and comply with HIPAA and the HITECH Act. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HITECH Act.

IN WITNESS WHEREOF, the parties have caused this Addendum to be duly executed as of

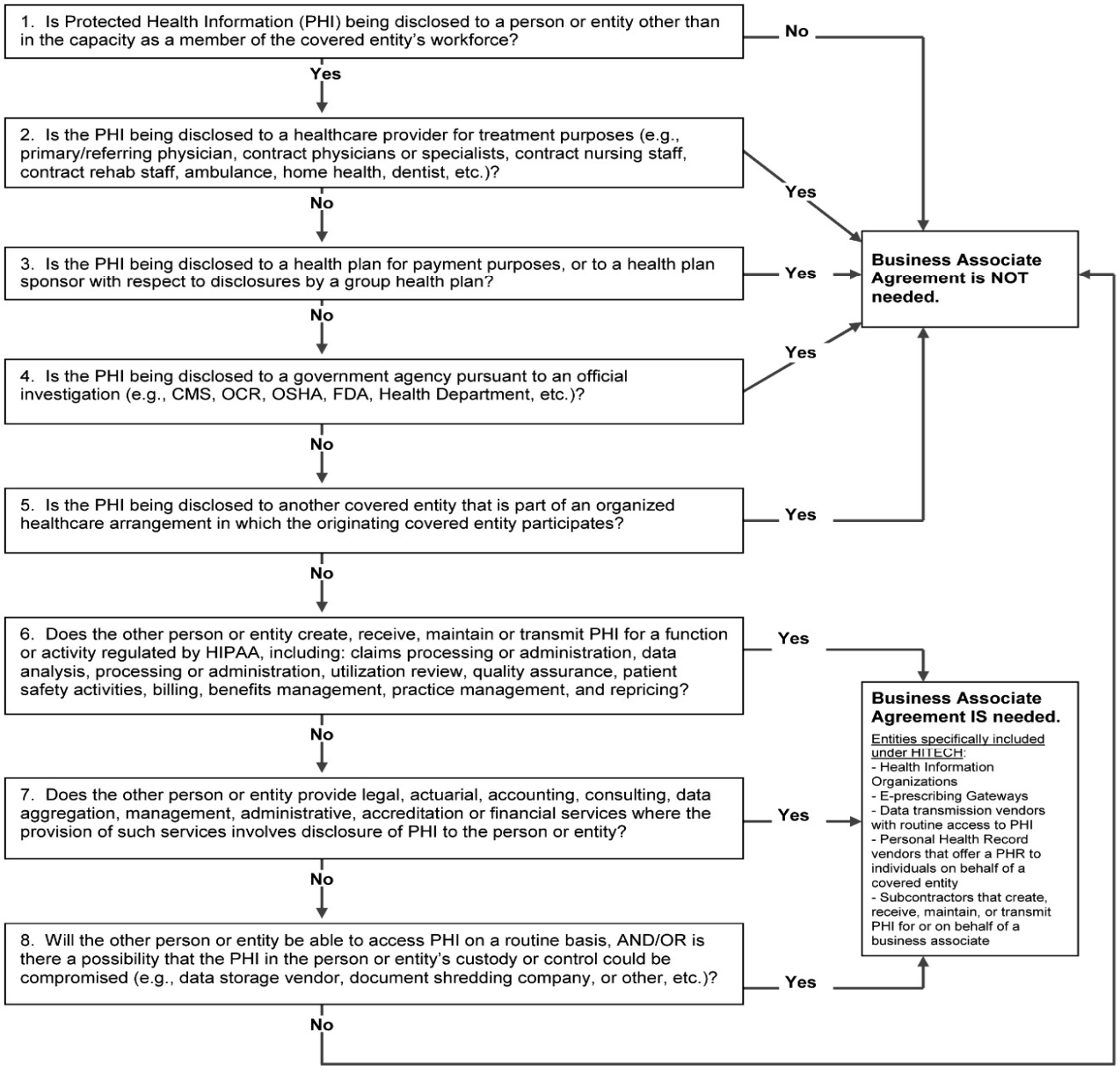
DATE _____.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
Mahaska County	[Business Associate]
By:_____	By:_____
[Covered Entity]	[Business Associate]
President	President & CEO

Business Associate Decision Tree

AS-260 c

HIPAA/HITECH
Business Associate Decision Tree



Carosh Compliance Solutions, LLC
10769 Broadway, #106 Crown Point, IN 46307
Phone: 219-310-2027 Fax: 866-792-3665 -- email: info@Carosh.com

Updated: July, 2013

Notice of Privacy Practices (sample of required information)

Header. A statement as a header or otherwise prominently displayed that states: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

Uses and Disclosures. A description of the types of disclosures that HIPAA allows without an authorization, including:

a) A description of at least one example of the types and disclosures that HIPAA permits the CE to make for treatment, payment, and healthcare operations.

b) A description of each of the other disclosures for which the CE is permitted or required to use or disclose PHI without the patient's authorization. These may include:

c) to family members and others involved in the patient's healthcare unless the individual has objected

d) to personal representatives,

e) to business associates, for facility directories unless the patient objects,

f) as required by law (this includes child or elder abuse, or domestic violence is state law allows),

g) to avert a serious threat or imminent harm to the patient or others,

h) for certain public health activities,

i) under certain conditions, for judicial or administrative proceedings,

j) for certain public health activities,

k) for health oversight activities,

l) for judicial or administrative proceedings if certain conditions are met,

m) for specified law enforcement activities if certain conditions are met,

n) to the extent allowed by state workers compensation laws,

o) to coroners, medical examiners, or funeral directors,

p) for research purposes if certain conditions are met, and

q) for certain specialized government functions.

A description of the types of uses and disclosures that require authorization, including psychotherapy notes, marketing, and sale of PHI. For marketing and fundraising, a specific statement is needed that the CE may contact the individuals regarding this, and that the patient has the right to opt out of these communications

A statement that other uses and disclosures not described in the NPP will be made only with the patient's written authorization (these should be listed out).

Individual Rights. Individual rights must be described, including:

a) the right to request restrictions and uses or disclosures of their PHI for treatment, payment, or healthcare operations,

b) the right to receive confidential communication by alternative means or at alternative locations (e.g. a patient may request email communication),

c) the right to inspect and copy their PHI (with the exception of psychotherapy notes, depending upon state law),

d) the right to amend their PHI,

e) the right to receive an accounting of disclosures of their PHI,

f) a right to request and receive a paper copy of the NPP,

g) a brief description of how the patient may exercise these rights (i.e. submitting a written request to your Privacy Officer). At least one example must be provided for which you are permitted to make disclosures for treatment, payment, or healthcare operations.

HITECH requires statements that also must be included are:

a) authorization is required for most uses and disclosures of psychotherapy notes,

b) an authorization is required for use and disclosures of PHI for marketing purposes or disclosures that constitute sale of PHI, and

c) a statement that other uses and disclosures that are not described in the NPP will require an authorization.,

d) a statement that the individual may opt out of receiving fundraising communications,

e) a statement that individuals who pay out of pocket in full for a healthcare item or service have the right to restrict disclosure of this PHI to their health plan,

f) they will be notified upon a breach of their PHI, and

g) a statement must be made that indicates the patient who pays out of pocket in full for a healthcare item or service has the right to restrict disclosures of PHI to their health plan.

Covered Entity Duties. A statement of the CE's duties must be included, stating the CE will:

a) maintain the privacy of the patient's PHI,

b) provide individuals with notice of its legal duties and privacy practices regarding their PHI,

c) notify them following a breach of their unsecured PHI,

d) abide by the terms of the NPP, and that the NPP will distribute any revised NPP to the patient. If the CE wishes to apply privacy practices changes to previously acquired PHI, the CE must include a statement to this effect (reserving the right to apply changes to all of the patient's PHI)

Complaints. The following statements regarding complaints must be included:

a) the patient has a right to complaint to the CE and to the Secretary of HHS if they believe their privacy rights have been violated,

b) the patient will not be retaliated against for filing a complaint, and

c) the CE must provide the process for how to file a complaint with the CE (you are not required to detail how they can complain to HHS)

Contact Person. The name of or title of the contact person and their telephone number must be provided for the person or office to contact for further information regarding their privacy rights

Optional Information. You may also include check off boxes for patient approval or denial to provide appointment reminders, provide information on treatment alternatives or marketing and fundraising solicitations as listed above.

Effective Date. CE's must provide the effective date of the notice, which may not be earlier than the date of printing of the (current) NPP. The notice must include an effective date, and a Covered Entity is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices (within 60 days).

Revised Notice of Privacy Practice: In the future if HHS revises its' NPP requirements, you are not required to hand out a revised NPP to your patients already in treatment, you need only post the revised NPP in a prominent location. You need to provide a revised NPP upon request. New patients need to receive the updated NPP, with an effort on your part to obtain good faith acknowledgement of receipt. Again, if any use or disclosure is prohibited or limited by state law, the more stringent law must be reflected and described in the NPP.

Good Faith Effort of Written Acknowledgement: Written acknowledgements of receipt of NPP or documentation of good faith efforts to obtain this acknowledgement should be documented and retained for at least 6 years. The acknowledgement may not be combined with other authorizations.

In addition, the Notice of Privacy Practices must be in *plain language.* HHS provides examples of this in the model NPPs. These examples are provided in both English and Spanish, and are editable for the specific entity. The examples are available at: http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html .

Pledge of Confidentiality and Privacy

In becoming compliant with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information and Technology for Economic and Clinical Health (HITECH) and the applicable rules issued by the Department of Health and Human Services and State Agencies, it is the policy of Mahaska County to maintain an individual's privacy and confidentiality at all times. HIPAA specifically requires workforce members and volunteers to use and or access protected health information (PHI) needed to reasonably accomplish the intended purpose, only to the extent of the function and duties they are providing as workforce members of Mahaska County. We further maintain that all protected health information will be secured and continually protected during its collection, use, disclosure, dissemination, storage and destruction at Mahaska County.

All persons associated with Mahaska County including workforce members, Department Heads, volunteers, contractors, and /or agents of the above mentioned and Business Associates shall be bound by this "Pledge of Confidentiality and Privacy of Protected Health Information."

All Mahaska County workforce members, Department Heads and volunteers and persons associated with Mahaska County are responsible for protecting the security and confidentiality of all protected health information (PHI, see definition of terms), whether in oral, written or electronic format. This applies to any PHI that is obtained, handled, learned, heard or viewed, while in the course of your work or association with Mahaska County.

Use or disclosure of PHI is acceptable only in the discharge of responsibilities and duties based on the need to know as minimally necessary. Discussion regarding PHI should not take place in the presence of persons not entitled to such information or in public places, such as break areas, common hallways, outdoor spaces, parking areas or areas off premises of Mahaska County.

I agree to comply with this pledge of Confidentiality and Privacy of Protected Health Information during my course of duties here at Mahaska County.

Additionally, I will not impart or make known to any person, or remove from Mahaska County premises or make, whether secured or unsecured copies of any such data, material or other information except as authorized to do so in writing by the privacy officer.

Finally, I understand that if I breach patient confidentiality, I am may be subject to disciplinary actions under Mahaska County Policy No. AS- 130 "Disciplinary Actions for Breach of Patient Privacy" and subject to the civil and/or criminal penalties pursuant to the HIPAA and HITECH laws and rules.

Accepted and Agreed to by:

_____Date_____

Workforce Member Signature & Title

Pledge of Confidentiality and Privacy for Contractors

In becoming compliant with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information and Technology for Economic and Clinical Health (HITECH) and the applicable rules issued by the Department of Health and Human Services and State Agencies, it is the policy of Mahaska County to maintain an individual's privacy and confidentiality at all times. HIPAA specifically requires workforce members and volunteers to use and or access protected health information (PHI) needed to reasonably accomplish the intended purpose, only to the extent of the function and duties they are providing. We further maintain that all protected health information will be secured and continually protected during its collection, use, disclosure, dissemination, storage and destruction at Mahaska County.

All persons associated with Mahaska County including workforce members, Department Heads, volunteers, contractors, and /or agents of the above mentioned and Business Associates shall be bound by this "Pledge of Confidentiality and Privacy of Protected Health Information."

All Mahaska County workforce members, Department Heads, volunteers, contractors and persons associated with Mahaska County are responsible for protecting the security and confidentiality of all protected health information (PHI, see definition of terms), whether in oral, written or electronic format. This applies to any PHI that is obtained, handled, learned, heard or viewed, while in the course of your work or association with Mahaska County.

Use or disclosure of PHI is acceptable only in the discharge of responsibilities and duties based on the need to know as minimally necessary. Discussion regarding PHI should not take place in the presence of persons not entitled to such information or in public places, such as break areas, common hallways, outdoor spaces, parking areas or areas off premises of Mahaska County.

I agree to comply with this pledge of Confidentiality and Privacy of Protected Health Information during my course of duties here at Mahaska County.

Additionally, I will not impart or make known to any person, or remove from Mahaska County premises or make, whether secured or unsecured copies of any such data, material or other information except as authorized to do so in writing by the privacy officer.

Finally, I understand that if I breach patient confidentiality, I am may be precluded from continuing my duties at Mahaska County and may be subject to the civil and/or criminal penalties pursuant to HIPAA, HITECH, and State law, rules and regulations.

Accepted and Agreed to by:

_____Date_____

Contractor Signature & Title

Acknowledgement of Receipt of Notice of Privacy Practices

Mahaska County
106 South 1st Street, Oskaloosa, IA 52577
641-673-9819

I have received a copy of Mahaska County's Notice of Privacy Practices effective [Date].

Name (please print): _____
Signature: _____
Date: _____

I am a parent or legal guardian of _____ (patient name). I have received a copy of Mahaska County's Notice of Privacy Practices effective [Date].

Name (please print): _____
Relationship to Patient: ☐ Parent ☐ Legal Guardian
Signature: _____
Date: _____

If the individual or parent/legal guardian did not sign above, staff must document when and how the Notice of Privacy Practices was given to the individual, why the acknowledgment could not be obtained, and the efforts that were made to obtain it.

Notice of Privacy Practices effective [date] given to individual on _____ (date)

☐ In Person ☐ Mailing ☐ Email ☐ Other _____

Reason individual or parent/legal guardian did not sign this form:

☐ Did not want to
☐ Did not respond after more than one attempt
☐ Other _____

The following good faith efforts were made to obtain the individual or parent/legal guardian's signature. Please document with dates, times, individuals spoken to, and outcome, as applicable, the efforts that were made to obtain the signature. More than one attempt must be made.

☐ In person conversation _____
☐ Telephone contact _____
☐ Mailing _____
☐ Email _____
☐ Other _____

Staff Name (please print): _____Title: _____
Signature: _____ Date: _____

Request for Access to Protected Health Information

File Number: _____

You have the right to inspect your protected health information in records, which Mahaska County creates or maintains. You also have the right to request copies of those records. You will be charged for the costs of copying and mailing for some records. Fees are indicated below. You will receive a response to your request within 30 days after we receive your request and payment. If you want copies of your records mailed, you need to send us a photocopy of your Driver's license, State Identification Card, or other valid identification. You will also need to send documentation verifying your address.
Checks should be made payable to: Mahaska County.

Mail this completed form to: Mahaska County 106 South 1st Street, Oskaloosa, IA 52577.
641-673-9819.

INDIVIDUAL INFORMATION

LAST NAME	FIRST NAME	MIDDLE INITIAL
ADDRESS	CITY/STATE	ZIP CODE
ID NUMBER	DATE OF BIRTH	
DAYTIME TELEPHONE NUMBER (REQUIRED)		
EVENING TELEPHONE NUMBER		
EMAIL ADDRESS		

DIRECTIONS

Please read the following before completing this form. If any of the circumstances below applies to you, you may not need to fill out this form.

You have a personal injury case and Mahaska County has paid for services related to the injury and you want information about these services and/or payments,
or
You are requesting access to records on behalf of a deceased Mahaska County beneficiary in order to repay Mahaska County for services received by the deceased beneficiary. You may have received an Estate Recovery Questionnaire in the mail,
or
You are involved in a worker's compensation case in which Mahaska County has paid for services for the injury you received while on the job.

Please call 641-673-9819 for further information. If none of these circumstances apply, please complete the form.

To continue with your request for access to your Mahaska County records, please go to page 2 and indicate which records you wish to get a copy of. Also, be sure to include the required information for verifying your identity and address, and include payment as indicated.

Form PR-130a

WHAT TYPE OF PROTECTED HEALTH INFORMATION DO YOU WANT TO ACCESS?

☐ TREATMENT RECORDS, which include visit records, lab/test results, immunizations, medications orders, referrals and treatment plans.

☐ TREATMENT AUTHORIZATION REQUEST SCREENS. Printouts contain patient names, which providers have requested services, which services were requested, the decision about the service(s), including a simple description of the decision, and whether the provider has billed for these services.

☐ CASE MANAGEMENT RECORDS, which contain case manager notes

☐ CLAIM DETAIL REPORTS, which contain claims paid by Mahaska County for services received. ($XX fee)

Managed Care Records:

- ☐ Enrollment Records
- ☐ Disenrollment Records
- ☐ Capitation Paid to Health Plan

Please contact your managed care plan if you want access to your medical records.

I AM REQUESTING COPIES OF RECORDS FOR THE FOLLOWING DATES OF SERVICE

You must specify dates of service in order to get records.

FROM DATE (month/day/year)	TO DATE (month/day/year)

☐ PLEASE MAIL ME A COPY OF THE REQUESTED INFORMATION.

☐ I WISH TO REVIEW THE REQUESTED INFORMATION IN PERSON.

IF YOU REQUEST TO REVIEW RECORDS IN PERSON, YOU WILL BE CONTACTED TO SCHEDULE AN APPOINTMENT.

☐ I REQUEST THAT A PERSON OF MY CHOOSING BE ALLOWED TO INSPECT MY RECORDS.
NOTE: Any person or attorney may be named below. Records will not be sent to photocopy services.

NAME:

TELEPHONE NUMBER:

ADDRESS:

RELATIONSHIP TO YOU:

IDENTIFYING INFORMATION IS REQUIRED

ADDRESS VERIFICATION ATTACHED

TYPE:_____(UTILITY BILL, PHONE BILL, DRIVER'S LICENSE, ETC.)

COPY OF IDENTIFICATION ATTACHED

TYPE:_____(STATE DRIVER'S LICENSE, STATE IDENTIFICATION CARD, BIRTH CERTIFICATE, BENEFITS IDENTIFICATION CARD, MANAGED CARE CARD, STATE OR FEDERAL EMPLOYEE ID CARD)

NUMBER: _____

(IF NO IDENTIFICATION IS ATTACHED, YOUR SIGNATURE MUST BE NOTARIZED.)

NOTARIZED BY_____ON_____(DATE). NOTARY

PUBLIC NUMBER _____

UNOFFICIAL UNLESS STAMPED BY NOTARY PUBLIC.

I DECLARE UNDER PENALTY OF PERJURY THAT THE INFORMATION ON THIS FORM IS TRUE AND CORRECT.

BENEFICIARY SIGNATURE DATE

_____ _____

NOTE: ANY ATTEMPT TO FALSELY GAIN ACCESS TO PROTECTED HEALTH INFORMATION IS SUBJECT TO LEGAL PENALTIES.

Form PR-130a

Notice of Decision of Request to Access, Inspect or Amend PHI

Your request to access, inspect or amend your personal health information, as checked below:
_____ Medical Records
_____ Billing Records
_____ Other, please specify _____
for dates covering the period of _____through_____.

In the format of: (Please check appropriate box below).

	Access with copies (An Authorization is needed and Release of Information policies apply. This may include charges to cover the cost of copying, postage, etc.).
	Inspection of my health information at Mahaska County.

Your request has been _____ Accepted or _____ Denied

Reason for Denial:

You do not have a right to access the information nor to request a review of this decision as it falls under the following category;

	Psychotherapy Notes
	The information is related to civil, criminal or administrative action
	The Information is subject to or exempt from the Clinical Laboratory Improvement Amendments of 1988 (CLIA).
	You are an inmate and the information requested could jeopardize the health safety, security, custody or rehabilitation of yourself or others.
	You have agreed to participate in research and have identified that this information is restricted while in the course of the research. You may access the information upon completion of the research.
	The information is subject to the Privacy Act.
	The information requested was obtained from a third party (non-health care provider) under condition of confidentiality.

Your request has been denied for the following reason; (Note: you may request a review of this decision by following the appeal procedure outlined on the back of this decision).

	A licensed Health Care Professional has determined that the access requested is likely to endanger the life or physical safety of yourself or others.
	The information requested makes reference to someone else and is likely to cause that person serious harm.
	As a personal representative it is believed that access to the requested information may subject the individual you represent to domestic violence, abuse or neglect or may endanger their life or is not in the best interest of the individual represented.
	Other (please specify);

Signature_____

Title: _____ Date_____

You may have the decision above appealed, by sending a written request to; Privacy Officer, Mahaska County 106 South 1st Street, Oskaloosa, IA 52577. Phone 641-673-9819. The request must be received within 10 days from the above date.

Form PR-130b

Request for Amendment of Protected Health Information

Mahaska County
106 South 1st Street, Oskaloosa, IA 52577
641-673-9819

Name _____ Record #_____

Date of Birth _____/_____/_____

Address _____

_____

Phone Number(s)_____

May we call you, if we deem it necessary? Yes ____ No ____
May we leave a message for you? Yes ____ No ____

After review of my healthcare/mental health record, I do not feel the original documentation reflects services rendered for the following service date(s)_____. I understand that Mahaska County may or may not supplement the record with an addendum based on my request and under no circumstances is it able to alter the original documentation of the record. In any event, this request for an addendum will be made part of my permanent medical record and will be sent as part of the medical record in response to any authorized requests for medical information.

I understand that Mahaska County will provide a response to this request within sixty days. I further understand that I have the opportunity to provide a statement of disagreement should my clinician or the agency deny my request.

Reason for the amendment

_____

_____

I request the following corrections/supplementation be made on my medical record:

_____

_____

Would you like this amendment sent to anyone to whom we have disclosed the information in the past?
Yes ____ No ____

If YES, please specify the name and address of the organizations or individuals.

_____

_____

_____

Name of Individual (Print)

_____

Name of Representative, if applicable (Print)

_____

Signature of Individual or Representative (Relationship) Date

CASE MANAGER or HEALTH CARE PROVIDER RESPONSE

____In response to your request, a correction/addendum will be made part of your permanent medical record.

____*Your request has been denied; however, your request is made part of your permanent medical record. The reason your request is denied is:*

_____

_____

If denied you may file a complaint with the Chief Privacy Officer, Mahaska County, 106 South 1st Street, Oskaloosa, IA 52577. Phone 641-673-9819.

Signature _____*Date:*_____

Response sent to individual by _____ *Date sent* _____

Mahaska County
106 South 1st Street, Oskaloosa, IA 52577
641-673-9819

Date

Patient/Individual Name
Address
City, State, Zip Code

Dear Patient/Individual Name,

Your request to amend your health information has been denied for the following reasons:

_____The protected health information in question was not created at Mahaska County.

_____The change to PHI that you requested is not accurate and or is incomplete.

_____PHI is not available to the patient for inspection as required by state and/or federal law for psychotherapy notes.

_____Other, as described: _____

_____

_____

Please contact is if we may be of any additional assistance.

Sincerely,

Chief Security Officer
Mahaska County Chief Privacy Officer
106 South 1st Street, Oskaloosa, IA 52577
641-673-9819

Consent for Health Information to be Communicated by Alternative Means

Name: _____

Address: _____

Electronic communications Address:_____

Telephone Number: _____

RISKS AND YOUR RESPONSIBILITY

At the discretion of Mahaska County, its workforce, volunteers and agents, and upon your agreement to the terms outlined within this consent form, you may use electronic communications to communicate with Mahaska County. These electronic communications may contain your personal health information. If you decide to use electronic communications to communicate with Mahaska County, you should be aware of the following risks and your responsibilities:

1) As the Internet is not secure or private, unauthorized people may be able to intercept, read and possibly modify electronic communications you send or are sent by Mahaska County.
2) You must protect your electronic communications account, password, SMS addresses and computer against access by unauthorized people.
3) Since electronic communications can be used to spread viruses, some which cause electronic communications messages to be sent to people who you do not intend to send electronic communications messages to, you should install and maintain virus protection software on your personal computer.
4) Since electronic communications can be copied, printed and forwarded by people to whom you send electronic communications, you should be careful regarding whom you send electronic communications.

CONDITIONS FOR THE USE OF ELECTRONIC COMMUNICATIONS

By consenting to the use of electronic communications with Mahaska County, you agree that:

1. Mahaska County may forward electronic communications as appropriate for diagnosis, treatment, reimbursement, and other related reasons. As such, Mahaska County staff members, other than the recipient, may have access to electronic communications that you send. Such access will only be to such persons who have a right to access your electronic communications to provide services to you. Otherwise, Mahaska County will not forward electronic communications to independent third parties without your prior written consent, except as authorized or required by law.
2. Although Mahaska County will try to read and respond promptly to your electronic communications, Mahaska County staff may not read your electronic communications immediately. Therefore, you should not use electronic communications to communicate with Mahaska County if there is an emergency or where you require an answer in a short period of time.
3. If your electronic communications requires or asks for a response, and you have not received a response within a reasonable time period, it is your responsibility to follow up directly with Mahaska County.
4. You should carefully consider the use of electronic communications for the communication of sensitive medical information, such as, but not limited to, information regarding sexually transmitted diseases, AIDS/HIV, mental health, developmental disability, or substance abuse.
5. You should carefully word your electronic communications messages so that the information that you provide clearly describes the information that you intend to convey.

6. You are responsible for correcting any unclear or incorrect information.
7. Mahaska County reserves the right to save your electronic communications and include your electronic communications or information contained within your electronic communications in your medical record.
8. It is the patient's responsibility to follow up and/or schedule an appointment if warranted or recommended by Mahaska County.
9. Electronic communications may not be the only form of communication that Mahaska County will use to communicate with you. Additionally, Mahaska County may decide that it is not in your best interest to continue to communicate with you by electronic communications. In such case, Mahaska County will notify that it no longer intends to communicate with you by electronic communications.

INSTRUCTIONS

a) You shall immediately inform those individuals with whom you communicate with at Mahaska County of changes in your electronic communications address.
b) You shall send electronic communications only to such Mahaska County electronic communications addresses as instructed.
c) You shall put your name and appropriate identifying information in the body of the electronic communications.
d) You shall include the category of the communications in the electronic communications' subject line, for handling purposes (e.g. prescription, appointment, medical advice, billing question, etc.)
e) Prior to sending the electronic communications, you shall review the electronic communications to make sure it is clear and that all relevant or requested information is provided.
f) You shall withdraw your consent to communicate by electronic communications by sending an electronic communication to all of the electronic communications addresses for which you had previously communicated.

PATIENT ACKNOWLEDGMENT AND AGREEMENT

Mahaska County will use reasonable means to protect the privacy of your health information sent by electronic communications. However, because of the risks outlined above, Mahaska County cannot guarantee that e- mail communications will be confidential. Additionally, Mahaska County will not be liable in the event that you or anyone else inappropriately uses your electronic communications. Mahaska County will not be liable for improper disclosure of your health information that is not caused by Mahaska County's intentional misconduct.

I acknowledge that I have read and fully understand this consent form. I understand the risks associated with the communications of electronic communications between Mahaska County and me, and consent to the conditions outlined herein, as well as any other instructions that Mahaska County may impose to communicate with me by electronic communications. Any questions I may have had were answered.

Patient Signature_____Date_____

Authorization for Use and Disclosure of Protected Health Information

I voluntarily consent to, and authorize, Mahaska County to use or disclose my health information during the term of this Authorization to the recipient(s) that I have identified below.

Recipient: I authorize my health care information to be released to the following recipient(s):

Name:_____

Address:_____

Purpose: I authorize the release of my health information for the following specific purpose:
_____.
(Note: "at the request of the individual" is sufficient if the individual is initiating this Authorization)

Information to be disclosed: I authorize the release of the following health information: (check the applicable box below)

- ❑ All of my health information that the provider has in his or her possession, including information relating to any medical history, mental or physical condition and any treatment received by me.
- ❑ Only the following records or types of health information:
  _____.

Term: I understand that this Authorization will remain in effect:

- ❑ From the date of this Authorization until the _____ day of _____, 20___.
- ❑ Until the Provider fulfills this request.
- ❑ Until the following event occurs:_____

Redisclosure: I understand that my health care provider cannot guarantee that the recipient will not redisclose my health information to a third party. The third party may not be required to abide by this Authorization or applicable federal and state law governing the use and disclosure of my health information.

Refusal to sign/right to revoke: I understand that signing this form is voluntary and that if I don't sign, it will not affect the commencement, continuation or quality of my treatment at Mahaska County. If I change my mind, I understand that I can revoke this authorization by providing a written notice of revocation to the Mahaska County Office of Compliance at the address listed below. The revocation will be effective immediately upon my health care provider's receipt of my written notice, except that the revocation will not have any effect on any action taken by my health care provider in reliance on this Authorization before it received my written notice of revocation.

Questions: I may contact the Mahaska County Chief Privacy Officer for answers to my questions about the privacy of my health information at Mahaska County 106 South 1st Street, Oskaloosa, IA 52577 or by phone at 641-673-9819.

Individual Information / Approval			
Printed name of Individual			
Signature of Individual		Date	
If individual is unable to sign this Authorization, please complete the information below:			
Printed name personal representative and his or her relationship to individual			
Signature of Individual		Date	
FOR OFFICE USE ONLY			
Application received Date		Identity of Individual Verified	YES / NO
Individual Record Number:			
Comments			
Staff's Name and Signature:			
Date:			
Date Entered into System:			

IT Asset Inventory

For Location:_____

ePHI Servers

Name	OS & Service Pack	Description

Network Devices

Name	Make and Model	Notes

ePHI Repository Summary - Include # of: desktops, laptops, PDAs, USB drives, DVD/CD, Backup and any other electronic media

Number	Make and Model	Notes

ISP, WAN, LAN and Data Circuit Summary (Please Attach)

For:	
By:	
Signature:	Date:

Appendix B

Electronic Signature Acknowledgement

Sue Brown 6/27/17

LEGAL NAME (please PRINT name clearly) DATE

Sue Brown

Sample Signature

SCOPE:
This Acknowledgement Form applies to electronic signatures executed for policies and procedures executed as part of your HIPAA compliance program.

AGREEMENT:
By signing this Electronic Signature Acknowledgment Form, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding.

By signing below, I accept the conditions of this agreement.

Signature Date

Electronic Signature Acknowledgement

James Blomgren — 6/27/17

LEGAL NAME (please PRINT name clearly) — DATE

James Blomgren

Sample Signature

SCOPE:
This Acknowledgement Form applies to electronic signatures executed for policies and procedures executed as part of your HIPAA compliance program.

AGREEMENT:
By signing this Electronic Signature Acknowledgment Form, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding.

By signing below, I accept the conditions of this agreement.

James R Blomgren — July 7, 2017

Signature — Date

Electronic Signature Acknowledgement

Darin Hite 6/27/17

LEGAL NAME (please PRINT name clearly) DATE

Darin Hite

Sample Signature

SCOPE:
This Acknowledgement Form applies to electronic signatures executed for policies and procedures executed as part of your HIPAA compliance program.

AGREEMENT:
By signing this Electronic Signature Acknowledgment Form, I agree that my electronic signature is the legally binding equivalent to my handwritten signature. Whenever I execute an electronic signature, it has the same validity and meaning as my handwritten signature. I will not, at any time in the future, repudiate the meaning of my electronic signature or claim that my electronic signature is not legally binding.

By signing below, I accept the conditions of this agreement.

Signature Date