INFORMATION TECHNOLOGY AND COMMUNICATION COMMITTEE MEETING

THURSDAY, DECEMBER 3, 2015
5:00 P.M.
MINUTES

MEMBERS PRESENT: Commissioners Mike Hosey, Jim Osieczonek, Kent Austin, Brian Lautzenheiser, Barbara Rogers and Howard Spence

ALSO PRESENT: Commissioner Blake Mulder, Jeff Parshall and John Fuentes

The December 3, 2015 regular meeting of the Information Technology and Communication Committee was called to order at 5:00 p.m. by Chairperson Hosey.

Commissioner Rogers moved to approve the minutes of the November 5, 2015 meeting, as presented. Commissioner Lautzenheiser seconded. Motion carried.

Technical Services Director Parshall was present to discuss the County's Health Insurance Portability and Accountability Act (HIPAA) Security and Compliance Plan (attached). The Compliance Plan incorporates several current County policies, adds additional technological security aspects regarding protected health insurance and provides a framework for reporting potential breaches of such information. Discussion held.

Commissioner Austin moved to recommend approval of the HIPAA Security Rule and Compliance Plan to the Board of Commissioners. Commissioner Rogers seconded. Motion carried.

Based on correspondence with Commissioner Spence, a sample of a Certificate of Appreciation that could be issued in lieu of a resolution was presented for discussion. Discussion held, centered around how such a certificate would be utilized and who the signatories would be. The consensus of the Committee was that such a certificate would be beneficial for individual Commissioners to be able to issue on their behalf. Further discussion held.

Commissioner Austin moved to direct the Controller to develop a Certificate of Appreciation template to be utilized by individual Commissioners that could be issued on their behalf for consideration by the Committee. Commissioner Spence seconded. Motion carried.

It was reported that the County is currently receiving quotes to upgrade the capacity of the County's internet and the connection to Delta Township. Based on the quotes received and the project budget, a vendor is anticipated to be identified in January 2016.

Commissioner Rogers discussed the possibility of enhancing the County's Geographic Information System (GIS) map data to include available river access locations. Mr. Parshall will find out if the data is currently available from another source that could be incorporated into the County's GIS or would need to be identified and acquired.

Commissioner Austin moved to adjourn the meeting at 5:39 p.m. Commissioner Rogers seconded. Motion carried.

The next regularly scheduled meeting of the Information Technology and Communication Committee is tentatively scheduled for Thursday, January 7, 2016, at 5:00 p.m. or 10 minutes following the adjournment of the Public Safety Committee meeting, whichever is later, in the Sheriff's Training Room located at 1025 Independence Blvd., Charlotte, MI 48813.

Mike Hosey, Chairperson

Eaton County Technology Services Policies and Compliance Guide Relating to the HIPAA Security Rule

November 2015

Table of Contents

Introduction

Scope: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule contains standards and implementation specifications for administrative, technical, and physical safeguards for electronic protected health information (PHI) held in any electronic device by a HIPAA covered entity. Implementation of policies and procedures to support the standards and specifications is required. The rules have been strengthened over time. For example, the 2009 HITECH ACT required the Breach Notification Rules and other enhancements to HIPAA that were intended to enhance public confidence in the privacy of patient information as health care providers increased their use of electronic health record (EHR's). Many of the HITECH enhancements are embodied in new regulations issues on January 25, 2013 ("the Final Rule").

Source: The HIPAA Security Rule is 45 CFR Parts 160, 162, and 164, *Health Insurance reform: Security Standards; Final Rule*, February 20, 2003, which may be downloaded as a PDF formatted file over the Internet at the Web address http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf. A Federal Register reference to the 2013 HITECH update can be found at: https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the

Every Agency Is Unique: One of the foundations of the HIPAA Security Rule is that each agency under the rule is different and will need to respond to the details of the rule differently, according to its own background and capabilities. Eaton County is committed to complying with the rule and developing the procedures necessary to support its security policies, based on its own business processes and characteristics.

Required and Addressable Implementation Specifications: Of the implementation specifications, some are required and some are Addressable. The Required items must be met as specified, while agencies can decide how best to meet Addressable items, based on their own context. If an Addressable item is not implemented as stated in the rule, Eaton County will perform the analysis and documentation necessary to justify its actions.

Risk Assessment: Central to the analysis required by the Security Rule is risk assessment of information security. Decisions about what should be done to be in compliance with the HIPAA Security Rule will be supported by an assessment of the information security risks that exist at Eaton County. The process identified in the preamble to the HIPAA Security Rule is described by the National Institute of Standards and Technologies in their document *Risk Management Guide for Information Technology Systems* (NIST SP800-30, available at: http://csrc.nist.gov/publications/PubsSPs.html#800-30).

Flexibility: As required in the flexibility provisions in Security Rule §164.306(b), Eaton County will take measures to manage security by considering not only risk assessment, but also the costs of various measures, the size of the agency, and the hardware and software security capabilities.

Culture: The establishment of a culture of privacy and security supported by policies and procedures is an essential step in creating a successful security program. Eaton County is committed to having sufficient policies and procedures in place to support a culture of privacy and security, and the workforce that works within the Eaton County culture.

Security Management Process: The first action item listed in the Security Rule's safeguards is to establish a Security Management Process that includes risk analysis and a regular periodic assessment of security (among other requirements). Security is not a one-time event – it is a process that requires maintenance and attention for success. The policies included here will also need to be revisited on a regular basis to ensure that they meet the needs of the agency and provide the necessary protection of health information security in an environment where new threats are discovered on nearly a daily basis.

Safeguards: Administrative safeguards in the Security Rule include a security management process, workforce security policies and procedures, information access management policies and procedures, training and awareness requirements, security incident procedures, contingency and disaster plans, periodic evaluation requirements, and Business Associate contract requirements. Physical safeguards include physical access controls, workstation use and security policies and procedures, and device and media (i.e., disks, tapes, etc.) controls. Technical safeguards include access controls, audit controls and mechanisms,

data integrity controls, entity authentication, and transmission security. In addition, there are sections for organizational and documentation requirements.

Electronic and Non-Electronic Information: While the Security Rule applies only to information that is held electronically, the rule's concepts should be used to support information security for non-electronic information wherever possible as well, since the principals involved are sound and should be considered for all kinds of protected health information.

Justification and Documentation: Eaton County is committed to the process of thorough analysis, justification, and documentation required for compliance with the HIPAA Security Rule. Any actions taken by Eaton County relating to information security will be properly justified through analysis and fully documented.

This Document

This document provides a reference tool, in the compliance guide in the section following, to show how Eaton County meets its obligations under the HIPAA Security Regulation, by listing the requirements in the regulation and identifying which policies support those requirements. The sections following the guide detail the policies themselves. A glossary is included, followed by sample forms for establishing and terminating access to computer systems.

Guide to Eaton County Compliance with the HIPAA Security Regulation

This guide is intended to assist with compliance with the Health Insurance Portability and Accountability Act Security regulation by identifying the policies and documents that ensure compliance with HIPAA Security standards. Compliance with the HIPAA Security regulation is required.

This guide is organized using the HIPAA Security Standards Final Rule as a template. The final rule is organized by General Rules, Administrative Safeguards, Physical Safeguards, Technical Safeguards, Organizational Requirements, and Polices & Procedures and Documentation Requirements. Each section describes the HIPAA requirement as stated in the Federal Register Final Rule and describes how Eaton County is meeting this requirement, by the inclusion of Compliance Statements and References to policies. In addition the reference to the Federal Register section is provided and each requirement is identified as Required (R) or Addressable (A).

I. General Rules

I. General Rules - §164.306

(a) *General requirements*

Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information [PHI] the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

References: All HIPAA Security Policies

(b) *Flexibility of approach*

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to

reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic PHI.

(c) *Standards*

A covered entity or business associate must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.

(d) *Implementation specifications*

In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word ''Required'' appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word ''Addressable'' appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard is adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) *Maintenance*

Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.

References: Policy 2.4 and Policy 2.6

II. Administrative Safeguards

II. **Administrative Safeguards** - § 164.308

(a) A covered entity must, in accordance with § 164.306:

(1)

(i) *Standard*: *Security Management Process* - § 164.308(a)(1)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

Reference: Policy 2

(ii) Implementation Specifications

(A) Risk Analysis (R)

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Reference: Policy 2.2

(B) Risk Management (R)

Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Reference: Policy 2.2

(C) Sanction Policy (R)

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Reference: Eaton County Personnel Policies and Practices Manual

(D) Information System Activity Review (R)

Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Reference: Policy 2.4

(2) *Standard: Assigned Security Responsibility* – 164.308(a)(2)

Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. **Reference: Policy 2.1**

(3)

(i) *Standard: Workforce Security* – § 164.308(a)(3)

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

References: Policy 1 and Policy 3

(ii) Implementation Specifications

(A) Authorization and/or Supervision (A)

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Reference: Policy 1.1

(B) Workforce Clearance Procedure (A)

Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

References: Policy 1.1 and Policy 3.1

(C) Termination Procedures (A)

Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

Reference: Policy 3.2

(4)

(i) *Standard: Information Access Management* – § 164.308(a)(4)

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part [the Privacy Rule].

Reference: Policy 3

(ii) Implementation Specifications

(A) Isolating Health Care Clearinghouse Function (R)

If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Compliance Statement: Eaton County does not engage in Clearinghouse operations. This section does not apply to Eaton County.

(B) Access Authorization (A)

Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Reference: Policy 3.1

(C) Access Establishment and Modification (A)
Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
Reference: Policy 3

(5)

(i) *Standard: Security Awareness and Training* – § 164.308(a)(5) Implement a security awareness and training program for all members of its workforce (including management).
Reference: Policy 1.2

(ii) Implementation Specifications

(A) Security Reminders (A) Periodic security updates.
Reference: Policy 1.2

(B) Protection from Malicious Software (A)
Procedures for guarding against, detecting, and reporting malicious software.
Reference: Policy 1.2

(C) Log-in Monitoring (A)
Procedures for monitoring log-in attempts and reporting discrepancies.
Reference: Policy 1.2

(D) Password Management (A)
Procedures for creating, changing, and safeguarding passwords.
Reference: Policy 1.2

(6)

(i) *Standard: Security Incident Procedures* – § 164.308(a)(6) Implement policies and procedures to address security incidents. **Reference: Policy 2.3**

(ii) *Implementation Specification*: Response and Reporting (R) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity; and document security incidents and their outcomes. **Reference: Policy 2.3**

(7)

(i) *Standard: Contingency Plan* – § 164.308(a)(7)

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

Reference: Policy 4

(ii) Implementation Specifications

(A) Data Backup Plan (R)

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

Reference: Policy 4.1

(B) Disaster Recovery Plan (R)

Establish (and implement as needed) procedures to restore any loss of data.

Reference: Policy 4.2

(C) Emergency Mode Operation Plan (R)

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Reference: Policy 4.2

(D) Testing and Revision Procedure (A)

Implement procedures for periodic testing and revision of contingency plans.

Reference: Policy 4.2

(E) Applications and Data Criticality Analysis (A)

Assess the relative criticality of specific applications and data in support of other contingency plan components.

Reference: Policy 4.2

(8)

(i) *Standard: Evaluation* – § 164.308(a)(8)

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. **Reference: Policy 2.6**

(b)

(1) *Standard: Business Associate Contracts and Other Arrangements* – § 164.308(b)(1) A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

Reference: Policy 3.9

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)I, when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)I are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with

the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) *Implementation Specification:* Written Contract or Other Arrangement (R)
Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).
Reference: Policy 3

III. Physical Safeguards

III. <u>Physical Safeguards</u> – § 164.310
A covered entity must, in accordance with § 164.306:
(a)

(1) *Standard: Facility Access Controls* – § 164.310(a)
Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Reference: Policy 3.8

(2) Implementation Specifications

(i) Contingency Operations (A)
Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
Reference: Policy 3.8

(ii) Facility Security Plan (A)
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Reference: Policy 3.8 and Policy 5

(iii) Access Control and Validation Procedures (A)
Implement 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.

Reference: Policy 3.8

(iv) Maintenance Records (A)

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).

Reference: Policy 3.8

(b) *Standard: Workstation Use* – § 164.310(b)

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Reference: Policy 1.3

(c) *Standard: Workstation Security* – § 164.310(c)

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

References: Policy 1.3 and Policy 3.8

(d)

(1) *Standard: Device and Media Controls* – § 164.310(d)

Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

References: Policy 3 and Policy 4

(2) Implementation Specifications

(i) Disposal (R)

Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

References: Policy 3.7

(ii) Media Re-use (R)

Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Reference: Policy 3.7

(iii) Accountability (A)

Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Reference: Policy 3.7

(iv) Data Backup and Storage (A)

Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Reference: Policy 4.1

IV. Technical Safeguards

IV. Technical Safeguards - § 164.312

A covered entity must, in accordance with § 164.306:

(a)

(1) *Standard: Access Control* – § 164.312(a)

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

References: Policy 1.1 and Policy 3

(2) Implementation Specifications

(i) Unique User ID (R)

Assign a unique name and/ or number for identifying and tracking user identity.

Reference: Policy 3.3

(ii) Emergency Access Procedure (R)

Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Reference: Policy 3.3

(iii) Automatic Logoff (A)

Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

References: Policy 3.3

(iv) Encryption and Decryption (A)

Implement a mechanism to encrypt and decrypt electronic protected health information.

References: Policy 3.6 and Policy 3.7

(b) *Standard*: *Audit Controls* – § 164.312(b)

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. **References: Policy 2.4**

(c)

(1) *Standard: Integrity* – § 164.312(c)

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

References: Policies 3.3, 3.4, 3.5, and 3.6

(2) *Implementation Specification*: Mechanism to Authenticate Electronic Protected Health Information (A)

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. **Reference: Policy 3.6**

(d) *Standard: Person or Entity Authentication* – § 164.312(d)

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Reference: Policy 3.3

(e)

(1) *Standard: Transmission Security* – § 164.312(e)

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

References: Policies 3.3, 3.4, 3.5 and 3.6

(2) Implementation Specification

(i) Integrity Controls (A)

Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

References: Policies 3.3, 3.4, 3.5 and 3.6

(ii) Encryption (A)

Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

References: Policies 3.3, 3.4, 3.5 and 3.6

V. Organizational Requirements

V. <u>Organizational Requirements</u> - § 164.314 (a)

(1) *Standard: Business associate contracts or other arrangements*

Reference: Policy 3.9

(i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—

(A) Terminated the contract or arrangement, if feasible; or

(B) If termination is not feasible, reported the problem to the Secretary.

(2) Implementation Specifications

(i) *Business associate contracts*

The contract between a covered entity and a business associate must provide that the business associate will—

(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality,

integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(ii) *Other Arrangements*

(A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—

(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

(2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of (b)business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph

(a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

(C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(1) *Standard: Requirements for group health plans*

Reference: None Required

Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) *Implementation Specifications (R)*

The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

VI. Policies and Procedures and Documentation

VI. Policies and Procedures and Documentation - § 164.316

A covered entity must, in accordance with § 164.306:

(a) *Standard: Policies and Procedures* – § 164.316(a)

Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

Reference: All HIPAA Security Policies

(b)

(1) *Standard: Documentation* – § 164.316(b)

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

Reference: Policy 2.5

(2) Implementation Specifications

(i) Time Limit (R)

Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

Reference: Policy 2.5

(ii) Availability (R)

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Reference: Policy 2.5

(iii) Updates (R)

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Reference: Policy 2.5

Incident Response Plan

If the security of unsecured PHI is breached, the Plan shall provide notice within the time period prescribed by law after the breach is discovered to the affected individual(s), HHS and the media as described below.

I. Definitions

The following definitions apply for purposes of the Plan's breach notification procedures:

1. *"Unsecured"* PHI is all PHI except ePHI secured through encryption, and ePHI or paper PHI that has been destroyed. HHS has issued guidance prescribing acceptable encryption and destruction technologies and methodologies for this purpose.

2. *"Breach"* means the unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the privacy or security of the information. In order for a breach to occur, the acquisition, access, use or disclosure must be in violation of the HIPAA privacy rules.

3. *"Discovery"* occurs as of the first day on which the breach is known or by exercising reasonably diligence would have been known to the Plan, or if earlier, the day on which any workforce member (e.g., employee, volunteer, trainee, etc.) or other agent has knowledge of the breach or by exercising reasonable diligence would have knowledge (except for the individual who committed the breach).

4. *"Time period prescribed by law"* means without unreasonable delay and in no case later than 60 calendar days. Sixty calendar days of the breach should be considered an outer limit and depending on the circumstances, it may be an unreasonable delay to wait until the 60th day to provide notification.

II. Other Issues to Consider Before Breach Notification is Required

1. *No notification if low probability of compromise*. A breach of unsecured PHI is presumed unless the Plan demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk PHI has been mitigated.

The Plan should conduct an assessment to determine if the low probability standard is met and should document the determination.

2. *Exceptions*. If the Plan discovers a breach of unsecured PHI but it falls within one of the following three exceptions, no notification is required:

a. First, any unintentional acquisition, access or use of PHI by a workforce member (employee, volunteer, trainee, etc.) or person acting under the authority of a covered entity or business associate, if the acquisition, access or use was made in good faith and within the scope of the person's duties and does not result in further use or disclosure in violation of the privacy rules. For example, a co-worker mistakenly sends an email with PHI to another co-worker who opens it in the normal course of business but then deletes it and notifies the first employee.

b. Second, an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another similarly situated person authorized to access PHI at the same covered entity or business associate and the information is not further used or disclosed in violation of the HIPAA privacy rules. For example, an employee of business associate for health plan A is working on-site at Plan Sponsor and Plan Sponsor's benefit manager inadvertently discloses PHI to the employee regarding health plan B.

c. Third, a disclosure of PHI where a covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, two Jane Smiths work for the same employer. A Human Resources employee provides an enrollment form or explanation of benefits regarding the health plan to the wrong Jane Smith, recognizes the error and immediately takes back the document.

III. Notification Steps

If unsecured PHI has been breached and a determination has been made that there is a significant risk of harm and no exception applies, the affected individual(s), HHS and the media should be notified as described below.

1. Individual Notice

The affected individual(s) should be notified within the time period prescribed by law after discovery of the breach.

a. *Content.* The content of the individual notice must be written in plain language and must include the following:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what the Plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, email address, website or postal address.

A sample notice is attached as Appendix 4.

vi. See Appendix 5 for sample.

b. *Method of Notice*

i. Generally, the individual notice should be provided in writing by first-class mail to the individual's last known address. If multiple affected individuals reside at the same address, one notice can be sent.

ii. Alternatively, written notice may be in the form of email provided the individual agrees to receive electronic notice and such agreement has not been withdrawn.

iii. If the individual is a minor or legally incapacitated, notice to the parent or personal representative is acceptable.

iv. If the individual is deceased, notice must be sent to the last known address of the next of kin.

v. If the Plan does not have sufficient contact information for some or all of the affected individuals or if some of the notices are returned as undeliverable, substitute notice should be provided to the unreachable individuals in a manner reasonably calculated to reach them. For example, if the Plan does not have the individual's last known address, but has the individual's email or telephone number, notice can be provided electronically or by phone without the individual's consent. Posting a notice on Employer's website may also be appropriate.

If the Plan has insufficient contact information for ten or more affected individuals, the Plan must either post a conspicuous notice on the home page of Employer's website for at least 90 days or a conspicuous notice must be made in major print or broadcast media in the geographic area(s) where the affected individuals likely reside. The notice must include a toll-free telephone number that

remains active for at least 90 days for individuals to call regarding the breach.

vi. If the Plan determines that because of imminent possible misuse of the unsecured PHI, immediate notice is necessary, immediate contact such as by telephone can be made in addition to the normal individual notice which is required.

2. **HHS Notice**

a. *Breaches involving less than 500 individuals.* The Plan must maintain a log or other documentation of the breaches and submit the information annually to HHS for breaches occurring during the preceding calendar year. The information will be required to be submitted within 60 calendar days after the end of each calendar year. The information required will be specified by HHS on its website (HHS.gov). The internal log must be kept for six years. A sample log to use for this purpose is attached as Appendix 3.

b. *Breaches involving 500 or more individuals*. The Plan must notify HHS immediately by following instructions on the HHS website (HHS.gov) and HHS will identify the Plan on its website. For this purpose, "immediately" means contemporaneously with the individual notice(s).

3. **Media Notice**

Notice to the media is only required where a breach of unsecured PHI is reasonably believed to affect more than 500 individuals in a state. In this circumstance, the Plan must provide notice to prominent media outlets, such as a general interest newspaper with daily circulation covering the area where the affected individuals live.

a. The same content as the individual notice must be provided and within the same timeframe.

b. The notice can be in a form of a press release.

IV. Business Associates

1. If a business associate discovers the breach, it must notify the Plan without unreasonable delay and within any time period prescribed by the business associate agreement which shall generally be in no event be later than 60 days after discovery (but see last sentence of this paragraph). For this purpose, "discovery" means the first day on which the breach is known to the business associate or by exercising reasonable diligence would have been known to the business associate. A business associate will be deemed to have knowledge of a breach if the breach is known or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is an employee, officer, subcontractor or other agent of the business associate. However, if the business associate is acting as an agent for the covered entity, the business associate must notify the covered entity as soon as possible because the business associate and covered entity are treated as one for purposes of the 60-day time limit described in Section IV(A)(4).

   The notification must include identification of each individual whose unsecured PHI has been or has reasonably believed to have been breached and any other available information in its possession which the Plan is required to include in the individual notice.

   a. The Plan and the business associate may agree, pursuant to the business associate agreement, that the business associate will assume the notice obligation on behalf of the Plan in the following circumstances.

      i. Where a breach of unsecured PHI was committed by the business associate or an employee, officer, subcontractor or other agent of the business associate or is within the unique knowledge of the business associate, as opposed to the Plan, the parties may agree pursuant to the business associate agreement that the business associate will provide the notice to the affected individuals. However, in this situation, the parties may further agree that the Plan shall have the right to promptly review and approve of any

notices before sent and that such approval shall not be unreasonably withheld.

ii. Where a breach involves more than 500 individuals and where the breach was committed by the business associate or an employee, officer, subcontractor or other agent of the business associate or is within the unique knowledge of the business associate, as opposed to the Plan, the parties may agree pursuant to the business associate agreement that the business associate shall provide notice to the media. Again, the parties may further agree that Plan shall have the right to promptly review and approve of any notice before sent and that such approval shall not be unreasonably withheld.

b. Where required by the business associate agreement, the business associate shall maintain its own log of breaches of unsecured PHI with respect to the Plan and shall submit the log to the Plan within 30 days following the end of each calendar year so that the Plan may report the breaches to HHS.

V. Law Enforcement

If any law enforcement individual indicates to the Plan or a business associate that a breach notification would impede a criminal investigation or cause damage to national security, the covered entity or business associate shall delay in providing the notice by up to 30 days from the date of the law enforcement official's statement unless a longer time period is specified in any written document supplied by the law enforcement official.

Policy 1. Workforce Compliance with HIPAA Security Provisions

Purpose

The purpose of the policy on Workforce Compliance with HIPAA Security Provisions is to ensure that the Eaton County workforce complies with all elements of the HIPAA Security Rule and its related policies, as called for in §164.306(a)(4). The security of protected health information is of critical importance to the agency and must be ensured at all times. All workforce members must be made aware of the importance of the confidentiality, integrity, and availability of electronic protected health information (PHI). Workforce compliance is also addressed in the Mobile Data Management Policy 6, Electronic Mail Policy 7, Acceptable Use Policy 8, and Password Policy 9.

Policy

1.1 Workforce Authorization and Clearance

Eaton County shall adopt procedures to ensure that all members of the workforce have appropriate access to electronic PHI and do not have unnecessary or inappropriate access to electronic PHI. Procedures shall be established to ensure that all workforce members working with electronic PHI or working in areas where electronic PHI is accessible shall be authorized to do so and/or shall be supervised while doing so. For instance, contractor or service personnel needing access to areas where electronic PHI is accessible should be known to the agency and granted access and/or supervised accordingly.

1.2 Information Security Awareness and Training

Eaton County shall establish an Information Security Awareness and Training Program for the purpose of ensuring that all workforce members, including management, are aware of Eaton County's security policies and procedures and general principles of information security.

Each member of the workforce shall receive appropriate training in HIPAA and information security policies and procedures:

1. Prior to being allowed to access or use electronic PHI.
2. When their responsibility is increased.

3. When they are promoted or reassigned.
4. When systems in use change.
5. When security policies and procedures change.
6. On a continuing education basis at least annually.

The training program shall include:

1. Periodic security updates (such as logon reminders, periodic e-mails, newsletter entries, posters, etc.).
2. Procedures for guarding against, detecting, and reporting malicious software (such as worms, viruses, Trojan horses, etc.).
3. Procedures for monitoring log-in attempts and reporting discrepancies (such as what to do if your log-in does not work properly).
4. Procedures for creating, changing, and safeguarding passwords (such as how often to change them, good password lengths and character combinations, etc.).
5. Documentation of all training activities performed, including attendance.

1.3 Workstation Use

On-the-job e-mail and Internet access are powerful tools that can help Eaton County staff accomplish their work more efficiently. As with any of Eaton County's limited resources, Internet access and e-mail services are made available to staff primarily for business use. However we recognize that from time to time, staff may need to use these resources for personal reasons to balance demands between their work and personal lives. As such, employees may use Eaton County e-mail and Internet resources for both business and certain non-business purposes subject to the following:

1. Eaton County e-mail and Internet services are the property of Eaton County. Use of these resources whether in the office or from a remote connection, is not private.
2. Non-business use of these resources must be governed by good judgment and restraint, and must be limited to non-work time, i.e. before or after work or during lunch hour.
3. Eaton County network and computing resources must be available for business use at all times. Management will limit non-business use if it interferes with the overall availability or cost of the services or with the productivity of individual employees.

4. Eaton County can and will monitor individual use of network services including visits to specific websites. Those who use Eaton County resources to access web sites containing sexually explicit material or content that could be construed as hostile or inconsistent with Eaton County policies and values, may be subject to disciplinary action, up to and including dismissal. Employees who question whether a particular site is prohibited should check with their supervisor.
5. Eaton County e-mail and Internet services are business tools. They must not be used to send or forward threatening or harassing messages or chain letters, or to express personal opinions on behalf of the Bureau in on-line forums.
6. Staff must obtain the approval of the Eaton County Systems Administrator before downloading pictures, screensavers, messenger software from websites such as AOL, Yahoo, Google, MSN, or any other software.
7. Users may not share their log-in or access codes or passwords with others and may not allow others to use their workstations except as allowed in an approved business process.
8. Protected health information may not be sent, copied, or removed from a workstation by any method except as part of an approved business process.
9. Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate business or healthcare reason to access that information, to the extent practicable.

Policy 2. Information Security Management Process

Purpose

The purpose of the Information Security Management Process policy is to establish requirements for an Information Security Management Process for Eaton County. Such a process is required by the HIPAA Security Rule §164.308(a)(1) as a means of managing the security of PHI now and over time. The process includes the following topics:

Policy

2.1 Assigned Security Responsibility

Eaton County will assign responsibility for all matters relating to the safeguarding of health information to a HIPAA Security Officer. This individual will be responsible for ensuring that all PHI in electronic form is protected against reasonably anticipated threats or hazards to the security and integrity of PHI, and against reasonably anticipated improper uses and disclosures under the Privacy Rule.

The Security Officer will:

1. Ensure that all policies and procedures required by the HIPAA Security Rule are established and maintained over time.
2. Be responsible for monitoring the appropriate and consistent implementation of policies and procedures.
3. Ensure that all members of the workforce, contractors, and business associates are aware of and abide by the policies and procedures.
4. Be responsible for the investigation of information security incidents and/or breaches.
5. Ensure that any security weaknesses discovered in the course of security incidents or security evaluations will be prioritized for correction and corrected.
6. Ensure that analyses and documentation required by the HIPAA Security Rule and/or Eaton County's security policies and procedures are carried out fully and completely.

2.2 Risk Analysis and Management

Eaton County shall establish procedures for risk analysis and assessment according to HIPAA Security Rule §164.308(a)(1). Such procedures shall include the conduct of an accurate and thorough assessment of the potential risks and vulnerabilities to PHI held by the agency. Risk analysis and assessment shall be carried out using a process that substantially conforms to the process defined in the National Institute of Standards and Technology (NIST) Special Publication 800-30, "Risk Management Guide for Information technology Systems" (document available at: http://csrc.nist.gov/publications/PubsSPs.html#800-30).
Risks shall be mitigated and managed by Eaton County to the best of its abilities within reasonable constraints of cost, staff ability, and hardware and software capabilities. Technology Committee with Technology Services staff and other program staff meets at least twice a year to discuss risk analysis and other Technology Services concerns.

2.3 Information Security Incident Procedures

Eaton County shall develop procedures for the reporting, processing, and response to suspected or known information security incidents, in order to investigate, mitigate, and report such incidents, so that security violations may be reported and handled promptly, using a known, orderly process. Such procedures will be made known to all workforce members. Procedures shall follow the agency's usual incident handling procedures and, as practicable, incorporate recommendations described in National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide" (document available at: http://csrc.nist.gov/publications/PubsSPs.html#800-61).

2.4 Information Systems Usage Audits and Activity Reviews

It is the policy of Eaton County to use, to the extent practicable, procedures and available technologies to record and examine activity in information systems holding PHI in order to discover and facilitate investigations into information security incidents, and provide information for input to the agency's security management process. The level of detail to be audited will be set as part of the overall information systems risk management program.
As systems are modified and expanded, abilities to audit access in greater detail shall be pursued where practicable and according to any risk mitigation plan in place.
Eaton County shall establish procedures to conduct the periodic review of the agency's internal security controls. Such controls may include, for example:

1. Logs produced by firewall or system monitoring applications
2. Access reports and other documentation provided by application programs in use
3. System security status reports
4. Incident tracking systems and procedures
5. Sign-in logs for service personnel.

Such reviews of information system activity shall be sufficient to determine the effectiveness of security procedures and controls, and discover any security issues that may not be addressed by the procedures or controls in place.

2.5 Documentation for HIPAA

It is the policy of Eaton County to document any policies and procedures implemented under the requirements of the HIPAA Security Rule.
The agency shall also document any actions, activities, and assessments required to be performed under the Rule, or under the requirements of agency policies enacted in support off the HIPAA Security Rule.
Documentation may be in electronic or paper format.

Documentation under this policy shall be maintained for at least six years from the date of issue or the date of last effect, whichever is later.

Relevant documentation shall be made available to the people responsible for implementing policies and procedures enacted under the HIPAA Security Rule. Documentation shall be periodically reviewed and updated as needed or in response to environmental or operational changes affecting the security of electronic PHI.

2.6 Information Security and Compliance Evaluation

Eaton County shall perform regular, periodic evaluations of the information security- related policies and procedures in place at the agency to ensure that they continue to meet the requirements of the HIPAA Security Rule. The period of review shall be determined according to the agency's information systems risk analysis and consideration of best practices.

Evaluations shall also be performed whenever there is a change in environmental or operational conditions that may affect the security of electronic protected health information. For example, such changes would include (but not be limited to):

1. The emergence of a significant new threat such as
    a) Terrorist attacks of facilities
    b) The emergence of new type of computer virus
2. Significant change in information systems such as
    a) The installation of a new computer system or
    b) Installation of new services such as wireless or remote access.

Evaluations shall include the review of relevant information security-related policies and procedures, and shall be documented for compliance with the HIPAA Security Rule and to provide direction to the agency in the execution of its security plans.

Policy 3. Information Access Management and Control

Purpose

The purpose of the Information Access Management and Control policy is to ensure that all members of the workforce have access to the systems and information appropriate to their job functions, and to ensure that inappropriate access is prevented. The policy includes the following topics

Policy

3.1 Information Access Management

Eaton County shall institute procedures for granting access to electronic PHI (for example, through access to a workstation, transaction, program, process or other mechanism) to authorized persons. Such access shall be granted only within the bounds of the "minimum necessary" requirements of the HIPAA Privacy Rule.

The agency shall institute procedures to establish, document, review, and modify a user's right of access to a workstation, transaction, program, process or other mechanism. Access lists will be reviewed regularly. **Reference Appendix 2**.

Supervisors are required to complete the following information and submit it by e- mail to the Eaton County Technology Services department (MakingITHappen@EatonCounty.org) in order to establish or modify access:

1. First Name
2. Middle Name
3. Last Name
4. Title or New Title
5. Phone Number of Extension
6. Department
7. Location
8. Is a PC in the location desired?
9. Specify Software to be used (for example: Microsoft Office, Internet Access, New World Systems LOGOS.net, LaserFiche, etc.)
10. Justification for Internet Access, if desired

3.2 Termination Procedures

Eaton County shall adopt procedures to ensure that terminated workforce members or workforce members whose access to electronic PHI is restricted shall have physical and/or system access privileges removed and shall surrender any keys or other objects that allow access. In addition, combination locks and alarm system codes known by such workforce members shall have their combinations or codes changed.

Procedures shall identify:

1. The parties to be involved in termination activities
2. The steps to be taken in the process of termination
3. The timing of termination activities, such as coordination of notice of termination with removal of access to systems and networks.

Supervisors are required to complete the following information and submit it by e- mail to the Eaton County Technology Services department as soon as termination information is available:

1. First Name
2. Middle Name
3. Last Name
4. Title
5. Phone Number of Extension
6. Department
7. Location
8. Termination Date and Time
9. Are electronic files needed from the terminated user's accounts?
10. Specify Needed Files (Note that files will not be available after deletion so please describe here any and all files desired for retention)

3.3 Technical Access Control and Authentication

It is the policy of Eaton County to limit, through technical means as practicable, access to electronic protected health information (PHI) to only those persons or software programs that have been properly granted access rights.

Eaton County follows the authentication rules created by the CJIS (Criminal Justice Information Services). Please refer to Policy Area 5.6 in the CJIS security policy rules at: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.

3.4 Technical Perimeter Security

It is the policy of Eaton County to establish technical perimeter security controls, such as properly configured routers and firewalls and any other devices related to Eaton County's computer network security, in order to protect the electronic protected health information (PHI) held within the agency's systems and allow access where appropriate.
Wireless network access shall be allowed only in approved locations and shall be configured so as to protect the security of the agency's perimeter and its electronic PHI.

3.5 Remote Access

Eaton County allows remote access to electronic networks containing protected health information (PHI) only with approved and proper security measures.
Any remote access requests must be approved by the Eaton County Technology Services Director, Eaton County Controller. All requests must show the need for remote access. The Technology Services Director will ensure that adequate authentication and safeguards in place.
Vendor remote access to systems must be approved by the Technology Services Department and may be performed only by a defined procedure and under the supervision of the Technology Services Director. **Reference Policy 6.**

3.6 Data Encryption and Integrity

It is the policy of Eaton County to encrypt electronic PHI at rest or in transmission where a risk analysis indicates that such encryption is necessary to protect the security of PHI. Such risk analysis shall consider the probability and criticality of risks to security.

1. Technical procedures shall be instituted to provide encryption and decryption capabilities where deemed necessary by the risk analysis.

2. Unencrypted e-mail or e-mail attachments to outside of Eaton County must not contain any PHI unless required by a city or state agency requesting specific information as part of a regular Eaton County process.
3. Electronic transmission of PHI outside of Eaton County by other than e-mail may only be as part of regular Eaton County processes, such as claims submission, and must be secured through encryption.
4. Portable devices such as laptop computers, tablet computers, “USB memory sticks”, and other devices that are easily lost or stolen shall use encryption technologies to protect PHI resident on those devices.
5. Data Backup devices and programs shall encrypt the contents of files containing any PHI, if feasible with the technologies in use at Eaton County.
6. Procedures shall be developed to ensure that encrypted electronic PHI at rest shall be accessible by approved personnel in an emergency situation.

It is the policy of Eaton County to use, to the extent practicable, available technologies to corroborate that electronic protected health information held by Eaton County has not been altered or destroyed in an unauthorized manner. New systems procured should ensure the integrity of the information stored on them to the extent practicable, using readily available technologies.

3.7 Electronic Information Device and Media Controls

It is the policy of Eaton County that the movement of hardware and electronic media which contain electronic PHI into and out of agency facilities shall be controlled.

There shall be procedures to record the movement, and the person responsible for the movement, of hardware and electronic media containing electronic PHI into, out of, and within agency facilities.

The disposal or reuse for another purpose of any hardware or electronic media containing electronic protected health information (PHI) shall include the destruction of any such PHI before ultimate disposal or reallocation to a new use. The destruction of electronic PHI shall be carried out by physical or electronic means that ensures the actual destruction of the information. Simply “dragging files to the trash” is not sufficient to destroy PHI. Procedures shall be defined in order to ensure the destruction of information in systems that are de-commissioned, reused, or sold.

The use of portable memory devices, such as “USB memory sticks”, for the purpose of removing PHI from Eaton County facilities is prohibited without prior approval from the HIPAA Security Officer. Any such approved devices must encrypt any PHI stored thereon.

3.8 Physical Access Controls

Equipment should be protected from fire, flood, and other natural disasters. Servers should be in locked rooms or closets with access restricted to the Technology Services department and maintenance staff only.
Security procedures shall be employed to safeguard facilities and the equipment therein from unauthorized physical access, tampering, and theft, while ensuring that properly authorized access is allowed. Such plans and procedures may include security guards at entrances enforcing sign-in by visitors, employee awareness of personnel authorized to be in areas where client information is present, access control during emergencies, staff monitoring of information system vendor personnel, and documentation of physical security modifications and maintenance.

3.9 Contracts and Memoranda of Understanding and PHI

Eaton County shall enter into written agreements with any entities that use or disclose electronic protected health information on behalf of the agency, in order to require the protection of the security of any and all such information. Such agreements shall be Business Associate Contracts or Memorandums of Understanding designed to meet the requirements of HIPAA Security Rule §164.308(b) and §164.314(a).
This policy shall not apply in the following situations:

1. When electronic PHI is transmitted to a provider for purposes of treatment

2. When electronic PHI is transmitted by a group health plan (or an HMO or health insurance issuer on behalf of a group health plan) to the plan sponsor (provided the recipient provides assurances it will safeguard the PHI)

Policy 4. Data Backup and Contingency Planning

Purpose

The purpose of the Data Backup and Contingency Planning policy is to ensure that Eaton County has a usable copy of electronically held PHI and can properly respond to emergencies or other occurrences that may damage systems containing electronic PHI, as required by HIPAA Security Rule §164.308(a)(7). The policy includes the following topics:

Policy

4.1 Data Backup

Eaton County shall develop procedures for the regular and periodic backup of electronically held health information. Backups shall be sufficient to restore damaged data with a useful duplicate.
Backup procedures shall include the following elements:

1. Definition of which file systems to back up
2. Definition of frequency of backups
3. Definition of frequency of media rotation
4. Definition of off-site storage requirements and frequency
5. Documentation and labeling of storage media
6. Regular testing of backed up data to ensure adequacy.
7. Performing backups before the movement of systems.

4.2 Contingency Planning

Eaton County shall develop procedures for the development and execution of contingency plans in order to properly respond to emergencies or other occurrences that may damage systems that contain electronic PHI, resulting in the loss of confidentiality, integrity, or availability of PHI.
Contingency plans must provide for the continued operation of essential or strategic activities and their critical systems in the event of an interruption or degradation of service.
Contingency plans should take into account the effects of short-term interruptions (such as

brief power failures) and long-term interruptions (such as a loss of facilities to fire or contamination of some kind).

Contingency plans shall include the following required elements:

1. Disaster Recovery plans and procedures, to ensure the restoration of lost data and system access, including a full range of information and activities needed to assure that the Plan will be effective and its operation will be as smooth as possible.
2. Emergency Mode Operation plans and procedures, as described in the agency's Disaster Preparedness Plan.
3. Plans and Procedures for the testing and revision of contingency plans, as described in the agency's Disaster Preparedness Plan.
4. Assessment of the criticality of applications/systems and data, in support of the other contingency plan components and information system backup policies and procedures.

Policy 5. Use of Photographic or Video Recording Devices

Purpose

The purpose of the policy on the Use of Photographic or Video Recording Devices is to ensure that Eaton County establishes procedures, such as signs prohibiting such use, to limit the use of image recording devices at agency facilities in order to limit the collection of unauthorized electronic protected health information (PHI) and protect the privacy of agency clients.

Policy

It shall be the policy of Eaton County that photographic and video recording devices not be used to capture the image, voice, or other PHI of any client except as part of an approved business process. The agency shall post notices in areas open to clients to the effect that cameras and video recorders of any type should not be used on the premises except for designated purposes in designated areas.

Policy 6. Mobile Data Management Policy – Last Revision Adopted August 2015

Purpose

The purpose of this document is to set policy as to the appropriate use, security, support of, assignment of, governance, and employee responsibilities for the use of mobile devices whether owned solely by the county or supplied by employees for any purpose germane to the business/work flow processes of the county.

Because all county employees share a common network that includes law enforcement data, mobile devices connected to the network are subject to the federal security guidelines known as CJIS (criminal justice information network). This policy, therefore, and its operational requirements will be influenced by these guidelines.

6.1 Definitions

1. Mobile Device: Any device or medium not permanently connected to the county network used for the purpose of receiving, sending, or storing information. This may include, but is not limited to, cell phones, laptops, computers, smart phones, tablets, USB thumb drives; digital storage media (CD, DVD, Thumb Drives, floppy disks, hard drives, etc.).
2. Board: The Eaton County Board of Commissioners.
3. Director: Technology Services Director.
4. Department Head: Refers to appointed department heads and elected officials.
5. County Network: Refers to the county's computer network which is further defined as a group of computers connected to each other electronically. This means that the computers can communicate with each other and that every computer in the network can send information to the others.
6. Bluetooth: A wireless technology standard for exchanging data over short distance from fixed and mobile devices. These devices must pair together to form a unique bond that allows for secure data transfer.
7. Bluetooth enabled device: A device that is capable of short-range Bluetooth wireless communication with another Bluetooth enabled device.

6.2 Responsibilities and Enforcement of this Policy

1. The Board has set forth this policy in an effort to meet departmental goals, improve employee satisfaction related to mobile devices, to improve efficiency for the department and employees by enabling the use of mobile devices, and, where appropriate, enabling those devices with access to county resources.
2. Each employee is responsible for the conditions set forth within this policy as well as any subsequent or supporting policy set forth and/or previously adopted by the county board (i.e., Acceptable Use Policy, Electronic Mail Policy).

3. Under his management for meeting the requirements set forth within this policy, and shall communicate the requirements of this policy for any and all persons that this policy applies.
4. The Director or designee shall oversee all technical aspects of enforcing this policy, including creating and updating all approval forms, recording logistical and technical information for devices, and manage and update inventory records which enable mobile devices to access county resources.
5. Information and communications used or stored on any mobile device shall be considered as important for security and records retention as any paper or digital document or database in the operation of the department, including services provided to other departments for conducting county business.
6. Violations of this policy will be subject to enforcement policies, up to and including termination in accordance with the Personnel Policy's "at will" employment clause.

6.3 Cell Phones, Smart Phones, Tablets, etc. (General)

1. All cell phones, smart phones, tablets, etc. purchased for use in any department shall be purchased in accordance with current purchasing requirements and from approved vendors as established by the County.
2. Voice/data service contracts shall follow the county's current operating practices and are therefore negotiated, agreed upon, and managed by Eaton County Technology Services. When the Department has requested a county-owned mobile device for an employee that requires a voice/data service contract, a suitable contract with all related costs to be billed to the Department.
3. The need for a county purchased mobile device, and securing all necessary funds shall be determined by the Department Head. Costs include any cost for the device, monthly service fees, licensing fees, client access licenses, and MDM (Mobile Device Management) licensing.
4. Any mobile device that connects to the county network shall be managed by MDM (Mobile Device Management) software and licensing. This includes any device that accesses resources located within the county network(s). Employees understand that this gives the Eaton County Technology Services Director and/or designee the ability to manage, copy, see, retrieve, download, install, disable, lock, change passwords, track, and wipe any device under the management platform.
5. Conditions which must be met for any mobile device to be enabled to access network resources:
    a. All employees will be provided a copy of the Mobile Device Management Policy, and will be required to abide by all policy statements within.
    b. If at any time any county-owned network resource enabled device is lost or stolen, the employee shall immediately report the loss to Eaton County Technology Services. The Director or his designee shall, in the most expedient manner available, remotely disable, lock, and/or "wipe" the device, therefore rendering the device inoperable and cancel services if the mobile device is linked to a voice/data service plan.

i. Employees shall not disable location tracking on the mobile device (also refer to the section titled *Other General Issues, bullet item 'e' for a supporting requirement*).

c. All communications (i.e., email, text) enabled devices shall be required to automatically "lock" after a reasonable period of inactivity (for instance, 5 minutes), and must be password or biometrically protected to "unlock" the device. This is to ensure that a device left unattended will not be able to access network resources or information by parties not governed by this policy.

d. All communications (i.e., email, text) shall be retained in accordance with established records retention policy for county departments. The Department Heads and employees shall be aware of the Fair Labor Standards Act (FLSA) and appropriate use of network resources for Exempt and Non-Exempt employees. Employees granted access to county email, for instance, on mobile devices shall strictly follow work schedules when replying to any email request. Replying when not at work or otherwise "not on the clock" is not authorized and therefore not eligible for overtime pay or compensation time without explicit authorization from the Department Head.

e. Employees shall access the Internet with mobile devices in a manner consistent with county practice/policy involving logging, filtering, reporting and in compliance with the county's Acceptable Use Policy, Internet Use Policy and all other applicable policies.

6.4 BYOD (Bring Your Own Device) - The department Director recognizes:

Employees may make BYOD requests to allow their personally-owned devices on the county network(s). Personal mobile devices may include, but are not limited to, smart phones, tablets, laptops, and GPS utilizing a variety of operating systems (iOS 7,, Android) and varied operating technologies (iOS, Android, Windows).

As noted earlier, in an effort to improve department service efficiency and effectiveness, the County sets forth the following policies to allow for personal technology enabled devices to access resources within the county network(s):

1. Any personal device enabled to access any resource provided within the network, and the employee given access to said resources on his/her personal device, shall adhere to all policy statements within this Mobile Device Management Policy and any supplemental departmental policies that are more stringent such as department-level SOPs (Standard Operating Procedures).
2. Any employee requesting their personal device be used to access network resources must sign the form titled Consent to Use Personally-Owned Device on County Network and have it counter-signed by their department head or direct supervisor. Upon receipt

of the consent form by Eaton County Technology Services, installation of MDM software will be coordinated directly with the employee in accordance with this policy. Employees granted access to county network resources on their personal devices shall allow the Eaton County Technology Services Director or his designee to install MDM (Mobile Device Management) software on the device for which access is granted. Employee understands this gives the Eaton County Technology Services Director and his designee the ability to manage, copy, see, retrieve, download, install, disable, lock, change passwords, track, and wipe any device under this device management platform.

3. Employee acknowledges that if lost or stolen, he/she must report the loss to the Eaton County Technology Services Director or his designee immediately to disable access to network resources.
4. Employee's personal device and/or data will not be the responsibility of the county to maintain, safeguard, backup, protect in any shape, form, or fashion.
5. All information contained on any personal device shall be considered as public record and subject to (but not limited to) freedom of information act requests, electronic discovery, investigations, and so on. Employee must provide all necessary passwords and any information requested in order to access the device by the requesting agent or agency. Failure to do so may result in disciplinary action up to and including termination of employment.
6. At no time may a personal device enabled with access to any network resource (such as email) be used by any person other than the employee granted access. (Example: If the Eaton County Technology Services Director or his designee enables your mobile device with county email, you cannot share your device with a spouse, child, friend, neighbor, colleague, etc.). Employee shall not share passwords with anyone other than those indicated in this policy.
7. Eaton County Technology Services staff will provide only necessary technical support to provide initial setup, security, MDM software, and to disable, lock, and/or wipe devices when needed to ensure the security and integrity of the network(s) for any personal mobile device. When needed, employees are encouraged to utilize the Internet (www.google.com, www.youtube.com, user groups, and their devices' manufacturer resources) for any problem resolution with their personal device.
8. Failure to meet any of the conditions set forth within this policy may result in the termination of access to network resources.

6.5 Criminal Justice Information (CJI) specific requirements

1. Bluetooth use on mobile device.
    a. This section is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the Eaton County/CJI networks with Agency owned devices. The intent of the minimum standard is to ensure sufficient protection for Personally Identifiable Information (PII) and confidential Criminal Justice Information (CJI).
    b. This section applies to any Bluetooth enabled device that is connected to an

Eaton County or Criminal Justice Agency owned device that needs to access any CJI data source.

i. Only devices that are owned by Eaton County or supported Criminal Justice Agencies will be allowed to connect to CJI data sources.

ii. No Bluetooth device shall be deployed on Eaton County equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization from Eaton County Technology Services. Any Bluetooth equipment purchase prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

iii. When pairing a Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised.

iv. If your Bluetooth enabled equipment asks for you to enter your PIN after you have initially paired it, you must refuse the pairing request and report it to Eaton County Technology Services, through the Help Desk, immediately.

v. Device Security Settings

- All Bluetooth devices shall employ 'security mode 3', which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- Use a minimum PIN length of 8. A longer PIN provides more security.
- Switch the Bluetooth device to use the hidden mode (non-discoverable)
- Only activate Bluetooth when it is needed.

vi. Security Audits

- Eaton County Technology Services may perform random audits to ensure compliancy with this policy. In the process of performing such audits, Eaton County Technology Service members shall not eavesdrop on any phone conversation.

vii. Unauthorized Use – The following is a list of unauthorized uses of Agency-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Connecting to and storing CJI on any non-authorized storage device.

viii. User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- PII, CJI and/or Eaton County Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled

devices.

- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to Eaton County Technology Services.

2. Compliance Measurements
    a. Eaton County Technology Services will verify compliance to the policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
    b. Any exception to the policy must be approved by Eaton County Technology Services in advance.
    c. Any authorized used found to have violated this policy may be subject to disciplinary action by that users agency or denied access to Eaton County supplied CJI information.

6.6 Other General Issues

1. From time to time employees approved to receive a county purchased mobile device may request a premium upgrade beyond budgeted amounts and/or currently accepted IT standards for certain requested devices. An employee with the approval of the Department Head may choose a supplemental mobile device but it will be managed in accordance with this entire policy and all costs remain the responsibility of the respective Department Head.
2. APPS (Software Applications) on mobile devices:
    a. Unless previously approved and budgeted for by the Department Head AND reviewed by the Director or his designee, no applications shall be downloaded to any device that causes a charge to be incurred, including (but not limited to) the general fund, computer fund, and so on.
    b. Mobile devices are generally capable of downloading and using APPS. The Director may at his discretion limit, or otherwise restrict, the types or size of APPS acceptable for download because they conflict with the operation of the device or other business APPS in use by the employee. Where instances of conflict exist, the Director shall provide the Department Head with information to explain the limit or restriction and will work with the department head to identify suitable alternatives.
    c. If at any point the Director discovers any downloaded APPS have the potential to compromise security to the network, the Director or his designee shall

disable, lock, and/or wipe the compromised device as soon as possible, and render it unusable for network access. If warranted, the Director will report the incident to the Sheriff's Department for supplemental computer forensic review and notify the affected Department Head of the nature of the compromise.

d. It shall be considered a violation of this policy for any device (county or personally- owned) approved for connection to the network(s) to be "hacked" resulting in any changes to the operating system provided by the manufacturer. If any unauthorized changes to the operating system of any device compromises security, this may result in permanent termination of service to the device or until such time that device audits reveal no future vulnerabilities. If warranted, the Director will report the incident to the Sheriff's Department for supplemental computer forensic review.

e. Other "for a fee" personal downloads such as Music, Videos, Movies, etc.: It is the SOLE responsibility of the employee to pay for any downloaded media of any type for which a fee is charged, for personal use, including downloading these files to a county-owned device.

    i. If county-approved APPS or other electronically stored information is "crowded out" because of a personal download, the employee must immediately remove one or more personal downloads to ensure county-approved APPS are capable of performing their intended purpose. When necessary, Eaton County Technology Services will take corrective action.

    ii. Eaton County Technology Services shall not be responsible to backup, maintain, or otherwise protect any personally downloaded application, content, music, video, movie, etc.

    iii. After all personal downloads occur, using an employee's personal iTunes (or other store) account, employees shall immediately reconnect their county- owned device to iTunes (or other store account) using their previously established county account (i.e., IS01, IS02, etc.).

f. County-owned mobile devices will be configured to use generic department accounts (i.e., IS01, IS02 rather than NNIGHBERT) in App Store, Android Market, Microsoft and other future "stores." Regardless of naming convention, these accounts will not have a county credit card associated with them. A master account will be used (i.e., iOS2020) to purchase APPS, administered by the Director. When purchased, a "redeem" code will be provided to the employee to download the APPS.

g. Remote access to network resources using any mobile device shall be subject to the requirements described in this policy. As such, this will require the installation of MDM software on the devices used for remote access.

Note: this policy will be updated as needed to reflect changes in technology, operational practices, or management and/or legislative philosophy.

Eaton County
Consent to Use Personally-Owned Device on County Network

Acknowledgement:

I acknowledge that I have read and agree to the requirements defined in the Mobile Device Management Policy and other supporting policies such as Acceptable User Policy, E-Mail Policy, and so on. Therefore, I hereby request that I be able to connect a personally-owned device to the county network.

Terms and Conditions:

1) The county makes no representation that a personally-owned device will be able to connect remotely to the county network.
2) Eaton County Technology Services will not provide support other than written instructions for connecting the personally-owned device to the county's network.
3) In compliance with the Mobile Device Management Policy, a personally-owned device that is lost or stolen will be immediately reported to Eaton County Technology Services. The Director of Technology Services, or his designee(s), will take the necessary steps to remotely wipe all data from the device, contingent upon the device being located using location tracking and/or the device being powered on.
    a. The county bears no responsibility for data loss of personal data stored on the device.
    b. Data backup of the device is the sole responsibility of the employee.
4) Information on my personally-owned device may be subject to Freedom of Information Act or discovery requests, where applicable.
5) While remote access to the county network is generally available 24/7, the county makes no warranty that such access will always be available given periodic maintenance to the network.
6) Communications may be logged/viewed by other parties, where applicable.
7) Remote access is a county offered privilege, not a right.

Employee's digital signature: Date: _____

Department Head's digital signature: Date: _____

Please <u>e-forward</u> this completed form to Eaton County Technology Services.

Policy 7: Electronic Mail Policy

POLICY

In order for government to function administratively, undergo periodic audits, provide for its legal requirements and document its heritage, it must manage its records properly. Through a collaborative process of policy development, this electronic mail policy meets the objectives stated above. Therefore, Eaton County , hereinafter referred to as County, requires its employees to retain and destroy electronic mail records that are sent and received in the course of conducting official business in accordance with an approved records Retention and Disposal Schedule. This schedule may be a general records schedule or an agency-specific schedule, both of which are approved by the Michigan Historical Center and the State Administrative Board.

The specific purpose of this policy is to provide guidance with regard to the capture, filtering, storage, use, management (organization, security, confidentiality) and disposal of electronic mail records.

SCOPE

This policy applies to all County-appointed department heads and their respective employees regardless of employment status (i.e. full-time, part-time, temporary, intern, etc.). Unless otherwise agreed upon in writing between the County Controller and the Chief Judge(s) of the Court(s) this policy shall not apply to the judiciary and its respective employees.

PROCEDURES

7.1 Definitions

- **Convenience Copies:** are copies of original records that document official County business transactions and are produced for dissemination to internal or external parties. A convenience copy may be stored in any format (i.e. paper, digital). A convenience copy shall not be considered a backup copy of the original record. A backup of the original record is created by the Information Systems Department and is stored offline and in an alternate location from the main computing facility.
- **Electronic discovery (e-discovery):** Electronic discovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline on a

particular computer or it can be done in a network. Court-ordered or government sanctioned hacking for the purpose of obtaining critical evidence is also a type of e-discovery.

- **Electronic mail (e-mail):** is a means of exchanging messages and documents using telecommunications equipment and computers. A complete e-mail message not only includes the contents of the communication, but also the transactional information (dates and times that messages were sent, received, opened, deleted, etc.; as well as aliases and names of members of groups), and any attachments. Transactional information can be found and printed or saved from the e-mail system (see Appendix A for a sample from the County's current e-mail system).

- **Freedom of Information Act (FOIA) and Litigation Coordinator:** is the County Controller and/or outside County legal counsel.

- **IT:** Information Technology. It is a common acronym used to represent the industry as well as local technology arrangements,

- **Litigation hold (also known as "preservation orders" or "hold orders"):** is a stipulation requiring the County to preserve all data that may relate to a legal action involving the County. This requirement ensures that the data in question will be available for the discovery process prior to litigation. The County must preserve records when it learns of pending or imminent litigation, or when litigation is reasonably anticipated. Litigation hold prevents spoliation (destruction, alteration, or mutilation of evidence) which can have a catastrophic impact on the defense. An attorney may issue a litigation hold letter or the County may issue a hold order internally. The order applies not only to paper-based documents but also to electronically-stored information (ESI).

- **Records:** includes general and agency-specific records, maintained in any format, which documents a County business transaction.

- **Records Retention and Disposal Schedules:** are listings of records or records series that are maintained by government agencies in the course of conducting their official business that identify how long the records must be kept, when they may be destroyed and when certain records can be sent to the Archives of Michigan for permanent preservation. In accordance with Michigan law, records cannot be destroyed unless their disposal is authorized by an approved Retention and Disposal Schedule. Retention and Disposal Schedules are developed by the Department of History, Arts and Libraries, Records Management Services, through consultation with an agency about its records. These schedules are then approved by the Michigan Historical Center and the State Administrative Board.

- **TIFF (T**agged **I**mage **F**ile **F**ormat): A widely used bitmapped graphics file format.

7.2 General Electronic Mail Guidelines

- The County provides an e-mail system to its employees and officials for conducting County business. Using this system is a privilege, not a right. The electronic records created are the property of the County, not the persons who create them.
- The County reserves the right to monitor the use of the e-mail system, make periodic technology updates to it (including replacement), and to retain or dispose of e-mail messages within the scope of this policy and general and agency-specific record retention schedules.
- The County informs employees and officials that Michigan law may require the reproduction of e-mail messages to third parties.
- The e-mail system shall not be used for any purpose the Board of Commissioners deems to be inappropriate, immoral, or illegal.
- The e-mail system may not be used for any political advocacy, including, but not limited to, campaigning for or against a candidate for any federal, state, or local elected office, implying that employee views are in any way a representation of official County policy, and areas that may violate the state of Michigan's Campaign Finance Act of 1976 (P.A. 388).
- The County reserves the right to implement appropriate filtering systems and processes to: 1) avoid sending and receiving non-productive e-mail, 2) and the elimination of potentially harmful e-mail and attachments containing computer viruses.
- E-mail records can be retained online until the allocated digital storage space (approximately 500MB) for each employee has been consumed through sending and receiving messages. Under the following conditions and procedures, additional storage space can be requested:
    - With approval from the employee's Department Head and/or immediate supervisor, employees may receive additional digital storage space if the nature and functions of their job responsibilities justify the request,
    - AND unused digital storage space is available for allocation to the employee.
        - In the event digital storage space cannot by allocated, without disrupting the storage requirements of other business systems, no additional space shall be granted. Under this condition, the Director of Information Systems will include a general plan to increase storage capacity during the next fiscal year's budget development cycle if not already planned for in the next budget.
        - However, if waiting for the next fiscal budget to be developed and adopted is unacceptable to the requesting Department Head, either the Department Head or the Director of Information Systems can submit a supplemental budget request to the Ways and Means Committee for consideration. The committee's decision shall determine if storage space will be expanded outside the County's normal budget cycle.
    - This storage policy shall be under continual review by the Director of Information Systems because of rapidly changing resource requirements and capacities.

7.3 Employee Responsibilities:

- Senders and recipients of e-mail messages shall evaluate each message to determine if they need to keep it as documentation of their role in a process that represents official County business.
- Senders are generally considered to be the person of record for an e-mail message. However, if recipients of the message take action as a result of the message, they should also retain it as a record.
- Shall evaluate the content and purpose of each e-mail message to determine which Retention and Disposal Schedule defines the message's approved retention period.

- Employees shall retain e-mail that has not fulfilled its legally-mandated retention period by: 1) printing a paper copy and filing it in an appropriate storage location, 2) printing it to an Adobe PDF © file and storing the e-mail on the County's computer network (i.e. H: drive) or transferring the PDF file into a document imaging system, 3) or printing it directly to a document imaging system as an image file (TIFF).
- Shall retain transactional information (see Appendix A for an example) with the e-mail message if there is a substantial likelihood of relevancy to litigation.
- Shall organize their e-mail messages so they can be located and used. It is recommended that employees store e-mail messages, transactional information, and attachments organized by the content or purpose of the message rather than by file type (i.e. do not organize Microsoft Word © documents together, do not organize Microsoft Excel © files together).
- Shall dispose of transitory, non-record and personal e-mail messages from the e-mail system.
- Shall dispose of e-mail messages that document the official functions of the agency in accordance with an approved Retention and Disposal Schedule. Note: Records, including e-mail, shall not be destroyed if they have been requested under FOIA, or if they are part of on-going litigation, even if their retention period has expired.
- Shall provide access to their e-mail to the FOIA or Litigation Coordinator upon request.
- Shall retain all work-related appointments, tasks and notes stored in the e-mail system, as calendar entries, for 2 years by: 1) printing a paper copy and filing it in an appropriate storage location, 2) printing it to an Adobe PDF © file and storing the e-mail on the County's computer network (i.e. H: drive) or transferring the PDF file into a document imaging system, 3) or printing it directly to a document imaging system as an image file (TIFF).
- Recognizing that e-mail messages that are sent and received using the County's e-mail system are not private, employees are encouraged to manually delete personal appointments (such as sick leave or annual leave) from the e-mail system after the event takes place.
- Convenience copies of records may be created as necessary and in support of business processes. Confidential data shall not be copied to any removable storage device (i.e. USB "storage stick") or attached to an e-mail addressed to an external account without authority from the employee's Department Head and/or immediate supervisor.

7.4 County and/or Department-Level Responsibilities

- Shall ensure that its records are listed on an approved records Retention and Disposal Schedule.
- Shall ensure that all employees with e-mail accounts are aware of and implement this policy.
- Shall notify the Information Systems Department when the accounts of former employees can be closed.
- Shall ensure that the e-mail messages of former employees are retained in accordance with approved Retention and Disposal Schedules.
- Shall notify the FOIA or Litigation Coordinator when a department or agency becomes involved in litigation or receives a FOIA request. The FOIA or Litigation Coordinator shall immediately notify the Director of Information Systems to prepare for an electronic discovery and to implement a litigation hold.
- Exceptions to the procedures in this document may be granted in writing by the Board of Commissioners.

7.5 FOIA and Litigation Coordinator Responsibilities:

- Shall work with the Information Systems Department to:
    - Identify if the records that are requested by the public are stored in e-mail, even if the public does not specifically request e-mail.
    - Notify affected employees that a FOIA or e-discovery request involving e-mail was received to prevent the destruction of relevant messages, thus creating a litigation hold.
        - The Director of Information Systems shall immediately take the necessary steps to prevent the destruction of relevant messages in compliance with a litigation hold notice.
    - Shall identify all records relevant to litigation to which the agency is a party that are stored in e-mail.
    - Ensure e-mail is retained and stored on suitable media for inspection and/or duplication in a secure environment.

7.6 Administration and Enforcement

- This policy is applicable to all departments and agencies referenced under the previous section of this policy titled SCOPE.
- In accordance with the mandates described in this policy, the Director of Information Systems, either directly or through delegation of authority to an experienced designee, shall:
    - Maintain an inventory of e-mail and/or other records storage assets including network and standalone servers, storage medium, and formats of electronically-stored information (ESI). The list of assets shall be updated at least once each fiscal year.
    - Periodically audit the capture, filtering, storage, use, management (organization, security, confidentiality) and disposal of electronic records and report notable violations of this policy to the County Controller.
    - Periodically evaluate the effectiveness of this policy through "readiness testing," including but not limited to, simulating a pre-discovery meeting seeking answers to specific IT questions relating to discovery of records based upon a pre-defined theme (i.e. contract management, sexual harassment).
    - When delegated by the Director of Information Systems, Information Systems staff shall comply with the IT Audit Policy previously adopted by the Board of Commissioners.
- As directed by the County Controller, or through a request from a department or court, the Director of Information Systems shall coordinate and schedule periodic informational training sessions to educate employees about this policy. Training material may be provided in small group sessions or made available on the County's internal shared network (Intranet) for efficient and cost-effective information dissemination.

7.7 Revision History:

- This policy was approved on 02/20/2008 by the Board of Commissioners and supersedes all earlier versions of Electronic Mail Policy's approved November 20, 2002 and December 2000.

Policy 8: Acceptable Use Policy

POLICY

8.1 Overview

This Acceptable Use Policy demonstrates a commitment to protecting the county's technology assets and access to digital data that is collected, stored, analyzed, and reported upon by employees throughout the county. County computer networks, including all host and server systems, locally or externally operated, are the property of Eaton County. These systems are to be used for business purposes in serving the interests of the county in the course of its business operations. Effectively securing our technology assets and digital data is an obligation of every employee who uses any component parts of the computer network. Therefore, employees must understand the impacts these guidelines have on their use of network and standalone resources.

8.2 Purpose

The purpose of this policy is to broadly outline acceptable use of any and all computer networks and individualized systems like personal computers, laptops, and mobile devices. Inappropriate use exposes both the county and the employee to risks that include disruptions in work processes resulting from computer viruses and other malicious software. Additional concerns include unauthorized access to, and/or the transfer of, digital data and identify theft. This policy shall be influenced by the requirements of the most current version of the Michigan Criminal Justice Information System Guidelines that mandate certain requirements as they relate to LEIN/NCIC. Periodic updates to this policy may be determined by these guidelines.

8.3 Scope

This policy applies to all employees and all technology assets (servers, PCs, laptops, mobile devices, and so on) that are owned or leased by the county.

8.4 General Use and Ownership

- Digital data created and stored in any computer system is the property of the county. Employees shall not copy or otherwise transfer files created during the course of their employment to a personally owned fixed or removable storage

device, Internet-based storage service (i.e., cloud storage) without approval from the highest ranking elected or appointed official responsible for administration and oversight of the digital data's use, storage, analysis and reporting.

- Digital data files, including databases, word-processing files, spreadsheet files, and similar universally accepted file formats, created during the course of an employee's official duties, shall be stored on the county's computer network to ensure protection, retention, and ongoing access to the files. "Convenience copies" of data may be stored on various media and/or locations following the requirements of item #1 above.

- The Director of Information Systems, or designee, shall regularly monitor and evaluate use and security of all component systems that make up the entire county network and shall do so in accordance with the previously adopted Audit Policy. Networks and systems may be audited on a regular basis to ensure compliance with this and other information technology policies adopted by the Board of Commissioners.

8.5 Security and Proprietary Information

- Employees should take all necessary steps to prevent unauthorized access to county digital data by anyone not authorized to access the data.

- Keep network and system login credentials (user Id and password) secure and do not share this information with anyone lacking authorization (i.e., an employee in a department not related to your own). Employees are required to periodically change their password(s). See the county's Password Policy for more information.

- Employees are required to logoff from or otherwise lock their personal computer, laptop, or mobile device when not in use.

- Because information contained on laptops and other mobile devices is especially vulnerable to loss, special care should be exercised when using these systems when working from remote locations. If a device is lost or stolen it must be immediately reported to the Information Systems Department.

- All network servers, personal computers, laptops, and related devices shall continually execute an approved virus protection program. Because these programs cannot guarantee the presence of a virus, employees shall continually exercise caution when sharing files, downloading files, connecting to the Internet, and other service-oriented sites.

- Employees shall not use their county e-mail account for a non-county enterprise (such as Barnes and Noble, Groupon, Facebook, and many other enterprises) unless it is explicitly related to their job responsibilities as defined and approved by their supervisor. See the county's Password Policy for more information.

8.6 Unacceptable Use

The following activities are prohibited. Employees may be exempted from these restrictions as approved by the Board of Commissioners, County Controller, Director of Information Systems or other authority. However, no exemption shall be allowed if one or more parties can show the exemption would be detrimental to the operational "welfare" of the county's computer network.

The lists below are by no means exhaustive. Rather, they attempt to provide a framework for activities which fall into the category of unacceptable use.

8.7 General

Under no circumstances is an employee authorized to engage in any activity that is illegal (under local, state, federal or international law) or deemed to be inappropriate or immoral by the Board of Commissioners.

8.8 Technical

- Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Eaton County. See also the Resolution to Comply with Software Licensing Agreements to Ensure Legal Software Use.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the county or the end user does not have an active license is strictly prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Appropriate management should be consulted prior to exporting any material that is in question.

- Introduction of malicious programs into the network, servers, personal computers, laptops, mobile devices, and related devices.

- Allowing use of your network account and/or password by other individuals not specifically authorized by the employee's supervisor to use the account.

- Using a computer to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

- Making fraudulent offers of products, items, or services originating from any county e-mail account.

- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Effecting security breaches or disruptions (such as denial of service) of network, servers, personal computers, laptops, and mobile devices. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a computer that the employee is not expressly authorized to access.

- Port scanning or security scanning is expressly prohibited unless prior notification to the county is made and the Director of Information Systems authorizes such scanning to occur.

- Executing any form of network monitoring which will intercept data not intended for the employee's host or server system, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any network or system access account.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, an employee's computer system.

- Sending unsolicited e-mail messages, including the sending of "junk mail" and "chain letters" or other advertising material to individuals who did not specifically request such material (this is e-mail spamming).

- Any form of harassment via e-mail, telephone or paging, whether through the use of language, frequency of occurrence, or size of messages.

- Unauthorized use, or forging, of e-mail header information. See the Electronic Mail Policy for additional information.

8.9 Enforcement

Employees found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8.10 Definitions

Term	Definition
Spam[ming]	Unauthorized and/or unsolicited electronic mass mailings.
LEIN	Law Enforcement Information Network
NCIC	National Crime Information Center

8.11 Revision History

This policy update supersedes the Acceptable Use Policy previously adopted by the Board of Commissioners on 12/2/2011.

Policy 9: Password Policy

POLICY

9.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for all of our respective access accounts. A poorly chosen password may result in an entire computer network being compromised. As such, all employees are responsible for taking the appropriate steps, as outlined below, to establish strong passwords and to protect these passwords from unauthorized access by other employees and third-parties.

9.2 Purpose

The purpose of this policy is to establish guidelines for creation of strong passwords, the protection of those passwords, and the frequency of change required to insure the integrity of county computer network and individual systems.

9.3 Scope

The scope of this policy includes all employees who have access to one or more computer systems, networks, and other technology devices.

9.4 General

All network and system-level passwords must be at least eight characters in length and will be prompted for a reset every 90 days. Passwords may not be reused for a minimum of ten reset cycles (i. e., 900 days). Where employees are able to perform this action themselves, they must do so in compliance with this policy.

Users shall be allowed a maximum of five login attempts on any host, hosted, or network server before the user's ID is disabled. Employees must not include passwords in email messages or other forms of electronic communication. In addition to a password, employees accessing data using wireless access must also use an approved form of advanced authentication such as biometric systems, smart cards, and so on. The use of "picture passwords" is an acceptable form of network and system-level security. Where applicable, other elements of this policy shall remain applicable (i.e., password reset requirements).

9.5 Guidelines

Password requirements have the following characteristics:

- Passwords must be at least eight characters in length.
- Contain both upper and lower case characters (e.g., a-z, A-Z) where appropriate.
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- Are alphanumeric characters.
- Do not use a common word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, such as names of family members.

Passwords should never be written down and accessible to other individuals.

B. Password Protection Standards

Do not use your county email address and/or network password for non-county accounts (personal accounts like eBay, home banking, and Amazon).

All passwords are to be treated as confidential.

Here is a list of "don'ts":

- Don't reveal a password over the phone except to an authorized requester (someone you know who is making a legitimate request). You are then responsible for changing the password immediately thereafter and/or notifying the Information Systems Department to assist with required changes.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

If you have any doubts about someone requesting a password, refer them to your supervisor or have them contact the Information Systems Department.

Do not use the "Remember Password" feature of applications like Internet Explorer, specific Web sites, etc. If you do, Microsoft Windows will store your password on the local disk drive of your computer making it available for discovery by an intrusive software program.

If an account or password is suspected to have been compromised, report the incident to the Information Systems Department and request assistance with changing all passwords.

C. Application Development Standards

Application developers (programmers) must ensure their programs contain the following security precautions where applicable. Applications:

- Should support authentication of individual users, minimize use of groups where appropriate.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

D. Passphrases (*applicable in some instances*)

Passphrases are generally used for public/private key authentication such as with wireless networks. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks" - an attack that uses words from the dictionary to try and determine your password.

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "The h0r$e r@n thr0ugh the w00d$"

9.6 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The Information Systems Department may perform a routine audit to determine compliance.

9.7 Definitions

Terms	Definitions
LEIN	Law Enforcement Information Network
NCIC	National Crime Information Center
LDAP	Lightweight Directory Access Protocol.

9.8 Revision History

This policy supersedes the Password Policy previously adopted by the Board of Commissioners on 12/2/2011.

Appendix 1: Glossary of Terms

Primary Source: CMS Information Systems Security Policy, Standards and Guidelines Handbook, version 1.0, February 19, 2002.

Access Control: A security mechanism used to grant users access to a system, based upon the identity of the user, and prevent access to unauthorized users. The user is commonly pre-defined to the system by the systems administrator with a User-id and password.

Access to Information: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.

Application System: Computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system.

Assets: These include information, software, personnel, hardware, and physical resources (such as the computer facility).

Asset Valuation: The value of an asset consists of its intrinsic value and the near- term impacts and long-term consequences of its compromise.

Audit Control: is two-fold in that it is:

1. An independent review and examination of system records, operational procedures, and system activities to ensure compliance with established policies, procedures, and
2. A record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction, from its inception to output of final results.

Authentication:

1. The corroboration that an entity (User, Process, etc.,) is the one claimed.
2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs, and processes.

Availability: Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.

Backup: The process of creating exact copies of data in storage that can be used to restore lost data in contingency circumstances. Also, the information so copied.

Biometrics: identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).

Certification: A technical evaluation with system owner's concurrence of a sensitive application and/or system to see how well it meets security requirements.

Checksum: is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can determine whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

Computer Security: The concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss.

Computer System: Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

Confidentiality: Assurance that data is protected against unauthorized disclosure to individuals, entities or processes.

Consequence (or Impact) Assessment: An estimation of the degree of overall, aggregate harm or loss that could occur, e.g., lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury, or loss of life.

Contingency Plan: A plan for emergency response, backup procedures, and post- disaster recovery. Synonymous with disaster plan and emergency plan.

Contingency Planning: A planned response to high impact events to maintain a minimum acceptable level of operation.

Data Integrity Technologies: The technological means of assuring that information stored in electronic systems has not been altered or destroyed in an unauthorized fashion. For example, hardware-based data integrity assurance technologies may include error-correcting memory or duplicated storage systems; software-based data integrity assurance technologies may include mathematical checksums or other programmatic means of detecting anomalies in stored information.

Database: A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; data is stored so that it can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data.

Digital Signature: An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters, such that the identity of a signer and the integrity of the data can be verified.

Disaster Recovery: A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.

Encryption: The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium.

Firewalls: Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

Guidelines: General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.

Hacker: A person who secretively invades others' computers, inspecting or tampering with the programs or data stored on them.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, under which the HIPAA Security Rule (and other HIPAA rules) is created.

HIPAA Security Rule: Published in the United States Federal Register as 45 CFR Parts 160, 162, and 164. Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. Washington, DC. Amended January 25, 2013 to add HITECH enhancements.

Technology Services Facility: An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. Technology Services Facilities range from large centralized computer centers to individual standalone workstations.

Illegal Access and Disclosure: Activities of employees that involve improper systems access and sometimes disclosure of information found thereon, but not serious enough to warrant criminal prosecution.

Information: Any communication or reception of knowledge, such as facts, data, or opinions; including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape.

Information Systems Security (INFOSEC): The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. Protection results from the application of a

combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.

Integrity: Assurance that data is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.

Internet: A worldwide electronic system of computer networks which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.

Local Area Network (LAN): A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. Local area networks commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.

Major Application (MA): An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. Note: All applications holding electronic protected health information require some level of protection. Certain applications, because of the information in them, however require special management oversight and should be treated as major.

Malicious Software: The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Malware, Trojan horses, and worms.

Media: Hard copy (including paper), PC/workstation hard disk, CD/DVD, “USB storage devices”, and other electronic forms by which CMS data is stored, transported, and exchanged. The need to protection information confidentiality, integrity, and availability applies regardless of the medium used to store the information. However, the risk exposure is

considerably greater when the data is in an electronically readable or transmittable form compared to when the same data is in paper or other hard copy form.

Misuse of Organization Property: The use of computer systems for other than official business that does not involve a criminal violation, but is not permissible under organization policies.

Mitigation: See Risk Mitigation.

Modem: Modem is short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line. Modems convert digital computer signals into analog telephone signals (modulate) and the reverse (demodulate).

Network: A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A network can be as small as a LAN consisting of a few computers, printers, and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer network exists to provide computer users with the means of communicating and transferring information electronically.

NIST: The National Institute of Standards and Technology, which (among many duties) creates standards and guides to be used in meeting various Federal requirements such as HIPAA. NIST documents are frequently cited in the preamble to the HIPAA Security Rule.

Passwords: A confidential character string used to authenticate an identity or prevent unauthorized access. Passwords are most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).

Personnel Security: Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness

which is commensurate with the value of information resources which the individual will be able to access.

PHI: An abbreviation for Protected Health Information (see below).

Physical Security: The application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information.

Policy: A high-level statement of enterprise beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

Procedures: Define the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.

Protected Health Information (PHI): The health information concerning health treatment of an individual and payment for such services. Virtually all health information held by a HIPAA covered entity is protected by HIPAA in some manner.

Risk: The potential for harm or loss. Risk is best expressed as the answers to these four questions:

1. What could happen? (What is the threat?)
2. How bad could it be? (What is the impact or consequence?)
3. How often might it happen? (What is the frequency?)
4. How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" *per se*.

Risk Analysis: A process whereby cost-effective security / control measures may be selected by balancing costs of various security control measures against the losses that would be expected if these measures were not in place.

Risk Assessment: The identification and study of the vulnerability of a system and the possible threats to its security.

Risk Management: The total process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk, including identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost/benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review. It encompasses the incorporation of the processes and results from both risk analysis and risk mitigation.

Risk Mitigation: The process of reducing the probability and / or consequences of an adverse risk event to an acceptable threshold.

Safeguard Analysis: An examination of the effectiveness of the existing security measures, actions, devices, procedures, techniques, or other measures that reduce a system's vulnerability to a threat and identification of appropriate new security measures that could be implemented on the system.

Security: All of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data.

Security-Related Event: An attempt to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also included are attempts to violate the security policy of the system (e.g., too many attempts to log on, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).

Security Violation: An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. This includes, but is not limited to, unusual or apparently malicious break-in attempts (either local or over a network), virus or network worm attacks, or file or data

tampering, or any incident in which a user, either directly or by using a program, performs unauthorized functions.

Sensitive Application: An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, or delivery interruption of the application.

Sensitive Data: Data that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an organization to accomplish its mission, proprietary data, and records about individuals requiring protection under HIPAA.

Significant Change: A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, adding remote access, and increasing the equipment capacity of the installation.

Standards: Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to meaningful and effective.

System/Owner Manager: The official who is responsible for the operation and use of an application system.

System Security Plan: A basic overview of the security and privacy requirements of the subject system and the organization's plan for meeting those requirements.

Telecommunications: A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such as telephone lines, microwave relay, satellite link, or physical cable.

Threat: An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.

Threat Identification: The analysis of recognized threats to determine the likelihood of their occurrence and their potential to harm assets.

Trojan Horse: A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. Also a destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful.

User: The person who uses a computer system and its application programs to perform tasks and produce results.

Virus: A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. May be a self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating component. Malware would be classified in this manner as well.

Vulnerability: A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.

Wide Area Network (WAN): A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. A WAN is a communications network that connects geographically separated areas.

Workforce: The collection of employees, trainees, contractors, and volunteers whose conduct, in the performance of work or services for a HIPAA-covered organization, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation: A workstation is a computer built around a single-chip microprocessor. Less powerful than minicomputers and mainframe computers, workstations have nevertheless evolved into very powerful machines capable of complex tasks.
Technology is progressing so quickly that state-of- the-art workstations are as powerful as mainframes of only a few years ago, at a fraction of the cost.

World Wide Web (WWW or WEB): The collection of electronic pages, (documents) that are developed in accordance with the HTML (hypertext markup language) Web format standard and may be accessed via Internet connections.

Worm: A worm is a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information.

Appendix 2: Form for Personnel Changes (New Hire, Termination, Promotion)

Eaton County Technology Services

Computer Services Request for New Hire, Termination, and Promotion

Supervisors are required to complete the Personnel Change Request form for all their new hires, promoted staff or terminations. The form can be located at: http://lfservices/Forms/Account/LogIn?returnUrl=%2fForms%2fPersonnel_Change_Form.

This form will require the supervisor to enter data relating to the employee being changed, what the status of the change is and what applications will be required.

Appendix 3: Log for Data Breach Documentation

Log for Covered Entity to Document Breaches Required to be Disclosed Annually to the U.S. Department of Health & Human Services ("HHS")

The information to be disclosed and the procedure for disclosure will be set forth on the HHS website (HHS.gov).

Date of Breach	Affected Individual(s)	Date of Discovery

Attached to each entry should be a copy of the individual notice(s) sent in connection with the breach.

Appendix 4: PHI Non-Routine Disclosure Documentation

Accounting of Non-Routine Disclosures of Protected Health Information ("PHI")

Name of individual who is the subject of PHI:_____

Date of Disclosure	Name and Address of Recipient of PHI	Description of PHI Disclosed	Purpose of Disclosure (or indicate that copy of written request or authorization is attached)

Appendix 5: Sample Notice of Breach Notification

Sample Individual Notice for Breach Notification

[Employer Letterhead]

_____

_____

_____

Re: Notice of Breach of Unsecured Protected Health Information

Certificate of Appreciation

County of Ingham

This is to certify that

Anita Beavers

is hereby awarded for outstanding service and contributions to

the citizens of Ingham County. We the undersigned Commissioners hereby honor and commend Anita Beavers and extend our sincere appreciation for her years of service as President of the Colonial Village Neighborhood Association and for her dedication and commitment to improving the quality of life for the residents in the community

on this 17th day of November, 2010.

Debbie De Leon Chairperson, Board of Commissioners, District 2	Victor G. Celentino Vice-Chairperson, Board of Commissioners, District 1	Dale Copedge County Services Committee Chairperson, District 6