

BEFORE THE BOARD OF COUNTY COMMISSIONERS
OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF UPDATING POLICIES)
REGARDING THE SECURITY OF)
ELECTRONIC PROTECTED HEALTH)
INFORMATION AND ADOPTING POLICIES)
REGARDING THE HEALTH INFORMATION)
TECHNOLOGY FOR ECONOMIC AND)
CLINICAL HEALTH (HITECH) ACT OF 2013)

RESOLUTION NO. R-16-0041

WHEREAS, pursuant to Neb. Rev. Stat. §23-104(6) (Reissue 1997), Lancaster County has the power to do all acts in relation to the concerns of the County necessary to the exercise of its corporate powers; and

WHEREAS, pursuant to Neb. Rev. Stat. §23-103, the powers of a county are exercised by the Board of County Commissioners; and

WHEREAS, the U. S. Department of Health and Human Services enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2013; and,

WHEREAS, HITECH required the U.S. Department of Health and Human Services Office for Civil Rights (OCR) to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security and Breach Notification Rules; and

WHEREAS, as a result Lancaster County reviewed and updated existing HIPAA security policies to ensure Lancaster County is in compliance; and

WHEREAS, the attached security policies will apply to the following County departments and programs that are covered by the HIPAA regulations:

Lancaster County Mental Health Crisis Center
Lancaster County Medical and Dental Insurance Plans; and

NOW, THEREFORE, BE IT RESOLVED by the Board of County Commissioners of Lancaster County, Nebraska as follows:

1. The Lancaster County HIPAA Security Policies and Procedures, marked "Exhibit A", attached hereto and incorporated herein by this reference, are hereby approved and adopted with an effective date of July 19, 2016. Such policies shall be utilized, as applicable, by Lancaster County departments and programs covered by HIPAA.
2. The appointed Security Officer is hereby authorized to amend the HIPAA Security Policies without further action of this County Board provided such amendments are consistent with state and federal law.

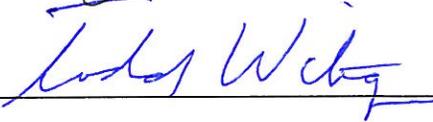
DATED this 19 day of July, 2016, at the County-City Building, Lincoln, Lancaster County, Nebraska.

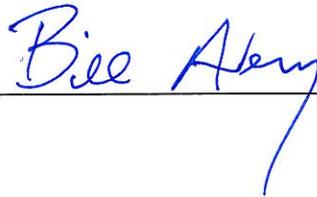
BY THE LANCASTER COUNTY BOARD OF COMMISSIONERS











APPROVED AS TO FORM

This 19 day of


_____, 2016.

for JOE KELLY, County Attorney

POLICY #7-01

HIPAA Security Administration

GENERAL SECURITY COMPLIANCE §164.306

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers Lancaster County's approach to compliance with the HIPAA Security Regulations, 45 CFR 160, 162 and 164 (hereinafter referred to as "the Security Regulations"). Lancaster County will:

1. Ensure the confidentiality, integrity and availability of all ePHI Lancaster County creates, receives, maintains and 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
4. Ensure compliance with the Security Regulations by its Workforce.

Policy:

1. Hybrid Entity

Lancaster County is a hybrid entity under HIPAA with both covered and non-covered departments. Lancaster County hereby designates its HIPAA covered departments as health care components for purposes of the Security Regulations. Lancaster County's covered health care components are listed in Exhibit A.

2. Security Personnel and Implementation

Lancaster County has designated a Security Officer with overall responsibility for the development and implementation of policies for the Security Regulations. Further, Lancaster County directs all HIPAA covered departments to name a HIPAA Security Liaison. The HIPAA Security Liaison is responsible for ensuring that the department:

1. Complies with the Lancaster County HIPAA Security Policies and Procedures
2. Maintains the confidentiality of all ePHI for which they are responsible
3. Assists in training all workforce members within the department at the appropriate level of HIPAA training

Lancaster County will implement reasonable and appropriate security measures to comply with the Security Regulations. To determine what is reasonable and appropriate Lancaster County will take into account its size, capabilities, complexity, technical infrastructure, hardware, software, security capabilities, the costs of the security measure, and the probability and criticality of potential risks to ePHI.

3. Security Compliance

The Security Officer is responsible for facilitating a process for individuals to file a complaint regarding the handling of ePHI by a Lancaster County workforce member. The Security Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

4. Sanctions and Non-Retaliation

Lancaster County will ensure that workforce members will be appropriately disciplined and sanctioned for violating the Lancaster County Security Policies and Procedures. Lancaster County will refrain from intimidating or retaliating against any person exercising his or her rights under the Security Regulations for reporting any concern, issue or practice that such person believes to be in violation of the Security Regulations or the Lancaster County Security Policies and Procedures. Lancaster County will not require any persons to inappropriately waive any rights to file a complaint with the Department of Health and Human Services.

5. Security Policies and Procedures

The Lancaster County HIPAA Security Policies and Procedures are designed to ensure compliance with the HIPAA Security Regulations. Such Security Policies and Security Procedures shall be kept current and in compliance with any changes in the law, regulations or practices of Lancaster County's covered departments. Workforce members will be appropriately trained on the importance of maintaining security.

6. Workforce Members

For purposes of the Lancaster County Security Policies and Procedures, workforce members include all full and part-time employees, volunteers, contractors, temporary workers and those employed by others to perform work on behalf of Lancaster County HIPAA covered departments and who have been granted access to Lancaster County information assets and systems.

7. Responsibility of All Employees Within a HIPAA Covered Department

Lancaster County workforce members are responsible for being aware of, and compliance with, Lancaster County Security Policies and Procedures.

EXHIBIT A

1. Lancaster County Mental Health Crisis Center
2. Lancaster County Clerk, but only to the extent it performs "business associate" type functions on behalf of a covered component of Lancaster County
3. Lancaster County Attorney's Office, but only to the extent it performs "business associate" type functions on behalf of a covered component of Lancaster County
4. Lancaster County Budget & Fiscal Office, but only to the extent it performs "business associate" type functions on behalf of a covered component of Lancaster county
5. Lancaster County Records Management, but only to the extent it performs "business associate" type functions on behalf of a covered component of Lancaster County
6. Employee Health Plans including medical insurance, vision plan, dental plan, flexible spending account, and COBRA administration of the health plans
7. City-County Information Services Division, but only to the extent it performs "business associate" type functions on behalf of a covered component of Lancaster County

POLICY #7-02

HIPAA Administrative Safeguards

SECURITY MANAGEMENT POLICY § 164.308(a)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to ensure that security violations are prevented, detected, contained and corrected in accordance with the Security Regulations and to protect ePHI.

Policy Statement:

This Policy covers the ePHI risk analysis that shall be conducted on each covered department, the security measures that each covered department will implement to protect its ePHI based upon the ePHI risk analysis, and information systems activity review to ensure security of ePHI by each covered department. Lancaster County shall conduct a thorough risk analysis to serve as a basis for HIPAA Security Regulation compliance efforts. As changes in technology occur, and business processes change, risks to their ePHI shall be reevaluated.

Procedures:

1. Risk Analysis

- A. Lancaster County acknowledges the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that is associated with storing ePHI and transmitting ePHI inside Lancaster County, outside of Lancaster County, and to other County departments that are not covered entities.
- B. An Assessment Team (Information Services, the County's HIPAA Privacy and Security Officer, County Attorney) shall be responsible for coordinating the risk analysis. The Assessment Team shall identify the appropriate departmental representatives within Lancaster County to assist with the ePHI analysis. The Assessment Team will conduct an analysis of the potential risks and vulnerabilities to ePHI by:
 1. Developing/updating a comprehensive systems inventory including:
 - a. Hardware Inventory (network devices, workstations, printers, etc.)
 - b. Software Inventory (operating systems, applications, interfaces, etc.)
 - c. Update logical and physical network diagrams to illustrate the current environment

2. Identifying and documenting all systems containing ePHI
 - a. Document/describe ePHI
 - b. Determine the source of the data (created vs. received)
 - i. If received from a third party identify source and method of receipt
 - c. Determine if the data is forwarded to a third party
 - i. If the data is forwarded identify the receiver and method of transfer
 - d. Determine the criticality (impact to the County if data were no longer available for long or short period of time) of the software application and associated data.
 - e. Determine the sensitivity (potential harm that could result from a security breach) of the data.
 - f. Identify existing controls/policies/security measures in place to protect ePHI and assess the reasonableness and appropriateness of existing security measures protecting ePHI.
3. Identifying and assessing any potential risks and vulnerabilities to the integrity, confidentiality, and availability of ePHI held.
 - a. Such assessment will include identifying potential vulnerabilities from the following threats:
 - i. Intentional malicious attacks (i.e. electronic based scanning, snooping, viruses, etc.)
 - ii. Unintentional human errors (i.e. application/network programming problems)
 - iii. Natural threats (i.e. storms, tornados, floods, etc.)
 - iv. Environmental incidents (i.e. chemical spills, fire, power outage)
4. Determining adequacy of existing controls, policies and procedures and taking necessary corrective actions identified in the aforementioned review.
 - a. Institute and test necessary safeguards to ensure that ePHI is adequately protected and safeguarded. These actions could include vulnerability assessments or controlled hack (internal or external)

- C. The Assessment Team will reassess the potential risks and vulnerabilities to the integrity, confidentiality, and availability of ePHI as part of a periodic review.
1. Risk Management
 - a. Reasonable and appropriate security measures will be implemented that are sufficient to reduce risks and vulnerabilities to ePHI
 - b. The Assessment Team shall:
 - i. Reassess the potential risks and vulnerabilities to ePHI as part of a periodic review and update the security measures when reasonable and appropriate
 - ii. Identify appropriate follow up measures to ensure security procedures and policies remain adequate for the protection of ePHI based on:
 - Changes in relationships (new ePHI is created/identified)
 - New legislation related to ePHI (Federal, State or Local)
 - Occurrence of a breach in County security
 - c. Document their follow up procedures
 - i. Interviews
 - ii. Analysis
 - iii. Review new/modified policies
 - iv. Recommendations/modifications
 2. Sanctions for Noncompliance
 - a. To ensure all members of a covered department's workforce fully comply with the Lancaster County Security Policies and Procedures, Lancaster County will do the following:
 - i. An employee found to have violated any provision of these Security Policies and Procedures will be subject to disciplinary action up to and including termination from employment
 - ii. Discipline will be administered in accordance with the applicable labor agreement and/or the Lancaster County Personnel Rules, as adopted
 - iii. Other workforce members found to have violated any provision of these Security Policies and Procedures will be sanctioned appropriately
 - iv. The covered department shall inform the Lancaster County Security Officer of all incidents that may lead to disciplinary action or sanctions pursuant to this policy

- v. Lancaster County shall not retaliate against any person for reporting a security violation or for participating in the investigation of such violation.

3. Information System Activity Review

- a. Internal audit procedures will be implemented to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports
- b. Lancaster County shall perform ongoing reviews of systems' activities, identify and investigate potential security violations, and take appropriate actions to minimize security violations
 - i. Refer to the Audit Controls Policy for a description of the specific tools that will be used to monitor, track and record activities on systems that contain ePHI
 - ii. To carry out this policy Information Services shall
 - Conduct reviews of County information systems activities
 - Document these reviews including
 - Name of individual performing the review
 - Date and time of the review
 - Observations and findings
 - Corrective action taken
 - iii. These review should be performed periodically, but at least annually, or as driven by a known or suspected breach. Reviews shall include:
 - Login activities (and account lock outs)
 - Security incidents (failed network navigation attempts, malicious activities, denial of service attacks, activity probing activities, etc.)
- iv. The Security Incident Procedures Policy shall be followed in corrective efforts.

POLICY #7-03

HIPAA Administrative Safeguards

ASSIGNED SECURITY RESPONSIBILITY POLICY § 164.308(a)(2)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Policy covers the procedures for identifying the security official who is responsible for the development and implementation of the policies and procedures for HIPAA Security.

Policy:

Lancaster County will assign and document the security official who is responsible for the development and implementation of the policies and procedures for HIPAA Security. See Exhibit A.

EXHIBIT A

Designation of Security Officer

Security Officer: Deputy Chief Administrative Officer for the Lancaster County Board of Commissioners or his/her designee

Address: 555 S. 10 St
Lincoln, Ne 68508

Phone: 402-441-7447

Contact Office: Lancaster County Board of Commissioners

Address: 555 S. 10 St.
Lincoln, NE 68508

Phone: 402-441-7447

POLICY #7-04

HIPAA Administrative Safeguards

WORKFORCE SECURITY POLICY § 164.308(a)(3)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to ensure that all workforce members have appropriate access to ePHI and to prevent workforce members who do not have access to ePHI from obtaining such access. The purpose of this Policy is to implement procedures to ensure that all members of the workforce have appropriate access to ePHI and to prevent those workforce members who do not need access from obtaining access to ePHI.

Policy Statement:

Lancaster County has established guidelines for determining each workforce members' need to access ePHI. Only authorized users will be granted access to ePHI. The fundamental principle of "need to know" will be applied by the covered department to determine access privileges. Reasonable efforts shall be made to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

Procedures:

1. The department head or his/her designee shall determine the necessary and appropriate level of access for workforce members to ePHI. This determination should be based on their specific requirements to fulfill their job responsibilities, and includes access to both hardware and software. Department head or designee shall maintain a current list of levels of access for all workforce members to ePHI.
2. No workforce members access rights shall be made or modified without formal documentation of approval from the department head or his/her designee.
3. Information Services in conjunction with the department head or his/her designee shall determine workforce members need to utilize smart cards and/or tokens to facilitate their access to data.
4. If job responsibilities change for a workforce member, the department head or designee shall perform a reevaluation and make appropriate changes as necessary. All such determinations shall be communicated by the department head or designee to Information Services.
5. Any workforce member who either successfully or unsuccessfully attempts to gain access to ePHI for which they are not authorized shall be subject to disciplinary actions up to and including termination.

6. The department head or his/her designee shall conduct periodic audits to determine whether actual access to ePHI by workforce members is in compliance with the established requirements as determined in the procedures above. This shall be done at least annually.
7. In the event of termination or transfer to another position, the workforce member's department head or designee shall ensure that all existing access is terminated. The department head or designee will also determine if any other precautionary measures are to be taken (other physical security measures).
8. To terminate access, the department head or designee shall notify Information Services.
9. Upon being informed to terminate access, Information Services will:
 - A. Inactivate the user account
 - B. Remove the user profile from all PC's
 - C. Where applicable, remove user from any remote connectivity systems
 - D. Where applicable, copy user folders to location specified by the department head or designee
10. In the event that devices (smart cards, token)s are not returned to department head or designee, the department head or designee shall promptly provide all necessary information to Information Services.

POLICY #7-05

HIPAA Administrative Safeguards

INFORMATION ACCESS MANAGEMENT POLICY § 164.308(a)(4)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to ensure that access to ePHI is properly authorized.

Policy Statement:

Lancaster County is committed to protecting ePHI and has developed an Information Access Management Policy to ensure that access to ePHI is properly authorized and consistent with the Security Regulations.

Procedures:

1. Health Care Clearinghouse Functions
 - A. Lancaster County is not a health care clearinghouse that is part of a larger organization so Lancaster County has no access by a larger organization.
2. Access Authorization
 - A. Lancaster County has established procedures for granting access to ePHI through a workstation, transaction, program or process. Procedures include the following:
 - i. Department head or his/her designee is responsible for authorizing access to systems and networks containing ePHI for his or her subordinates. Workforce members are not permitted to authorize their own access to ePHI or be granted authorization from another supervisor.
 - ii. Department head or his/her designee is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.
3. Access Establishment and Modification
 - A. Department head or his/her designee is responsible for periodically reviewing the access to ePHI granted to each of his or her subordinates and for modifying such access if appropriate.

- B. Information Services will be responsible for security on networks, servers and systems by establishing security to support the separation and accessibility of ePHI data and programs.
- C. Lancaster County has established procedures for terminating access to ePHI through a workstation, transaction, program or process. Procedures include the following:
 - i. If a workforce member's employment or services are terminated, the Department head or his/her designee is responsible for ensuring that all such workforce member's accounts to access ePHI are terminated.
 - ii. If a workforce member's employment or services are terminated, the Department head or his/her designee is responsible for ensuring that such workforce member's access to all facilities housing ePHI is terminated, including but not limited to access cards, keys, codes, and other facility access control mechanisms. Codes for access, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.
- D. Transfer of Employment within Lancaster County
 - i. If a workforce member transfers to another department within Lancaster County:
 - a. The workforce member's access to ePHI within his or her current department must be terminated as of the date of the transfer.
 - b. Department head or his/her designee for which the workforce member subsequently works is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

POLICY #7-06

HIPAA Administrative Safeguards

SECURITY AWARENESS AND TRAINING POLICY § 164.308(a)(5)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to provide security awareness and training for all members of its workforce. It is Lancaster County's purpose to implement a security awareness and training program for all workforce members who possess access to ePHI.

Policy Statement:

Lancaster County shall establish a training methodology to provide adequate initial and ongoing training regarding the risks associated with the improper access, use and disclosure of ePHI.

Procedures:

1. Security Training Program
 - A. The covered departments shall provide ongoing information security awareness and education for all members of its workforce. This shall cover information security basics, associated policies, procedures, and workforce member responsibilities.
 - B. The covered department shall ensure that workforce members under their supervision are aware of information security policies, procedures, and guidelines and have access to current versions of the same.
 - C. The covered department shall inform new full and part-time employees, temporary workers and volunteers of the importance of information security and their role in protecting valuable and sensitive information. This should occur during new employee orientation.
 - D. Workforce members shall acknowledge they have been informed and are aware of Lancaster County's Security Policies and Procedures and their role in protecting Lancaster County's information systems and information assets by signing an Employee Acknowledgement Form.
 - E. The department head or designee shall be responsible for collection and management of the signed Employee Acknowledgement Form.

- F. The covered department shall hold an annual awareness and education session to review information security basics and current information security policies with workforce members under their supervision. This can be in conjunction with any privacy training.
- G. The covered department shall inform all other authorized users of the importance of information security and their role in protecting Lancaster County information systems and information assets through the terms of a Business Associate Contract, where applicable.

2. Security Reminders

- A. Information Services shall issue security reminders on a regular basis. These shall address such topics as password protection, virus protection, the handling of suspicious email attachments, and how to handle and report breaches. These may be circulated via formal training, network log in messages, emails, newsletters, etc.

3. Protection from Malicious Software

- A. In the event of a security event, Information Services shall provide information on countermeasures to be taken to reduce the negative impact of said event.
- B. Information Services will develop and implement procedures to detect and guard against malicious code such as viruses, worms, ad ware, and any other computer program or code designed to interfere with normal operation of a system.
- C. A virus detection system must be implemented on all workstations including a procedure to ensure that the virus detection software is maintained and up to date.
- D. Information Services will notify all departments and users of new and potential threats from malicious code such as viruses, worms, denial of service attacks, and any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.
- E. Departments and users must notify Information Services if a virus, worm or other malicious code has been identified.
- F. Information Services will be responsible for ensuring that any system that has been infected by a virus, worm or other malicious code is immediately cleaned and properly secured or isolated from the rest of the network.

4. Log-in Monitoring

- A. Information Services will implement a mechanism to log and document failed login attempts on each system containing ePHI.
- B. Department head or designee will review such log-in activity reports and logs on a periodic basis.

- C. Procedures for reviewing logs and activity reports will be contained in the Audit Control Policy, Policy #7-16.
- D. All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported to the Lancaster County Security Officer and Information Services.

5. Password Management

- A. All workforce members who access the network or applications that contain ePHI (access, transmit, receive or store) shall be supplied with a unique user id and password to access said systems.
- B. All passwords used to gain access to any network or applications that contain ePHI must be of sufficient complexity to ensure that is not easily guessed.
- C. Workforce members are responsible for the proper use and protection of their passwords.
 - 1. Passwords must not be disclosed to other workforce or family members.
 - 2. Appropriate identification or verification shall be made on all persons representing themselves as service providers needing temporary access to machines that have access to any network.
 - 3. Passwords shall not be written down, posted or held in an insecure manner.
 - 4. A password must be changed immediately if it is suspected of being disclosed.
 - 5. Workforce members should refuse all offers by software and/or internet sites to automatically login the next time they access those resources.
- D. Automated password controls shall be set so that:
 - 1. All passwords are changed a minimum of every 56 days.
 - 2. Workforce members cannot reuse a password on consecutive cycles.
 - 3. Passwords must be at least eight (8) digits in length and contain a minimum of
 - a. One alphabetic character
 - b. One numeric character (0- 9)
 - c. One of the following special characters (#, \$, @)

POLICY #7-07

HIPAA Administrative Safeguards

Security Incident Procedures Policy §164.308(a)(6)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This policy establishes appropriate procedures to identify, report and respond to security incidents.

Policy Statement:

Lancaster County is committed to protecting ePHI and has developed an Incident Response and Reporting system to identify, respond, mitigate and document HIPAA security incidents and violations.

Procedures:

1. All incidents, threats or violations that affect or may affect the confidentiality, integrity or availability of ePHI must be reported and responded to using the following procedures:
 - A. Any workforce member suspecting a security incident shall immediately notify their department head or his/her designee. If the incident involves viruses, worms, or malicious code, network or system attacks, Information Services shall also be informed immediately.
 - B. To the fullest extent possible, such employee shall provide the date, time and incident specifics. This information is to be treated as confidential information.
2. The department head or his/her designee shall immediately contact Information Services to minimize the negative impact of the security incident. The department head or his/her designee shall work with Information Services to identify the extent and cause of the security incident. Additionally, the department head or designee shall complete a Security Incident Form. The completed form should be sent to the Lancaster County HIPAA Security Officer. The department should keep a copy of the completed form.
 - A. The department head or designee and Information Services shall document the following to the fullest extent possible:
 - i. Assets that may have been compromised (hardware and software)
 - ii. Any interviews related to incident review

- B. The department head or designee and Information Services shall:
- i. Take necessary actions to attempt to limit the damage associated with the incident
 - ii. Ensure that all evidence on the matter is secured
 - iii. Restore affected systems
 - iv. Determine and implement any remedial measures to reduce future exposure in the area
 - v. Conduct interviews related to the incident
 - vi. Contact law enforcement if necessary
 - vii. Prepare a summary report of the incident. The report shall be part of the ongoing risk analysis review referred to in the Security Management Policy, Policy #7-02.

POLICY #7-08

HIPAA Administrative Safeguards

Contingency Plan Policy §164.308(a)(7)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County's objective is to establish appropriate policies and procedures for responding to an emergency or other occurrence (fire, vandalism, system failure, natural disaster, etc.) that damages systems containing ePHI.

Policy Statement:

Lancaster County is committed to minimizing the impact of emergencies or other events that negatively impact systems containing ePHI. We will continue to monitor and update our procedures to ensure that they stay current and accurate.

Procedures:

1. Data Backup Plan
 - A. Information Services will establish and implement a data backup plan which will allow for the successful retrieval of all data and files on systems supported at the Data Center.
 - B. Information services will assist agencies who perform their own system support from remote locations to ensure they can successfully retrieve all data and files from their data systems.
 - C. The data backup plan will require that all media used for the backups are stored in a physically remote location from the system hardware.
 - D. Data backup procedures will be tested on a periodic basis to ensure files are retrievable.
2. Disaster Recovery Plan
 - A. Information Services will create and maintain a plan to recover from the loss of data due to an emergency or disaster.
 - B. The plan shall consider the level of disaster and the estimated impact on County operations.
 - C. The plan shall include procedures for restoration of data systems.

- D. The plan shall be documented and easily available to necessary personnel at all times.
3. Emergency Operation Plan
- A. Lancaster County will establish procedures to continue critical business operations during an emergency.
 - B. The plan shall include provisions for the continued protection of ePHI during the emergency period.
 - C. The plan shall be documented and easily available to necessary personnel at all times.
4. Testing and Revision Procedure
- A. Data backup procedures shall be tested and easily available to necessary personnel at all times.
 - B. The Disaster Recovery Plan shall be tested on a periodic basis to ensure systems and exact copies of all data can be retrieved and restored.
 - C. Emergency mode operation procedures shall be tested on a periodic basis to ensure critical business processes can continue in a satisfactory manner while operating in emergency mode.
5. Applications and Data Criticality Analysis
- A. Lancaster County shall assess the relative criticality of specific applications and data in support of other contingency plan components.

POLICY #7-09

HIPAA Administrative Safeguards

Evaluation Policy §164.308(a)(8)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This policy is to ensure that Lancaster County performs a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Regulations and subsequently in response to environmental or operational changes affecting the security of the ePHI. The periodic evaluation will establish the extent to which Lancaster County's Security Policies and Procedures meet the requirements of the Security Regulations.

Policy Statement:

Lancaster County is committed to ensuring the Security Policies it has adopted are periodically evaluated for technical and non-technical viability.

Procedures:

1. Periodic Evaluation
 - A. Lancaster County will evaluate its Security Policies to determine their compliance with the Security Regulations. Lancaster County's Security Policies shall be evaluated on a periodic basis to assure continued viability in light of technology, environmental or operational changes that could affect the security of ePHI.
 - B. The Security and Privacy Officers will annually review the Policies and Procedures Lancaster County has adopted for compliance with the Security Regulations.
 - C. The Security and Privacy Officers will develop and recommend to the County Attorney's Office, Information Services, and the County Board any necessary Security Policy or Procedure changes.
 - D. Security Liaisons for each covered department will review Security Policies and Procedures annually.
 - E. When changes are made to Security Policies or Procedures all covered departments will be notified.

2. Triggered Evaluations

- A. In the event one of the following events occurs the policy review and evaluation process described above will immediately occur:
- i. Changes in the HIPAA Security or Privacy Regulations
 - ii. New federal, state or local laws or regulations affecting the privacy or security of ePHI
 - iii. Changes in technology, environmental or business processes that may affect HIPAA Security Policies or Procedures
 - iv. A serious violation, breach or other security incident

POLICY #7-10

HIPAA Administrative Safeguards

BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS POLICY §164.308(b)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to ensure access to PHI is appropriately limited. This Policy covers the procedures to allow for a Business Associate to create, receive, maintain or transmit ePHI on the County's behalf.

Policy:

1. Lancaster County, in accordance with §164.306, may permit a Business Associate to create, receive, maintain or transmit ePHI on the County's behalf only if the County obtains satisfactory assurances, in accordance with §164.314(a) that the Business Associate will appropriately safeguard the information.
2. This standard does not apply with respect to:
 - A. Transmission of ePHI by the County to a health care provider concerning the treatment of an individual; or
 - B. Transmission of ePHI 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
 - C. Transmission of ePHI from or to other agencies providing the services at §164.502(e)(1)(ii)(C) when the County is a health plan that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.
3. Lancaster County will document the satisfactory assurances through a written contract or other arrangement with the business associate. Business Associate contracts must be approved by the County Attorney's Office and the Lancaster County Board of Commissioners.

POLICY #7-11

HIPAA Physical Safeguards

Facility Access Controls Policy §164.310(a)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County is committed to ensure that only authorized access is allowed to County electronic information systems and technology facilities.

Policy Statement:

Lancaster County adopted this policy to limit physical access to its electronic information systems and the facility(s) in which such systems are housed, while still ensuring that proper authorized access is allowed.

Procedure:

1. Contingency Operations
 - A. The department or his/her designee will create procedures to allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.
2. Facility Security Plan
 - A. The department head or his/her designee at each facility housing PHI (both electronic and analog) shall be responsible for developing, implementing and maintaining a Facility Security Plan. Details related to access controls and validation shall be part of this plan.
 1. Access Controls
 - i. Plan shall include procedures for validation of the identity of persons physically present at the facility
 - ii. Workforce member ID badges
 - iii. Visitor sign-in, ID badges and escorts
 - iv. Patient escorts where applicable

B. The department head or his/her designee shall also review other environmental controls to determine which controls should be included in the Facility Security Plan. In determining which environmental controls should be included, relative threat, relative criticality and costs shall be considered. The following list contains the environmental controls that should be considered in this analysis:

1. Fire suppression equipment (halon, sprinklers)
2. Smoke detectors
3. Fire Alarms
4. UPS (Uninterruptible Power System) and/or power conditioners
5. Back-up generator facilities
6. Surge suppressors
7. Heat and humidity sensors and controls
8. HVAC systems for computer rooms

3. Access Control and Validation Procedures

- A. The department head or his/her designee will develop procedures to control and validate workforce member access to facilities where PHI (both electronic and analog) is maintained or available for review.
- B. The department head or his/her designee will implement procedures to control, validate and document visitor access to any facility where PHI is stored (both electronic and analog). "Visitors" includes vendors, repair personnel, and other non-employees.
- C. The department head or his/her designee will develop procedures to secure the physical locations where PHI is stored. This includes data centers, data closets, file cabinets and desks.
- D. Facilities where PHI is available will have appropriate physical access controls to limit access to the facility. This includes such things as key locked doors, code locked doors and/or badge reader locked doors.

4. Maintenance Records

- A. The department head or his/her designee will create procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

POLICY #7-12

HIPAA Physical Safeguards

Workstation Use Policy §164.310(b)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has implemented this policy to 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 workstations that can access ePHI.

Policy:

1. All workforce members will comply with the Lancaster County Internet and E-mail Usage Policy 99-1 to ensure that computers accessing ePHI are used in a secure and legitimate manner. Lancaster County Internet and E-mail Usage Policy 99-1 is attached as Exhibit A.
2. Workforce members and users of Lancaster County systems and workstations should have no expectation of privacy. To protect and manage its information systems and enforce appropriate security measures, Information Services may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information systems.
3. Lancaster County may remove or deactivate any workforce member or user privileges and access to secured areas when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, data or ePHI.

POLICY #7-13

HIPAA Physical Safeguards

Workstation Security Policy §164.310(c)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County adopted this policy to implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Policy:

1. Mobile Devices
 - A. Mobile devices with the capability to access or store ePHI shall have power on passwords or data encryption to reduce the exposure to ePHI being made available to unauthorized users. Examples of mobile devices are:
 1. Laptop/notebook computers/electronic tablets/any portable computing device
 2. Cellular phones with data capabilities
2. Anti-virus Software
 - A. Information Services shall be responsible for acquiring such software for all County computing devices.
 - B. Information Services shall be responsible for keeping current signature files available for installation. Whenever possible, automated means shall be used to ensure these updates are performed on a regular basis in an automated fashion with minimal workforce manual intervention.
 - C. Upon identification of malicious software on any County computing device, Information Services shall take necessary steps to prevent the spread of the virus.
 - D. Upon containment, Information Services or the appropriate department staff (in the case of devices being maintained or supported by other County offices or third party vendors) shall repair any infected files.

3. Physical Configuration of Work Areas

- A. Workstations which regularly display ePHI shall be positioned so as to reduce the likelihood of unauthorized viewing of ePHI. In high traffic areas privacy screen type devices shall be utilized to minimize unauthorized viewing of ePHI.

4. Log-Off Procedures

- A. Workforce members shall utilize automatic log-off options when leaving their work areas for extended periods of time.
- B. Workforce members shall log-off their computers at the end of each workday.

POLICY #7-14

HIPAA Physical Safeguards

Device and Media Controls Policy §164.310(d)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). To implement policies and procedures that govern the receipt and removal of hardware, electronic and analog media that contain ePHI into, out of, and within all County facilities this policy was adopted.

Policy Statement:

Lancaster County shall only dispose of or reuse media and/or equipment in an appropriate fashion to ensure the protection of all ePHI in their possession. This process shall include tracking, receipt and removal of hardware as well as electronic and analog media.

Procedures:

1. Disposal
 - A. Media
 - i. When storage media that contains ePHI is set for decommissioning it shall be disposed of in a secure manner. All media must be irretrievably destroyed. (A simple reformat is not sufficient as it does not overwrite the data.)
 - Disks and magnetic tapes can be degaussed or destroyed
 - Hard drives can be cleansed by a rewriting process
 - Optical media is not magnetic in nature so degaussing is not an option. In the case of CDR (write once) media, the media is to be destroyed. In the case of rewritable CDRWs overwriting is a viable alternative.
 - For flash drives/memory sticks, deguassing is not an option. Secure overwrites may be acceptable based on manufacturer specifications to ensure the data is not retrievable. If this is not possible they are to be destroyed.
 - Analog paper copies containing PHI should be mechanically shredded using either a strip cut shredder or a crosscut shredder.

B. Hardware

- i. Surplus equipment containing ePHI shall be routed to Information Services for proper disposal. Information Services shall be responsible for maintaining a log of such disposal.

2. Media Reuse

- A. Any hardware or storage media containing confidential information, including ePHI, or information for internal use only shall be erased by appropriate means or destroyed before the equipment or media is reused.

3. Accountability

- A. Information Services shall maintain an up to date inventory of hardware and software used by County agencies.
- B. All surplus operations of technology equipment shall be coordinated by Information Services.

4. Data Backup and Storage

- A. As outlined in Policy Number 7-08 (Contingency Planning - Data Backup, Disaster Recovery Plan, Emergency Operation Plan) all ePHI must be backed up on a regular basis. Backups should be tested regularly to ensure that ePHI can be retrieved.
- B. All backups shall be stored in a location different from the main data storage.

POLICY #7-15

HIPAA Technical Safeguards

Access Control Policy §164.312(a)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this policy is to ensure Lancaster County maintains an appropriate level of access controls proportionate to the sensitivity and criticality of networks, systems and applications containing ePHI.

Policy Statement:

Lancaster County is committed to implementing technical safeguards for information systems containing ePHI to allow data access only to those persons granted access rights as specified in §164.308(a)(4) of the Security Regulations.

Procedures:

1. Unique User Identification
 - A. All users who require access to any network, system or application will be provided with a unique user identification (user ID).
 - B. Each workforce member's unique user identification shall be based on standard naming conventions established by Information Services.
 - C. Workforce members shall not share their unique user identification or password with anyone.
 - D. If a workforce member believes their user identification has been compromised they must immediately report that security incident to Information Services.
 - E. A generic/shared user ID may be established for access to shared or common area workstations as long as the login provides no access to ePHI. A unique user ID and password must be supplied to access applications and database systems containing ePHI.
2. Emergency Access Procedure
 - A. Information Services shall establish procedures for obtaining access to necessary ePHI during an emergency. Necessary ePHI is defined as information that if not available could inhibit or negatively impact patient care.

- B. Systems that do not affect patient care are not subject to the emergency access requirement.
3. Automatic Lock Out Procedures
- A. All workstations and portable computing devices, and servers that access or store ePHI will utilize automatic lock out (e.g. password protected screen savers) procedures after 15 minutes of inactivity.
 - B. Department head or his/her designee shall periodically inspect workstations to ensure password protected screen savers are functioning properly.
4. Encryption and Decryption
- A. Encryption of ePHI as an access control mechanism is not required unless the department head or his/her designee of said ePHI deems the data to be highly critical or sensitive. Encryption of ePHI is required in some instances as a transmission control and integrity mechanism.
 - B. Proven, standard algorithms shall be used as the basis for encryption technologies.
 - C. Encryption keys shall be revoked upon termination, change in job responsibilities, or as a result of non-compliance.
5. Remote Access
- A. All remote access to the network must be coordinated through Information Services.
 - B. Remote access connections require authentication and encryption mechanisms when connecting via an Internet Service Provider (ISP) or dial up connection.
6. Wireless Access
- A. All wireless access to the network must be coordinated through Information Services.

POLICY #7-16

HIPAA Technical Safeguards

Audit Control Policy §164.312(b)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this policy is to ensure Lancaster County implements hardware, software and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI.

Policy Statement:

Lancaster County is committed to routinely auditing user activities in order to assess potential risks and vulnerabilities to ePHI in their possession. Administrative, physical and technical security measures will continue to be assessed and appropriate corrective modifications will be made as deemed necessary to continue compliance with the HIPAA Security Regulations.

Procedures:

1. Security Management Standards
 - A. See Policy #7-02 (Information System Activity Review) for the administrative safeguards for auditing system activities.
2. Physical Safeguards
 - A. See Policy Numbers 7-11, 7-12, 7-13, 7-14 for the physical safeguards for protection of ePHI in possession of Lancaster County.
 - B. Information Services shall acquire appropriate network based and host based intrusion detection systems.
 - C. Information Services shall be responsible for installing, maintaining and updating such systems.
 - D. Information services shall be responsible for testing (or having tested) the physical safeguards established to protect the network.

POLICY #7-17

HIPAA Technical Safeguards

Integrity Policy §164.312(c)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this policy is to protect the ePHI in the possession of Lancaster County from improper alteration or destruction.

Policy Statement:

Lancaster County shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Procedures:

1. Data Integrity
 - A. Lancaster County will use electronic mechanisms such as error correcting memory and RAID storage arrays to protect data from destruction and/or alteration.
 - B. Lancaster County will utilize appropriate tools and software packages to protect data from alterations and/or destruction from viruses and other malicious computer code. These systems will be updated on a regular basis.
 - C. Information Services shall acquire appropriate network or host based intrusion detection systems. Information Services shall be responsible for installing, maintaining and updating these systems.
 - D. Lancaster County will implement a mechanism to corroborate that ePHI is not altered or destroyed during transmission. (FTP)
 - E. To prevent programming errors Lancaster County will test all information systems for accuracy and functionality before utilizing them in a production environment.
 - F. Lancaster County will update systems when vendors release program fixes to correct known problems.

- G. Workforce members shall take appropriate precautionary measures to ensure that magnetic media is not damaged due to exposure to weather, magnetic fields or any other environmental conditions that can damage magnetic media.

POLICY #7-18

HIPAA Technical Safeguards

Person or Entity Authentication Policy §164.312(d)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this policy is to implement procedures to verify that the person or entity seeking access to ePHI is the one claimed.

Policy Statement:

Lancaster County is committed to maintaining formal procedures to verify that an individual or entity seeking access to ePHI is the one claimed.

Procedures:

1. Entity Authentication
 - A. All workforce members who use any network, workstation or application system that contains ePHI will be required to login with a unique user identification (User ID) and associated password as addressed in Policy #7-06 (Password Management).
 - B. Workforce members must not misrepresent themselves by using someone else's User ID and password. Similarly, workforce members must not allow others to use their User ID and password.
 - C. Access to password files shall be limited to a "least privilege" and "need to know" basis.
 - D. Employees found to have violated this policy shall be subject to disciplinary action up to and including termination of employment.

POLICY #7-19

HIPAA Technical Safeguards

Transmission Security Controls Policy §164.312(e)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Lancaster County has adopted this policy to guard against unauthorized access to ePHI being transmitted over an electronic communications network, to ensure electronically transmitted ePHI is not improperly modified without detection until disposed of, and to implement a mechanism to encrypt ePHI whenever deemed appropriate.

Policy Statement:

Lancaster County shall implement reasonable technical safeguards to protect the confidentiality, integrity and availability of ePHI transmitted over any electronic communications network.

Procedures:

1. Integrity Controls
 - A. Transmitting ePHI via any mobile media (flash drive, DC, DVD, removable hard drive, computer, phone) requires the files to be password protected.
 - B. The receiving entity shall be authenticated before transmission.
 - C. Lancaster County recognizes that all wireless LANs do not utilize standard 2.4 GHz, 5.0 GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on laptops, printers, etc. to transmit ePHI may not allow encryption of the data stream. We consider this to be a low risk concern because this implementation of infrared is very short in both distance and power.
 - D. Information Services shall maintain adequate firewall protection of the network. The firewall protection shall be configured to "deny" rather than "allow" as the default setting. Unused firewall ports shall be closed. Information Services security staff shall examine firewall logs and reevaluate the security configurations periodically.

2. Encryption

- A. All encryption mechanisms utilized for transmission of ePHI are to support a minimum of 128 bit encryption.

POLICY #7-20

HIPAA Documentation Requirements

Documentation Policy §164.316(b)(1)

Original Issue Date: 4/21/2005

Revised Date: 7/12/2016

Objective:

Lancaster County is committed to protecting electronic Protected Health Information (ePHI) in accordance with standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Policy Statement:

Lancaster County will maintain the policies and procedures implemented to comply with the Security Regulations in written form. If an action, activity or assessment is required to be documented by the Security Regulations, Lancaster County shall maintain a written record of the action, activity or assessment. Records may be maintained electronically.

Policy:

1. Time Limit
 - A. Lancaster County will retain documentation for 6 years from the date of creation or the date it was last in effect, whichever is later.
2. Availability
 - A. Lancaster County will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
3. Updates
 - A. Lancaster County will review documentation periodically and update as needed in response to environmental or operational changes affecting the security of ePHI. Lancaster County may change its policies and procedures at any time, provided the changes are documented and implemented in accordance with the Security Regulations.