CITY OF LINCOLN

HIPAA Security Policies and Procedures

Updated November 2013

Contents

CITY OF LINCOLN
HIPAA SECURITY POLICIES AND PROCEDURES

OVERVIEW / OBJECTIVES

The City of Lincoln 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 City of Lincoln's approach to compliance with the HIPAA Security Regulations, 45 CFR 160, 162, and 164, (hereinafter referred to as "the Security Regulations"). The City of Lincoln will:

- Ensure the confidentiality, integrity, and availability of all ePHI the City of Lincoln creates, receives, maintains, and transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required;
- Ensure compliance with the Security Regulations by its workforce.

DEFINITIONS

- **Workforce members** include all full and part-time employees, volunteers, contractors, temporary workers, and those employed by others to perform work on behalf of the City of Lincoln HIPAA covered departments and who have been granted access to City of Lincoln information, assets, and systems.
- **ePHI (electronic Protected Health Information)** consists of identifiable health information that can be readily associated with a specific individual. Health information means any information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. ePHI is individually identifiable information about an individual with health care information that is recorded, transmitted, and maintained in electronic formats.
- **Mobile Devices**: Examples of mobile devices are: Laptop/Notebook computers/electronic tablets/pocket PCs, Personal Digital Assistants (PDAs), Cellular phones with data capabilities.
- **Covered entity**: A City of Lincoln department, division, or agency, or portion thereof, that has
- been designated as a covered health care component of the City subject to HIPAA and these policies and procedures.
- **Business Associate:** A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.
- **Risk Analysis and Management Team**: Team established by E.O. 85314, consisting of the City Attorney assigned to HIPAA, City Privacy Officer, City Security Officer, Fire Battalion Chief assigned to HIPAA, and Department level Privacy Officers.

HIPAA SECURITY AND RELATED POLICIES

GENERAL POLICIES

Hybrid Entity and Key Role Assignments

The City of Lincoln is a hybrid entity under HIPAA with both covered and non-covered departments. The City of Lincoln hereby designates its HIPAA covered departments as health care components for purposes of the Security Regulations and establishes the HIPAA Privacy Officer and the HIPAA Security Officer.

Security Policies and Procedures

1. The City of Lincoln HIPAA Security Policies and Procedures are designed to ensure compliance with the HIPAA Security Regulations.
2. Such Security Policies and Security Procedures shall be kept current and in compliance with any changes in the law, regulations, or practices of the City of Lincoln's covered departments.
3. Workforce members will be appropriately trained on the importance of maintaining security.
4. The City of Lincoln will evaluate its Security Policies to determine their compliance with Security Regulations.

Sanctions and Non-Retaliation

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

Expectation of Privacy and City Rights to Deactivate Access

1. Workforce members and users of the City of Lincoln systems and workstations should have no expectation of privacy. To protect and manage its information systems and enforce appropriate security measures, Department Heads or Information Services may log, review, or monitor any data (ePHI and non-ePHI) stored or transmitted on its information systems.
2. The City of Lincoln may remove or deactivate any workforce member's user privileges and access to secured areas, when necessary to preserve the integrity, confidentiality, and availability of its facilities, user services, data, or ePHI.

Risk Analysis / Risk Reduction

The City of Lincoln shall conduct a thorough risk analysis to serve as a basis for HIPAA Security Regulation compliance efforts. Risk Assessment and Analysis will be conducted at least biannually and in response to breach of information events.

Other Related City Policies

1. All workforce members will comply with the City of Lincoln Internet and E-mail Usage Policy 99-2 to ensure that computers that access ePHI are used in a secure and legitimate manner.
2. The City will utilize the current Record Retention Schedules established by the Secretary of State, including:
   a. Schedule 24 (Retention Schedule for Local Agencies)
   b. Schedule 160 (Retention Schedule for Lincoln-Lancaster County – Health Department,)
   c. Schedule 148 (Lincoln Fire and Rescue)
   d. Schedule 99 (Lincoln City Attorney)
   e. Schedule 143 (Lincoln-Lancaster County Personnel Department)

SECURITY POLICIES

Audit Control and Incident Response Reporting

1. The City of Lincoln is committed to routinely auditing users' activities in order to assess potential risks and vulnerabilities of improper disclosure of ePHI in an ongoing fashion. Administrative, physical, and technical security measures will continue to be assessed and appropriate corrective modifications will be made as deemed necessary to continue to comply with the HIPAA Security Regulations.
2. The Security Officer is responsible for facilitating an Incident Response and Reporting System to identify, respond, mitigate, and document HIPAA security incidents, complaints, and violations.
3. All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI and response actions to mitigate must be reported.
4. Internal audit procedures will be implemented to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports.
5. The City of Lincoln shall perform ongoing reviews of system activities to identify and investigate potential security violations and take appropriate actions to minimize security violations.

Access Control

1. The City of Lincoln has established guidelines for determining each workforce member's need to access ePHI.
2. The City of Lincoln has established procedures for granting access to ePHI through a workstation, transaction, program, or process.
3. 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.
4. The City of Lincoln workforce members are responsible for being aware of, and complying with, the City of Lincoln Security Policies and Security Procedures.
5. The City of Lincoln has established procedures for terminating access to ePHI through a workstation, transaction, program, or process.

Technical / Physical Controls

1. Technical safeguards for information systems that contain ePHI will be implemented to allow data access only to those persons who have been granted access rights.
2. Formal procedures will be established to verify the identity of an individual or entity seeking access to ePHI.
3. Mobile devices that have 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.
4. 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 the normal operation of a computer system.
5. The City of Lincoln shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
6. The City of Lincoln shall implement reasonable technical safeguards to protect the confidentiality, integrity, and availability of ePHI transmitted over any electronic communications network.
7. The City of Lincoln will maintain Continuity of Operations and Disaster Recovery Plans to minimize the impact of emergencies or other events that negatively impact systems that contain ePHI.
8. The City of Lincoln shall only dispose of or reuse media and/or equipment in an appropriate fashion to ensure the protection of all ePHI in its possession. This process shall include the tracking of, receipt of, and removal of hardware, as well as electronic and analog media.

Facility Access Controls

Facility Security Plan: The department head or his/her designee at each facility (physical premises) that houses PHI (both electronic and analog) shall be responsible for developing, implementing, and maintaining a Facility Security Plan.

Training

The City of Lincoln 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.

Documentation

The City of Lincoln will maintain the policies and procedures implemented to comply with the Security Regulations in written (which may be electronic) form. If an action, activity, or assessment is required by the Security Regulations to be documented, the City of Lincoln shall maintain a written (which may be electronic) record of the action, activity, or assessment. (See also City Record Retention Policies).

Breach Notification

The City of Lincoln will establish guidelines to assure that Breach Notifications to individuals and to the Secretary of Health and Human Services are timely and complete.

HIPAA SECURITY PROCEDURES

Hybrid Entity and Key Role Assignments

1) The City Attorney's Office will maintain a current organizational chart that designates HIPAA covered departments/programs and departments that act as business associates.
2) The City Attorney's Office will maintain documentation of the assignment of the City of Lincoln HIPAA Security Officer, HIPAA Privacy Officer, and the Privacy and Security Officers within each HIPAA covered entity.
3) The Security Officer is responsible for
   a) The development and implementation of policies for the Security Regulations.
4) The HIPAA Security Officer is responsible for ensuring that the department:
   a) Complies with the City of Lincoln HIPAA Security Policies and Procedures;
   b) Maintains the confidentiality of all ePHI for which he/she is responsible;
   c) Assists in training all workforce members within the department at the appropriate level of HIPAA training.

Security Policies and Procedures

1) The City of Lincoln will implement reasonable and appropriate security measures to comply with the Security Regulations.
   a) To determine what is reasonable and appropriate the City of Lincoln will take into account its size, capabilities, complexity, technical infrastructure, hardware, software, security capabilities, the costs of the security measures, and the probability and criticality of potential risks to ePHI.
2) Periodic Evaluation: The City of Lincoln's Security Policies should be evaluated on a periodic basis to assure continued viability in light of technology, and environmental or operational changes that could affect the security of ePHI.
   a) The Security and Privacy Officers will, on an annual basis, review the Policies and Procedures the City of Lincoln has adopted for compliance with the Security requirements.
   b) The Security and Privacy Officers will develop and recommend to the City Attorney's Office, Information Services, and the Mayor, any necessary Security Policy or Procedure changes.
      i) Security Liaisons for each department where ePHI is available will review, on an annual basis, Security policies and procedures that apply to their department
      ii) When changes are made to Security Policies or Procedures, all department Officers will be notified of the changes.
3) Triggered Evaluations: In the event that one of the following events occurs, the policy review and evaluation process described above will immediately occur:
   a) Changes in the HIPAA Security Regulations or Privacy Regulations;
   b) New federal, state, or local laws or regulations affecting the privacy or security of ePHI;
   c) Changes in technology, environmental processes, or business processes that may affect HIPAA Security Policies or Security Procedures;
   d) A serious violation, breach, or other security incident occurs.

Sanctions and Non-Retaliation

1) To ensure all members of a covered department's workforce fully comply with the City of Lincoln Security Policies and Procedures, the City of Lincoln will appropriately discipline and sanction employees and other workforce members for any violation of the Security Policies and Procedures.
    a) 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.
    b) Discipline will be administered in accordance with the applicable labor agreement and/or the City of Lincoln Personnel Rules
    c) Other workforce members found to have violated any provision of these Security Policies and Procedures will be sanctioned appropriately.
    d) The covered department shall immediately inform the City of Lincoln Security Officer of all incidents that may lead to disciplinary action or sanctions pursuant to this policy.
    e) The City of Lincoln shall not retaliate against any person for reporting a security violation or for participating in the investigation of such violation.

Risk Analysis / Risk Reduction

Risk Analysis

1) The City of Lincoln acknowledges the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI that is associated with storing ePHI and transmitting ePHI inside the City of Lincoln, outside the City of Lincoln, and to other City departments that are not covered entities.
    a) The Risk Analysis and Management Team shall be responsible for coordinating the risk analysis. The Risk Analysis and Management Team shall identify appropriate Departmental representatives within the organization to assist with the ePHI analysis. The Risk Analysis and Management Team will conduct an analysis of the potential risks and vulnerabilities to ePHI by:
        i) Develop/update a comprehensive systems inventory including:
            (1) Hardware Inventory (network devices, workstations, printers, etc.);
            (2) Software Inventory (operating systems, applications, interfaces, etc.);
            (3) Update logical and physical network diagrams to illustrate the current environment.
        ii) Identifying and documenting all systems containing ePHI:
            (1) Document/describe ePHI;
            (2) Determine the source of the data (created versus received from a third party);
            (3) If received from a third party, identify source and method of receipt.
        iii) Determine if the data is forwarded to a third party.
            (1) If the data is forwarded, identify the receiver and method of transfer.
            (2) Determine the "criticality" (impact to the City if data were no longer available for a long or short period of time) of the software application and associated data.
            (3) Determine the "sensitivity" (potential harm that could result from a security breach) of the data.
        iv) Identify existing controls/policies/security measures in place to protect ePHI and assess the reasonableness and appropriateness of existing security measures protecting ePHI.
        v) Identify and assess any potential risks and vulnerabilities to the integrity, confidentiality, and availability of ePHI held;
            (1) Intentional malicious attacks (i.e. electronic based scanning, snooping, computer viruses)
            (2) Unintentional human errors (i.e. application/network programming problems)
            (3) Natural threats (i.e. storms, tornados, floods, etc.)
            (4) Environmental incidents (i.e. chemical spills, fire, power outage)

vi) Determine adequacy of existing controls, policies, and procedures and take necessary corrective actions identified in the aforementioned review.

vii) Institute and test necessary safeguards to ensure that ePHI is adequately protected and safeguarded. These actions could include vulnerability assessments/controlled hacking attempts (internal or external)

b) The Risk Analysis and Management Team will reassess the potential risks and vulnerabilities to the integrity, confidentiality, and availability of ePHI as part of a periodic review.

Risk Reduction

2) Reasonable and appropriate security measures will be implemented that are sufficient to reduce risks and vulnerabilities to ePHI. The Risk Analysis and Management 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:

(1) Changes in relationships (new ePHI is created/identified);

(2) New legislation related to ePHI (Federal, State, or Local);

(a) Occurrence of a breach in City security.

iii) Document their follow up procedures:

(1) Interviews:

(a) Analysis;

(b) Review New/Modified Policies;

(c) Recommendations/Modifications.

Audit Control and Incident Response Reporting

Audit Procedures

1) Internal audit procedures will be implemented to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports.

a) Log-in Monitoring:

i) Information Services will implement a mechanism to log and document failed login attempts on each system containing ePHI;

ii) Department head or designee will review such log-in activity reports and logs on a periodic basis;

iii) Procedures for reviewing logs and activity reports will be maintained;

iv) All failed log-in attempts of a suspicious nature, such as continuous attempts, must be reported to the City of Lincoln Security Officer.

b) The City of Lincoln Security Officer shall conduct periodic audits to determine whether actual access to ePHI by workforce members is in compliance with the established guidelines. The Security Officer shall conduct audits on at least an annual basis.

Information Services shall:

i) Conduct reviews of City information systems activities.

ii) Document these reviews including:

(1) Name of individual performing the review;

(2) Date and time of the review;

(3) Observations and findings;

(4) Corrective action taken;

(5) These reviews should be performed periodically (at least annually), or as indicated by a

known or suspected breach. Reviews shall include:

(a) Login activities (account lock outs)

(6) Security incidents (including failed network navigation attempts, malicious activities such as virus introductions and denial of service attacks, or activity probing activities).

Incident Response Action and Report

2) The Incident Response Action and Reporting Procedures:
   a) Any workforce member suspecting a security incident shall immediately notify his/her department head or his/her designee by telephone or in person. If the incident involves viruses, worms, or malicious code, network, or system attacks, he/she will also immediately inform Information Services.
      i) To the fullest extent possible, such employee shall provide the date, time, and incident specifics. This information is to be treated as confidential information.
   b) The department head or his/her designee shall immediately contact Information Services to minimize the negative impact of the security incident.
      i) Department Head or his/her designee shall work with Information Services to identify the extent and cause of the security incident.
   c) Additionally, the department head or designee shall fill out a Security Incident Form. The completed form should be sent to the City of Lincoln Security Officer. A copy should be kept at the affected department.
      i) The department head or designee and Information Services shall document the following to the fullest extent possible.
         (1) Assets that may have been compromised (hardware and software);
         (2) Any interviews related to the incident review.
   d) 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 (this report should then be part of the ongoing Risk Analysis review).

Access Control

Access Authorization

1) Access Authorization Procedures include the following:
   a) Department head or his/her designee is responsible for authorizing access to systems and networks containing ePHI for his or her subordinates.
      i) Workforce members are not permitted to authorize their own access to ePHI
      ii) The department head or his/her designee shall determine the necessary and appropriate level of access for workforce members to ePHI.
         (1) This determination should be based on their specific requirements to fulfill their job responsibilities and includes access to both hardware and software.
      iii) 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 access required for each such subordinate’s job role and responsibilities.

iv) Department head or his/her designee shall maintain a current list of levels of access to ePHI for all workforce members.

v) Information Services, in conjunction with the department head or his/her designee, shall determine the need for workforce members to utilize smart cards and/or tokens to facilitate their access to data.

b) 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. (See Sanctions)

c) The Department head or his/her designee is responsible for periodically reviewing the access to ePHI granted to each of his/ her subordinates and for modifying such access if appropriate.

d) 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.

Terminating Access

2) Terminating access to ePHI includes:

a) When a workforce member's employment or services are terminated or they transfer to another position, the Department head or his/her designee is responsible for ensuring that the workforce member's access to accounts that contain ePHI and applications containing ePHI are terminated. This includes, but is not limited to, access cards, keys, codes, and other facility access control devices. Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.

i) 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.

ii) The department head or designee will also determine if any other precautionary measures are to be taken (other physical security measures).

iii) To terminate access, the department head or designee shall notify Information Services and the departmental IT staff.

iv) Upon being asked to terminate access, Information Services and the departmental IT staff will:

(1) Inactivate the user account(s);

(2) Remove the user profile from all PC's;

(3) Where applicable, remove user from any remote connectivity systems;

(4) Where applicable, copy user folders to location specified by the department head or designee;

(5) In the event that smart cards or tokens are not returned to department head or designee, the department head or designee shall promptly provide Information Services with all information necessary to remove access.

3) Workforce member responsibilities

a) Workforce members shall utilize auto-log-off software, or software which inhibits access to ePHI when leaving their work areas for extended periods of time.

b) Workforce members shall log off of their computers at the end of each workday.

Technical / Physical Controls

Unique User Identification

1) Unique User Identification: All users who require access to any network, system, or application will be provided with a unique user identification (user ID).
   a) Each workforce member's unique user ID shall be based on standard naming conventions established by Information Services.
   b) Workforce members shall not share their unique user ID or password with anyone.
   c) If a workforce member believes his/her user ID has been compromised, he/she must report that security incident to Information Services.
   d) 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. An additional unique user ID and password must be supplied to access applications and database systems containing ePHI.

Password Management

2) Passwords / Entity Authentication
   a) All workforce members who use any network, workstation, or application system that contains ePHI will be supplied with and required to login with a unique user ID, and associated password.
   b) Workforce members must not misrepresent themselves by using someone else's User ID or password. Similarly, workforce members must not allow others to use their User ID or password.
   c) Access to password files shall be limited to a "least privilege" and "need to know" basis.
      i) Employees found to have violated this policy, shall be subject to disciplinary action up to and including termination of employment.
   d) All passwords used to gain access to any network or applications that contain ePHI must be of sufficient complexity to ensure that they are not easily guessed.
   e) Workforce members are responsible for the proper use and protection of their passwords. This includes:
      i) Passwords must not be disclosed to other workforce or family members.
      ii) Appropriate identification or verification shall be made of all persons representing themselves as service providers needing temporary access to machines that have access to any network.
      iii) Passwords shall not be written down, posted, or held in an insecure manner (i.e. on a post-it note).
      iv) A password must be changed immediately if it is suspected of being disclosed.
      v) Workforce members should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
   f) Automated password controls shall be set so that:
      i) All passwords are changed a minimum of every 56 days.
      ii) Workforce members cannot reuse a password on consecutive cycles.
      iii) Passwords must be a least six (6) digits in length and contain a minimum of
         (1) One alphabetic character;
         (2) One numeric characters (0-9);
         (3) One of the following special characters (#,$,@).

Accountability

3) Accountability
   a) Information Services shall maintain an up-to-date inventory of hardware and software used by City agencies.
   b) All disposal of surplus technology equipment shall be coordinated by Information Services.

Data Integrity

4) Data Integrity
   a) The City of Lincoln will use electronic mechanisms such as error correcting memory and RAID storage arrays to protect data from destruction and/or alteration.
   b) The City of Lincoln 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) To prevent programming errors, the City of Lincoln will test all information systems for accuracy and functionality before utilizing them in a production environment.
   e) The City of Lincoln will update their systems when vendors release program fixes to correct known bugs or problems.
   f) Workforce members shall take appropriate precautionary measures to ensure that magnetic media is not damaged due to exposures to weather, magnetic fields, or any other environmental conditions that can damage magnetic media.

Protection from Malicious Software

5) 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 notify all departments and users of new and potential threats from malicious code.
   c) Departments and users must notify Information Services if a virus, worm, or other malicious code has been identified in a City computer system.
   d) Information Services shall be responsible for acquiring and keeping anti-virus software and tools current and for taking the necessary steps to prevent the spread of discovered/identified viruses, including:
      i) Acquiring such software for all City computing devices.
      ii) Keeping current signature files available for installation. Whenever possible, automated means shall be used to ensure that these updates are performed on a regular basis in an automated fashion with minimal workforce manual intervention.
      iii) Upon the identification of malicious software on a City computing device, Information Services shall take the necessary steps to prevent the spread of the virus.
      iv) Upon containment, Information Service or the appropriate departmental staff (in the case of devices being maintained or supported by other City offices or third party vendors) shall properly secure or isolate the infected file(s) from the rest of the network and clean and repair such infected files.

Automatic Lockout

6) Automatic Lock Out / Encryption and other Access Control tools
   a) All workstations and servers that access or store ePHI will utilize automatic lock out (e.g. password protected screen savers) procedures after a reasonable period of time as determined by the department head.
   b) The department head or his/her designee shall periodically inspect workstations to ensure password protected screen savers are functioning properly.
   c) 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.

        i) Encryption of ePHI is required in some instances as a transmission control and integrity mechanism.
        ii) Proven, standard algorithms shall be used as the basis for encryption technologies.
        iii) Encryption keys shall be revoked upon termination, change in job responsibilities, or as a result of non-compliance.

Physical Safeguards

7) Physical Safeguards
    a) Information Services shall acquire appropriate network based and host based intrusion detection systems.
    b) Information Services shall be responsible for installing, maintaining, and updating such systems.
    c) Information Services shall be responsible for testing or having tested the physical safeguards established to protect the network.
    d) All remote access to the network must be coordinated through Information Services.
        i) Use of remote access connections requires proven, standard authentication and encryption mechanisms.
            (1) All wireless access to the network must be coordinated through Information Services.

Disposal of Media and Equipment

8) Disposal of Media and Equipment
    a) When storage media that contains ePHI is set for decommissioning, it shall be disposed of in a secure manner. All media (e.g. floppy diskettes, ZIP disks, magnetic tapes, hard drives, CD's, optical disks, flash cards, USB memory sticks, and analog hard copies) must be irretrievably destroyed. A simple reformat is not sufficient as it does not overwrite the data.
        i) Disks (e.g. floppies, ZIP disks, and the like) and magnetic tapes (both reel to reel and cartridges) must be "degaussed" or destroyed.
        ii) Hard drives must be cleansed by a re-writing process.
        iii) 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 re- writable (CDRW's), over-writing can be used as a viable alternative.
        iv) Flash Memory (including memory sticks), degaussing is not an option because of its composition. In the case of this media, secure over writes may be acceptable based on manufacturer specifications to ensure that data is not retrievable. If this is not possible, the flash memory devices are to be destroyed.
        v) Analog paper copies which contain PHI should be mechanically shredded using either a strip cut shredder or a cross-cut shredder.
    b) The Records Retention Schedule may require assurance that the data has been secured and is available and accessible. (See pertinent Record Retention Schedules for local government as set by the Secretary of State Record Retention Schedules).
    c) Surplus equipment that contains ePHI shall be routed to Information Services for proper disposal. Information Services shall be responsible for maintaining a log of such disposal.

Media Re-Use

9) Media Re-use
    a) Any hardware or storage media that contains confidential information, including ePHI, or information for internal use only shall be erased by appropriate means or destroyed before the equipment or media is re-used.

Backups / Contingency / Emergency and Disaster Recovery

10) Backups / Contingency / Emergency and Disaster Recovery

a) Information Services and departmental IT staff will establish and implement a Data Backup Plan which will allow for the successful retrieval of all data and files on systems that are supported at the Data Center.

b) Information Services will assist agencies who perform their own system support from remote locations to ensure that they can successfully retrieve all data and files from their data systems.

i) The Data Backup Plan will require that all media used for the backups are stored in a physically remote location for the system hardware and in a physically secured facility;

ii) Data backup procedures should be tested on a periodic basis to ensure that files are retrievable.

c) Information Services and departmental IT staff 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.

i) Systems that do not affect patient care are not subject to the emergency access requirement;

ii) The City of Lincoln will assess the **relative criticality of specific applications and data** in support of other contingency plan components.

d) Information Services will create and maintain a plan to recover from the loss of data due to an emergency or disaster. The plan will:

i) Consider the level of disaster and the estimated impact on City operations;

ii) Include procedures for the restoration of data systems;

iii) Be documented and easily available to the necessary personnel at all times

e) The City of Lincoln will establish procedures to continue critical business operations during an emergency. This plan will:

i) Include provisions for the continued protection of ePHI during the emergency period;

ii) Be documented and easily available to the necessary personnel at all times;

iii) The department head or his/her designee will create procedures to allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan.

f) Testing and Revision Procedure

i) Data backup procedures should be tested on a periodic basis to ensure that exact copies can be retrieved;

ii) The Disaster Recovery Plan should be tested on a periodic basis to make sure systems and data can be restored or recovered;

iii) Emergency mode operation procedures should be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

Integrity Controls

11) Integrity Controls

a) Transmitting ePHI via a removable media (e.g. floppy disk, memory stick, CD, DVD, or removable hard drive) requires the files to be password protected.

i) The receiving entity shall be authenticated before transmission;

ii) The City of Lincoln 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 PDAs, laptops, and printers 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;

iii) Information Services shall maintain adequate firewall protection of the network. The firewall protection shall be configured to "deny" rather than "allow" as their default settings. Unused firewall ports shall be closed. Information Services security staff shall examine firewall logs and reevaluate the security configurations periodically;

iv) All encryption mechanisms utilized for the transmission of ePHI are to support a minimum of 128 bit encryption.

Facility Access Controls

1) The department head or his/her designee shall review access and 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:
   a) Access controls;
   b) Validation;
   c) Fire suppression equipment (halon, sprinklers);
   d) Smoke detectors;
   e) Fire alarms;
   f) UPS Systems and/or Power conditioners;
   g) Back-up generator facilities;
   h) Surge suppressors;
   i) Heat and humidity sensors and controls;
   j) HVAC systems for computer rooms.
2) Access Control and Validation Procedures: The department head or his/her designee will ensure:
   a) Procedures to control and validate workforce members' access to facilities where PHI (both electronic and analog) is maintained or available for review.
   b) Procedures to secure the physical locations where PHI is stored. This would include data centers, data closets, file cabinets, and desks
   c) Facilities where PHI is available will have appropriate physical access controls to limit access to the facility. This would include such things as key locked doors, code locked doors, and/or badge reader locked doors.
3) Maintenance Records: 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.
4) Physical Configuration of Work Areas: Workstations which regularly display ePHI will be positioned to reduce the likelihood of unauthorized viewing of ePHI.

Training

1) The covered departments and departments acting as Business Associates shall provide ongoing information security awareness and education for all members of their workforce.
   a) This shall cover information security basics, associated policies, procedures, and workforce member responsibilities.
   b) This 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) This will include informing 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 the City of Lincoln’s Security Policies and Procedures and their role in protecting the City of Lincoln’s information systems and information assets by signing an Employee Acknowledgment Form.
   e) The department head or designee shall be responsible for collection and management of the signed Employee Acknowledgment Form.

2) The covered department and departments acting as Business Associates shall hold an annual awareness and education session to review information security basics and current information security policies with workforce members under their supervision.
   a) This can be in conjunction with any privacy training.
   b) The HIPAA Privacy and Security Policies will be reviewed annually with each person employed or under contract with each covered department. The date of the review and signature of the staff/contractor will be appended to the annual evaluation or contract renewal or other record maintained by the department.
3) The covered department shall reinforce to all other authorized users the importance of information security and their role in protecting the City of Lincoln’s information systems and information assets through the terms of a Business Associate Contract, where applicable.
4) 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.

Documentation

1) The City of Lincoln will retain the documentation for 6 years from the date when it last was in effect, or as required by City of Lincoln and State Record Retention Policies, whichever is later.
2) The City of Lincoln will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
3) The City of Lincoln will review documentation periodically and update as needed, in response to environmental or operational changes affecting the security of ePHI.

Breach Notification

1) Upon learning of an impermissible acquisition, access, use, or disclosure of protected health information, a breach will be presumed. The City Privacy and/or Security Officer will begin an investigation and, if appropriate, risk assessment to determine if the probability that the PHI has been compromised. This investigation shall begin as soon as practical and in no case more than 5 days after learning of the potential breach.

Incident investigation.

2) The incident and investigation will be documented. This will include the source of the discovery, the date discovered, the date of the breach, if known, and the PHI that was breached.
3) The City Security Officer shall determine if the impermissible use or disclosure of PHI was unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable.
   (i) Acceptable methods of rendering PHI unusable, unreadable, or indecipherable include:
      i. Encryption: valid encryption processes are those consistent with federal guidelines for protecting PHI.
      ii. Destruction: Media on which the PHI is stored or recorded must be destroyed before discarding: Paper, film. or other hard copy is shredded. Electronic media must be cleared, purged, or destroyed.

4) PHI was secured: This will be documented as such and the breach notification review closed. The Privacy and Security Officers will report to the City Risk Analysis and Management Team.

5) PHI was unsecured: Sufficient information will be gathered by workforce interviews, technical review, and other analysis to determine if the breach was an excepted circumstance. The three exceptions to be considered are:
   - (i) Any **unintentional** acquisition, access, or use of PHI by a work force member or person acting under the authority of a covered entity or business associate if it was made in good faith and within the scope of authority of the relationship and does not result in a further use or disclosure not permitted by HIPAA Privacy Rules.
   - (ii) Any **inadvertent** disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business association, provided that the recipient does not further disclose the information in violation of the HIPAA Privacy Rules.
   - (iii) A disclosure of PHI where a covered entity or business associate has a **good faith belief** that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

6) Impermissible use or disclosure of unsecured PHI is determined to NOT be an exception: A four factor risk assessment will be conducted to determine the probability of a compromise to the PHI.
   - (i) Determine if immediate notification of the individual and Department of Health and Human Services is needed.
   - (ii) Conduct four factor risk assessment
     - i. Nature and extent of the protected health information involved, including the types of identifiers and the likelihood of reidentification;
     - ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
     - iii. Whether the protected health information was actually acquired or viewed; and
     - iv. The extent to which the risk to the protected health information has been mitigated.

7) Based on the risk assessment, a determination will be made regarding the probability that the privacy and security of PHI was compromised.
   - (i) If it is determined the probability is low:
     - i. This will be documented and the investigation closed;
     - ii. The investigation and findings will be reviewed with the City Attorney assigned to HIPAA and with the City Risk Analysis and Management Team.
   - (ii) If it is determined that the probability of compromising the unsecured PHI is anything except low:
     - i. The City Privacy and/or Security Officer will promptly and without delay begin the notification process:
       1. In no case shall the notification be longer than 60 days after discovery;
       2. Determine if additional services need to be offered such as toll free number or credit monitoring services;
       3. Review the listing of individuals affected by the breach:
          - a. Determine the number (less than 500 or more than 500);
          - b. Determine if there are valid and current contact addresses for these individuals;
          - c. If there are more than 500 individuals, review the zip codes to determine jurisdictions represented;
          - d. Determine if there are other obligations (e.g. translation, disability requirements).
       4. If addresses are insufficient or out of date (10 or more out of 500 or less) or more than 500 individuals are affected, public notice must be given. This may include press release or prominent notice on the city website.

Notification of individuals:

8) All individuals with unsecured PHI that has been compromised will be notified. The written notification will include:
   (i) A brief description of what happened, including the date of the breach and the date of the discovery of the breach;
   (ii) A description of the types of unsecured PHI that 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 covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches;
   (v) Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, or postal address.
9) If urgent individual notification is needed, it will be made by telephone or email. This will be in addition to written notification.
10) If the individual is deceased, a minor, or incapacitated, the notification will be sent to the personal representative or parent or guardian.

Notification of Department of Health and Human Services

11) For a breach affecting fewer than 500 individuals, determine if an immediate notification to the Department of Health and Human Services is needed or preferred.
12) Notify the Department of Health and Human Services or
13) Maintain a log and submit within 60 days of the end of the current calendar year
14) Submit notification at http://ocrnotifications.hhs.gov
15) For a breach affecting more than 500 individuals in addition to the individual notification, The Security Officer shall comply with the notification requirements for breaches of more than 500 individuals, including:
16) a. Press release
17) b. Report to the Department of Health and Human Services concurrent with the press release
18) c. If law enforcement requests a delay:
   (i) A written request with a timeframe for the delay is preferred.
   (ii) Immediately after the expiration of time frame specified by the written statement from law enforcement, the Security Officer will commence notification procedures.
19) Breach notification will be followed by additional workforce training and mitigation efforts.