LANCASTER-LEBANON

INTERMEDIATE UNIT NO. 13

HIPAA & HITECH

PRIVACY AND SECURITY COMPLIANCE

Table of Contents

3. Minors

SECURITY POLICIES AND PROCEDURES

Technical Safeguards

1. Access Controls
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

Physical Safeguards

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Administrative Safeguards

1. Security Management Process
2. Assigned Security Responsibility
3. Standard Workforce Security
4. Information Access Management
5. Training
6. Security Incident Procedures
7. Contingency Plans
8. Evaluations

Introduction

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13 (the "IU") is committed to maintaining the security of the protected health information ("PHI") it creates, receives maintains or transmits, which is subject to the HIPAA statute and its related Privacy and Security Rules (collectively, "Original HIPAA"), as amended by the HITECH statute ("HITECH") and the Omnibus Rule (the "Omnibus Rule" and collectively with HITECH and the Omnibus Rule, "HIPAA"). The IU has adopted the attached Privacy and Security Policies and Procedures (the "Privacy and Security Policies and Procedures") to govern its access to and uses and disclosures of PHI in accordance with HIPAA, HITECH and applicable State law relating to the privacy and security of PHI.

The Privacy and Security Policies and Procedures apply to all information and data resources processed and maintained by and through the IU that include PHI, including network domains and their related connected devices, desktop and portable computing systems, communication networks, both voice and dated related devices, software products, paper files, records, magnetic media, film, fiche, imaging and disk storage systems, and the data on these systems. The Privacy and Security Policies and Procedures apply to all officers, managers, employees and contractors of the IU and any violation of the Privacy and Security Policies and Procedures will result in appropriate disciplinary action, up to and including termination of employment or contracts.

The IU has appointed a HIPAA Privacy Officer and a HIPAA Security Officer for the IU, responsible for promoting and enhancing its continuing commitment to confidentiality relating to PHI and ensuring compliance with HIPAA and other federal and state laws relating to the privacy and security of PHI.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13'S

HIPAA COMPLIANCE PROGRAM:

PRIVACY POLICIES AND PROCEDURES

* Unless otherwise defined in these Privacy Policies and Procedures, the terms used herein shall have the meanings and definitions assigned to such terms in the HIPAA Privacy and Security Regulations, 45 C.F.R Part 160, 162 and 164.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **MINIMUM NECESSARY STANDARD**

Date Adopted: **February 12, 2014**

Policy:

When using or disclosing PHI, or when requesting PHI from other sources, LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13 (the "IU") makes reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of any use, disclosure or request ("Minimum Necessary").

The IU applies the Minimum Necessary standard to all Privacy and Security Policies and Procedures adopted by the IU, except that the IU does not apply the Minimum Necessary standard to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the patient;
- Uses or disclosures made pursuant to a valid Authorization;
- Disclosures made to the Department of Health and Human Services;
- Uses or disclosures that are required by law; or
- Uses or disclosures that are required for compliance with the IU's Privacy and Security Policies and Procedures.

To the extent practicable, the IU delineates the specific staff members who are permitted to access PHI as necessary to perform their jobs.

Procedures:

To the extent practicable, the IU shall limit the use, disclosure or release of PHI to either:

1. the Limited Data Set for such PHI, which shall exclude the following direct identifying information of the individual or of relatives, employers, or household members of the individual:

    - Names;
    - Postal address information, other than town or city, State, and zip code;
    - Telephone numbers;
    - Fax numbers;
    - Electronic e-mail addresses;
    - Social security numbers;
    - Medical record numbers;
    - Health plan beneficiary numbers;
    - Account numbers;
    - Certificate/license numbers;
    - Vehicle identifiers and serial numbers, including license plate numbers;
    - Device identifiers and serial numbers;
    - Web Universal Resource Locators ("URLs");
    - Internet Protocol ("IP") address numbers;
    - Biometric identifiers, including finger and voice prints; and

- Full face photographic images and any comparable images;

OR

2. the Minimum Necessary amount of PHI to accomplish the intended purpose of the use, disclosure, or request. The IU or, where applicable, a Business Associate of the IU, or a Covered Entity for which the IU is a Business Associate, shall determine what constitutes the Minimum Necessary to accomplish the intended purpose of such disclosure.

If a request for, or use of, PHI by another person appears to be unwarranted or excessive, any concerned employee may consult with the person requesting the information to determine whether the scope of the request is appropriate, and must consult with the HIPAA Privacy Officer if it appears that use or disclosure exceeds the Minimum Necessary. In such an event, the PHI shall not disclosed or used in the manner requested until the HIPAA Privacy Officer approves the requested use or disclosure.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **SCOPE OF ACCESS BY WORKFORCE**

Date Adopted: **February 12, 2014**

Policy:

The IU has made determinations about internal Minimum Necessary disclosures and uses of PHI based on employee role or class of workforce, and has identified the category of persons who are permitted access to designated categories of information and the conditions, if any, of that access. Employees of the IU are expected to abide by the internal restrictions established by the IU and not access any PHI or categories of PHI if access is not required in connection with the employee's job functions.

Procedures:

1. Identify, by title or job description, all employees or categories of employees or other persons under the control of the IU who will need access to PHI to perform their duties.

2. Implement Technical and Administrative Safeguards (see the IU's Security Policies and Procedures) to ensure internal restrictions and boundaries to access of PHI are established.

3. Train employees on their level of permissible access to PHI based on job function.

4. Enforce and apply sanctions for non-compliance with this policy in accordance with the IU's Sanctions policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **REASONABLE SAFEGUARDS**

Date Adopted: **February 12, 2014**

Policy:

The IU uses administrative, technical, and physical safeguards to: (i) protect the privacy of PHI; (ii) reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the IU's Privacy Policies and Procedures; and (iii) limit incidental uses or disclosures of PHI made pursuant to an otherwise permitted or required use or disclosure.

Procedures:

- When using or disclosing PHI, the IU makes reasonable efforts to limit the information used or disclosed to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request.
- Conversations containing PHI shall be kept to a minimum while in public places or while people who are unauthorized to access PHI are near or within the IU's offices.
- Computer monitors shall be turned away from public view.
- Computer passwords shall be kept confidential and shall not be shared with others or posted in or around the computer.
- Fax machines shall be placed in secure locations and PHI shall be retrieved from the machines promptly.
- Fax machines, copy machines and other equipment that may retain information on hard drives or otherwise, such as computers, laptops, smartphones and other handheld devices, shall be scrubbed of all data before being withdrawn from service, transferred by the IU, disposed of, or sent offsite for repairs.
- Business Associate Agreements shall be obtained from all appropriate persons/entities.
- File cabinets containing PHI shall be secured, and personnel with access to such records shall be limited.
- The identity and authority of requesting individuals must be verified for permitted disclosures of PHI in accordance with the IU's Verification of Identity policy.
- Documents containing PHI must be shredded prior to disposal.
- Periodic "walk-though" inspections of the premises shall be conducted to determine whether there are any obvious unintentional disclosures of PHI (i.e., open file cabinets with member names showing on files, etc). PHI (whether oral or written) must be protected and kept confidential at all times, unless it is permitted to be disclosed under the IU's Privacy and Security Policies and Procedures.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **VERIFICATION OF IDENTITY**

Date Adopted: **February 12, 2014**

Policy:

Prior to making any disclosures of PHI, the IU: (i) verifies the identity of the person requesting the PHI; (ii) verifies the authority of the person to have access to the PHI; and (iii) obtains documentation, statements or representations, whether oral or written, from the person requesting the PHI, when such documentation, statements or representations are a condition of disclosure under the IU's policies.

If reasonable under the circumstances, the IU may rely on documentation that meets the applicable requirements set forth below. In addition, the IU may reasonably rely on any of the following to verify identity when the disclosure of PHI is to a public official or to a person acting on behalf of the public official:

- If the request is made in person, there is presentation of an agency identification badge, other official credentials, or other proof of government status;
- If the request is in writing, the request is on the appropriate government letterhead; or
- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead is provided stating that the person is acting under the government's authority or other evidence or documentation is provided, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

The IU shall exercise professional judgment and good faith when disclosing PHI.

Procedures:

If a request for PHI is made over the telephone, the IU may release PHI provided the identity and authority of the requester is verified and the proper documentation, statements or representations are obtained from the requester.

If the identity or authority of any person requesting PHI is not known to the particular IU employee, the employee must verify the identity and authority of the requester by alternate means. Verification may be made by requesting certain information assumed to be known only to the individual, such as the individual's driver's license number and a second piece of information, such as date of birth, address or mother's maiden name.

Where the person requesting the PHI appears in person, the IU shall request documentation to verify identity. The requesting individual can be asked for one or more of the following:

- Photo identification (e.g., driver's license);
- Birth Certificate;
- Passport.

Verification of the authority of the requester should be satisfied prior to permitting the requester access to the PHI.

Where applicable, specific documentation of authority should be obtained (e.g., identification as a parent or guardian, appointment as executor or other appropriate relationship to the individual).

The IU shall document the basis for the release of the PHI and the disclosure under the IU's Accounting of Disclosures policy, as required.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **ACCEPTING NON-IU AUTHORIZATIONS**

Date Adopted: **February 12, 2014**

Policy:

Except for uses and disclosures of PHI for purposes of treatment, payment or health care operations and uses and disclosures under a few, select other circumstances permitted under the IU's Privacy Policies and Procedures, PHI is not to be used or disclosed without first obtaining a signed "Authorization" that complies with the requirements of HIPAA. See form included after the IU's Sale of PHI policy.

In addition, PHI is not to be used or disclosed without first obtaining a signed Authorization when the use or disclosure involves psychotherapy notes, except where the use or disclosure is for purposes of treatment, payment or health care operations in the following situations in the following situations only:

(i) use by the originator of the psychotherapy notes for treatment;

(ii) use or disclosure by the IU for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve skills in group, joint, family, or individual counseling;

(iii) use or disclosure by the IU to defend itself in a legal action or other proceeding brought by the individual who is the subject of the psychotherapy notes;

(iv) use or disclosure that is required by the Secretary of the Department of Health and Human Services to investigate or determine the IU's compliance with HIPAA, or is required by law and complies with and is limited to the relevant requirements of such law;

(v) use or disclosure permitted under HIPAA for specified health oversight activities with respect to the originator of the notes;

(vi) use or disclosure to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law; or

(vii) use or disclosure necessary to avert a serious threat to health or safety, but only where the use or disclosure is consistent with applicable law and standards of ethical conduct and where the IU believes, in good faith, that the use or disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public and is made to a person or persons reasonably able to prevent or lessen the threat, including the target of threat.

The IU's "pre-approved" HIPAA-compliant Authorization form is used, whenever possible. If it is not possible to use the IU's form of Authorization, the IU ensures, before accepting and relying upon another form of authorization (a "Non-IU Authorization"), that the Non-IU Authorization complies with the requirements of HIPAA.

Procedures:

1. Whenever an individual presents the IU with a Non-IU Authorization to release PHI, the IU will request the individual to use the IU's form instead.

2. If the individual cannot or will not accept the use of the IU's form, the IU employee shall consult with the IU's HIPAA Privacy Officer and verify that the Non-IU Authorization is "Valid" before relying upon it to release PHI.

3. A Non-IU Authorization may be deemed Valid only if it:

   (a) Is not deemed "Invalid" by virtue of step 4 below; and

   (b) Contains all of the following "Core Elements":

      (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

      (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

      (iii) The name or other specific identification of the person(s), or class of persons, to whom the IU may make the requested use or disclosure;

      (iv) A description of each purpose of the requested use or disclosure. The statement "At the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;

      (v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the Non-IU Authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository;

      (vi) A statement setting forth the individual's right to revoke the Non-IU Authorization in writing and the exceptions to the right to revoke (if any), together with a description of how the individual may revoke the Non-IU Authorization and a reference to the applicable Notice of Privacy Practices;

      (vii) A statement regarding the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the Authorization;

      (viii) A statement that information used or disclosed pursuant to the Non-IU Authorization may be subject to another disclosure by the recipient and may no longer be protected;

      (ix) A reference to the applicable Notice of Privacy Practices provided to the individual concerning the uses and disclosures of PHI that may be made by the IU, and of the individual's rights and the IU's legal duties with respect to PHI; and

      (x) Date and signature of the individual or, if the Non-IU Authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual;

(c) Any additional elements or information contained therein are not contradictory to any of the Core Elements described above; and

(d) Is written in easy to understand language.

4. A Non-IU Authorization must be deemed Invalid when it has any of the following defects:

(a) The expiration date has passed or the expiration event is known by the IU to have occurred;

(b) The Non-IU Authorization has not been filled out completely;

(c) The Non-IU Authorization is known by IU to have been revoked;

(d) Where the Non-IU Authorization is a compound Authorization, it lacks an element required by the compound Authorization section of the IU's Privacy and Security Policy and Procedures;

(e) The Non-IU Authorization violates the prohibition on conditioning of authorizations as described in the IU's Privacy and Security Policy and Procedures; or

(f) A material provision in the Non-IU Authorization is known by the IU to be false.

5. If a Non-IU Authorization is Invalid, do not accept the Non-IU Authorization and suggest instead that the individual return it to the person or organization from which it was obtained to either obtain a new, Valid Authorization, or request such person or organization use the IU's Authorization form.

The IU shall document and retain any signed Authorization for a period of at least six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **RESOLUTION OF COMPLAINTS**

Date Adopted: **February 12, 2014**

Policy:

The IU provides a mechanism for reporting any issue of non-compliance with HIPAA. The IU and its employees and agents shall not threaten, intimidate or retaliate against any individual who files a complaint. Every person within the IU has direct access to and is encouraged to consult with the HIPAA Privacy Officer about issues of non-compliance with HIPAA. This policy applies to all of the IU's employees and agents.

Procedures:

Employee Reporting

- An employee or agent of the IU who acquires information that may give rise to a reasonable belief that (i) another employee or agent is engaged in conduct that violates any provision of HIPAA, or (ii) an agent, representative or other person or firm representing the IU in any transaction is engaged in conduct that violates HIPAA, shall promptly report such information to the HIPAA Privacy Officer.

- Reports to the HIPAA Privacy Officer shall be made in person, by telephone, in writing or e-mail. A sample report form is attached.

- The HIPAA Privacy Officer shall maintain a notebook log (the "Log") of all reports regarding HIPAA privacy matters. Each report shall be assigned a sequential file identification number by the HIPAA Privacy Officer for the specific year and shall be used for new or additional information on the same matter. The caller/author shall not be required to provide his/her name or any other facts that may give away his/her identity. If the caller/author provides his/her identity, then he/she shall be provided with the file identification number for the reported matter on a confidential basis. The caller/author shall be encouraged to provide as much information as possible to assist with the investigation of the matter. The caller/author shall also be advised that the HIPAA Privacy Officer will use reasonable efforts to keep the identity of the caller/author confidential; however, there may be a point in time when the individual's identity may become known or may have to be revealed.

- The HIPAA Privacy Officer shall conduct an investigation of the report, make a record in the Log of the results and the specific actions taken after completion of the investigation. The specific facts and circumstances surrounding the report must be kept confidential and any discussions regarding the complaints shall be limited to those parties with a "need to know" during the investigation.

- Upon final resolution of a problem, the HIPAA Privacy Officer shall provide feedback to the IU **[SPECIFY ANY SUBSET OF THE IU?]** regarding the possible need for a change to the IU's Privacy and Security Policies and Procedures. In addition, the HIPAA Privacy Officer shall prepare periodic reports to be submitted to the IU on the status of the IU's compliance with HIPAA and these Privacy and Security Policies and Procedures.

- No action should be taken against any employee for the good faith reporting of any suspected violation of HIPAA, regardless of whether such suspected violation is ultimately determined to exist following an investigation.

Privacy Investigation and Log.

The HIPAA Privacy Officer shall document, adequately investigate (or oversee the investigation of) and, in accordance with the direction of the IU [**SPECIFY ANY SUBSET OF THE IU?**], appropriately respond to each report of a suspected violation of HIPAA. The HIPAA Privacy Officer shall maintain a Log book that documents the following items in connection with these matters:

- Sequential file identification number;
- Date of report of a potential violation is received;
- Whether the reporter has identified himself or herself and has been advised of the file identification number;
- Whether the reporter has brought the matter to the attention of his or her immediate supervisor (and if not, why not);
- Description of the incident;
- Identification of the person designated as being primarily responsible for investigating the incident, and identification of any outside counsel or external consultants retained to assist in evaluation and investigation of the incident;
- Current status of the investigation, as periodically updated; and
- Date matter is resolved and type of resolution, including corrective action taken, where appropriate.

A copy of the form that will be used by the HIPAA Privacy Officer to document the reports is attached. The HIPAA Privacy Officer shall document the complaint and resolution and maintain all files in a secure location for a period of at least six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Sequential File ID #: _____

REPORT OF HIPAA COMPLAINT

(To be Completed By HIPAA Privacy Officer)

Name of Reporting Person (*optional*) ("Reporter"): _____

Position Held by Reporter (*optional*):_____

Date of this Report:_____

1. Describe the incident or activity that constitutes potential wrongdoing, including the name(s) of the person(s) involved and, if known, the date(s) of the relevant incident(s):_____
_____
_____

2. Describe when and how Reporter became aware of this activity: _____
_____

3. Describe any evidence that exists to prove the potential wrongdoing or other means available to verify relevant incident(s): _____
_____
_____

4. List any other person(s) inside or outside of the IU who may be able to verify the relevant incident(s):
_____
_____
_____

5. Has Reporter discussed the relevant incident(s) with any other person(s) inside or outside of the IU? Yes ____No ____. If "Yes," list the identity of such person(s):
_____
_____
_____

6. Would Reporter be willing to discuss the potential wrongdoing with others at the IU (e.g., [**SPECIFY**])? Yes _____No _____.

Note: Confidentiality is to be strictly observed except where report disclosure is determined to be required for further action and resolution.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **MITIGATION OF IMPROPER DISCLOSURES**

Date Adopted: **February 12, 2014**

Policy:

The IU mitigates, to the extent practicable, any harmful effect that is known to it that could or does arise from a use or disclosure of PHI in violation of HIPAA and these Privacy Policies & Procedures.

Procedures:

If an improper use or disclosure of PHI in violation of HIPAA or the IU's Privacy Policies & Procedures is discovered, or the IU is advised of a violation of HIPAA or its Privacy Policies & Procedures by the IU, a Business Associate or a Subcontractor, the IU shall:

- Take reasonable efforts to halt the improper use or disclosure, and shall mitigate any harmful effects of the use or disclosure; and

- Contact the HIPAA Privacy Officer immediately to determine the appropriate steps going forward.

In the event the improper use, disclosure or violation is isolated, the HIPAA Privacy Officer shall monitor remediation and refer any individual involved for re-training on the specific issue related to the improper disclosure.

In the event the improper use, disclosure or violation appears to be widespread, the HIPAA Privacy Officer shall document the event, re-evaluate safeguards and make changes, with the approval of the IU, as needed, and monitor remediation activities.

If a situation involves the possibility of a security breach, see the Security Breach Notification policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **COMPLIANCE WITH BREACH NOTIFICATION LAWS**

Date Adopted: **February 12, 2014**

Policy:

The IU strives to comply with both federal and state law regarding security breach notification requirements applicable to a breach of PHI, as such terms are defined under the applicable laws. Specifically, in the event of a breach of PHI, the IU follows the applicable standards of:

- The HITECH Act, and specifically §13402, as amended or implemented by the "Omnibus Rule" (45 CFR Part 160, Subparts A, B, C and D and Part 164, Subparts A and C) (collectively, the "Breach Statute"); and

- HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule" and together with the Breach Statute, collectively, the "Breach Notification Laws").

The IU will develop, implement, maintain and update, as necessary, security breach notification procedures in accordance with the Breach Notification Laws to:

- Detect potential and actual Breaches;

- Investigate and evaluate potential and actual Breaches;

- Respond to a Breach by furnishing the required notices; and

- Correct and prevent subsequent similar or dissimilar incidents.

- Any terms not otherwise defined in the IU's breach notification policies and procedures shall have the meanings ascribed to such terms in the Breach Notification Laws.

The IU is required to comply with both federal and state laws regarding security breach notification. In the event that federal and state breach notification laws contain contrary provisions, the IU will review the HITECH preemption standard to analyze its obligations. See 42 U.S.C. § 1320d-7 (the "Preemption Standard"). When necessary, the HIPAA Privacy Officer will conduct a preemption analysis using the Preemption Standard.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **DETECTING AND REPORTING OF BREACHES**

Date Adopted: **February 12, 2014**

Policy:

The IU strives to detect any and all breaches. Any employee, agent or other IU vendor who obtains information or has reason to believe that a breach has or may have potentially occurred and involves PHI created or maintained by the IU is expected to report such information to a supervisor or if a supervisor is not immediately available, then directly to the HIPAA Privacy Officer.

Procedures:

1. As part of periodic evaluations of systems pursuant to the IU's Audit Controls Policy, systems shall also be audited for evidence of any breach that may have resulted in or may result in an "unauthorized acquisition, access, use, or disclosure" of PHI. The Information Technology (IT) department shall work to develop IT solutions to detecting security breaches within the IU's systems.

2. The IU's reporting procedures for reporting privacy and security violations shall be expanded to allow for reporting of any known or suspected security incidents and/or breaches of, affecting, or potentially affecting, PHI.

3. Update HIPAA Business Associate Agreements to include provisions that require the Business Associates to notify the IU's HIPAA Privacy Officer, HIPAA Security Officer or Information Security Officer of any and all detected or suspected security incidents and breaches which involve the IU's PHI.

4. The IU shall educate and train, as appropriate, its employees and agents regarding the IU's breach notification policies and procedures.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *General*

Topic: **INVESTIGATING AND EVALUATING SECURITY INCIDENTS**

Date Adopted: **February 12, 2014**

Policy:

The HIPAA Privacy Officer, HIPAA Security Officer and Information Security Officer, and/or their respective designees, investigate and evaluate any and all reported or detected security incidents involving PHI, including potential breaches.

Procedures:

- Gather information relating to the reported or detected security incident.
- Evaluate information gathered to determine whether there is a "breach," as defined under the security breach notification laws.
- If it is determined that a "breach" has occurred, proceed to response procedures set forth in the IU's Response in the Event of Breach policy.
- An unauthorized acquisition or unauthorized access, use, or disclosure of PHI is ***presumed to be a breach*** unless the IU can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment. All determinations and analysis regarding the presumption of a breach and whether that presumption has been overcome must be documented. The Assessment Report set forth below should be used for this purpose.
- Final determinations should be vetted with legal counsel before any further steps are taken to make or not make notifications in connection with a particular breach incident.
- If it is determined that a breach has occurred and there is more than a low probability that the PHI has been compromised, then response procedures must be followed, as set forth in the IU's Response in the Event of Breach policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Risk Assessment

(to be completed by HIPAA Privacy, HIPAA Security or Information Security Officer)

Date of this Report:_____ **File ID #: ___**

1. Generally describe the nature of the potential breach of unsecured information (the "Breach"):

2. Who is the recipient (or potential recipient) that has or may have impermissibly accessed the information as a result of the Breach?

3. What type of and how much information was accessed/disclosed and was it actually acquired or viewed?

4. What steps have been taken to mitigate potential harm to individuals?

5. In light of the foregoing information available, is there a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

    - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the PHI or to whom the disclosure was made;
    - Whether the PHI information was actually acquired or viewed; and
    - The extent to which the risk to the PHI has been mitigated.

Explain how the IU determined that either (a) there was a breach; or (b) the presumption of a breach was overcome because there is a low probability that the PHI has been compromised.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *General*

Topic: **RESPONSE IN THE EVENT OF A BREACH**

Date Adopted: **February 12, 2014**

Policy:

In any case that it has been determined that there has been a breach of PHI, the IU notifies affected individuals, law enforcement, federal and state agencies as required under the security breach notification laws, or when otherwise determined by the IU to be appropriate. The IU also, as best as possible, strives to mitigate any harm that may result from a breach, and to take corrective actions to prevent similar incidents.

Procedures:

1. Notifying Secretary of Health and Human Services (HHS):

   - ❑ Breaches Affecting 500 or More Individuals: If a Breach affects 500 or more individuals, the HIPAA Privacy Officer shall be responsible for providing the Secretary of HHS with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. This notice must be submitted electronically by completing all information required on the form provided at: http://ocrnotifications.hhs.gov/

   - ❑ Breaches Affecting Fewer than 500 Individuals: If a security breach affects less than 500 individuals, log the incident in the IU's security breach log (maintained by the HIPAA Privacy Officer). Notification to HHS of such incidents (less than 500 individuals) shall be submitted annually. A separate form must be completed for every breach that has occurred during the calendar year. All notifications of breaches occurring in a calendar year must be submitted within 60 days of the end of the calendar year in which the breaches occurred. Annual breach notifications must be submitted at: http://ocrnotifications.hhs.gov/

2. Notifying Media (Breaches of 500+):

   - ❑ If a breach of unsecured PHI is discovered and involves 500 or more individuals of a single State or jurisdiction, the IU must provide Media Notice through prominent media outlets serving the State or jurisdiction of such 500 or more individuals if their unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. The content of the Media Notice must be the same as the written notice provided to the individual.

3. **Notifying Individuals**:

   - ❑ Notify individuals whose PHI may be affected as a result of the breach. Mail notice by first-class mail to the individual's last known address.

   - ❑ If there is a risk of "possible imminent misuse" of unsecured PHI and, therefore, the need to notify is "urgent," provide notice to the individual by telephone or other means, as appropriate, in addition to the written notice, which must still be provided.

- ❑ Written notice may be provided by e-mail (in lieu of US mail) only if (a) the individual has specified e-mail as a preferred method of receiving notice, and (b) the notice is consistent with Section 101 of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001.

    - ■ Obtain patient's agreement to receive breach notification by e-mail by: (a) updating patient intake forms; (b) providing means on the IU's website to allow an individual to inform the IU of preference to receive such notices by e-mail.

    - ■ The following language may be utilized to obtain a patient's agreement to receive notification of breaches by e-mail:

        "Federal and State law require that we notify you in the event of a breach of your personal information or personal health information. Should a breach occur, we will notify you by sending a written "Notice of Breach" form by first-class US mail to your last known mailing address, unless you prefer to have such notice sent to you via e-mail, consistent with applicable provisions regarding electronic records and signatures set forth in the federal Electronic Signatures in Global and National Commerce Act. If you would prefer e-mail notification, please indicate that preference by initialing where indicated and by providing your current e-mail address:

        Initial here if you prefer notification by e-mail: _____

        E-mail Address: _____

- ❑ A substitute form of notice to individuals must be used if: (a) out-of-date or insufficient contact information prevents direct or written (or e-mail) notice from being sent to the individual; or (b) contact information is lacking for ten (10) or more individuals. The substitute form of notice must consist of all of the following:

    - ■ E-mail notice, when the business has an email address; and

    - ■ Conspicuous posting on the home page of the IU's website for ninety (90) days or more or posting in major print or broadcast media, including major media in geographic areas where individuals affected by the breach likely reside; and

    - ■ A toll-free phone number designated for information about the breach that remains active for at least ninety (90) days; and

    - ■ Notification to major Statewide media.

- ❑ Individual notification must be provided without unreasonable delay.

    - ■ In no case can there be a delay longer than sixty (60) days after discovery of the breach, unless a law enforcement official determines that notification would impede an investigation and informs the IU of that fact.

    - ■ The foregoing should not be interpreted to mean that notifications can automatically be delayed up to 60 days. Notification cannot be delayed on the mere basis that an investigation has not been fully completed to affirmatively determine whether or not a "breach" has occurred as defined under the breach notification laws.

- Law Enforcement Delay: Before any notifications due to individuals are delayed per request by law enforcement, ensure that a "statement" has been received from law enforcement that notifying the individual could "negatively affect a criminal investigation or national security" (the "Police Statement to Delay").

  - The Police Statement to Delay can be accepted in writing, or orally (over the phone).

  - If in writing, the notification to individual can be delayed for the period specified in the written Police Statement to Delay.

  - If provided orally (e.g., over the phone), then document the Police Statement to Delay and the identity of the law enforcement official. Calendar to follow up with law enforcement within 30 days. If after 30 days a written Police Statement to Delay is not received, then notification of the breach must be furnished to individuals.

4. Notifying Law Enforcement:

   - Before notifying any individual regarding a breach involving electronic PI, the breach and any information pertaining to the breach must be reported to the Division of State Police in the Law Department of Law and Public Safety. Information, including PHI, should be provided to the Police in connection with the breach in accordance with the IU's Privacy and Security Policies and Procedures governing disclosures required by law and law enforcement disclosures.

   - Once the breach has been reported to law enforcement, there should be no "unreasonable delay" before notification of the breach is provided to the individual. Follow guidelines under previous section re: Law Enforcement Delay for this purpose.

5. Notifying Other Enforcement Agencies:

   - In the event of any breach requiring notification of more than 1000 individuals at one time, the IU must notify, without unreasonable delay, Consumer Reporting Agencies (that compile or maintain files on consumers on a nationwide basis) of the timing, distribution, and content of the notifications.

6. Take steps to mitigate any negative consequences resulting from the breach, as best as possible. See Mitigation of Improper Disclosures policy.

7. Take corrective action to prevent a repeat incident. Re-evaluate administrative, physical and technical HIPAA safeguards, and adjust same as needed to improve or close any gaps in security. Document corrective action steps taken.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***General***

Topic: **SANCTIONS**

Date Adopted: **February 12, 2014**

Policy:

The IU applies appropriate sanctions against employees who fail to comply with the IU's Privacy Policies and Procedures, or the requirements of HIPAA and applicable state laws.

Procedures:

Responsibility for Sanctions

The HIPAA Privacy Officer will recommend appropriate sanctions to be applied to the IU's employees who fail to comply with the IU's Privacy Policies and Procedures. The IU's Human Resources department and personnel will apply appropriate sanctions, as recommended by the HIPAA Privacy Officer.

Application

Sanctions will be administered according to the severity of the failure to comply with HIPAA and these Privacy Policies & Procedures. Sanctions may include, but are not limited to: verbal warning; written warning; probation; suspension; demotion; termination from employment; referral for criminal prosecution (or to other governmental authorities); and/or the demand for reimbursement for any losses or damages resulting from the violation.

Documentation

The IU's Human Resources Department and personnel, after notifying the HIPAA Privacy Officer of the imposition of sanctions, will maintain documentation of sanctions that are imposed within each employee's personnel file. Such documentation shall be retained for a period of six (6) years from the effective date of the sanctions.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS**

Date Adopted: **February 12, 2014**

Policy:

The IU uses or discloses PHI for treatment, payment and health care operations as described herein and without the need for prior written authorization, except where the use or disclosure involves psychotherapy notes (for such uses and disclosures, see Psychotherapy Notes Procedure, below). All uses and disclosures of PHI for treatment, payment and health care operations purposes adhere to the Minimum Necessary standard.

General Procedures:

A signed Authorization need not be obtained prior to the use or disclosure of PHI if such use or disclosure is:

- For the purposes of carrying out the IU's own payment operations or health care operations functions;
- For the treatment activities of a health care provider, even though the IU does not engage in treatment activities;
- To another Covered Entity (e.g., health care provider, payer or clearinghouse) for payment activities of the receiving entity;
- To another Covered Entity for its health care operations as long as the entity either has (or had) a relationship with the individual whose PHI is being used or disclosed, the information pertains to such relationship and the disclosure is either:
    - For the purposes of conducting quality assessment and improvement activities or reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities; or
    - For the purpose of health care fraud and abuse detection or compliance.
    - To another Covered Entity that participates with the IU in an organized health care arrangement for any health care operations activities of the organized health care arrangement.

"Treatment" is defined as "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."

"Payment" includes the activities undertaken by: (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (2) a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care.

The activities referenced in the definition of payment relate to the individual/patient and include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

- Risk adjusting amounts due based on enrollee health status and demographic characteristics;

- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

- Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and

- Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number and name and address of the health care provider and/or health plan.

"Health Care Operations" is defined to include any of the following activities of the IU to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the IU participates:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

- Most underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

- Business management and general administrative activities of the IU, including, but not limited to:

- Management activities relating to implementation of and compliance with the requirements of HIPAA;

- Customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer.

- Resolution of internal grievances;

- Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a Covered Entity or, following completion of the sale or transfer, will become a Covered Entity; and

- Creating de-identified health information.

Psychotherapy Notes Procedure:

PHI is not to be used or disclosed without first obtaining a signed Authorization when the use or disclosure involves psychotherapy notes, except where the use or disclosure is for purposes of treatment, payment or health care operations in the following situations in the following situations only:

- Use by the originator of the psychotherapy notes for treatment;

- Use or disclosure by the IU for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve skills in group, joint, family, or individual counseling;

- Use or disclosure by the IU to defend itself in a legal action or other proceeding brought by the individual who is the subject of the psychotherapy notes;

- Use or disclosure that is required by the Secretary of the Department of Health and Human Services to investigate or determine the IU's compliance with HIPAA, or is required by law and complies with and is limited to the relevant requirements of such law;

- Use or disclosure permitted under HIPAA for specified health oversight activities with respect to the originator of the notes;

- Use or disclosure to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law; or

- Use or disclosure necessary to avert a serious threat to health or safety, but only where the use or disclosure is consistent with applicable law and standards of ethical conduct and where the IU believes, in good faith, that the use or disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public and is made to a person or persons reasonably able to prevent or lessen the threat, including the target of threat.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **FAMILY MEMBERS, RELATIVES OR FRIENDS**

Date Adopted: **February 12, 2014**

Policy:

PHI may be disclosed to a family member, other relative, or a close personal friend of a patient, or any other person identified by the individual, so long as: (i) the information is directly relevant to the requesting individual's involvement with the individual's care or payment related to the individual's healthcare; and (ii) the individual has been provided with the opportunity to object to the disclosure, and the individual does not object, or it can be reasonably inferred from the circumstances, based on professional judgment, that the individual does not object.

Procedures:

Presume that the individual would not want the family member, relative or friend to have access to the PHI, unless there is information to clearly indicate to the contrary.

Clarify whether a patient desires to share PHI with any family members, relatives or friends by routinely attempting to obtain written permission listing those individuals with whom the IU may share PHI. The IU may use the attached form of Enrollment Authorization for this purpose.

Determine and document any family members, relatives or friends or other individuals who the individual does not want his or her PHI disclosed to, and if so, include such preferences on the Enrollment Authorization.

Unless the individual signs the Enrollment Authorization, the IU may not disclose PHI to a family member, relative or personal friend (or other person(s) identified by the individual) except under the circumstances set forth below:

- Notification of Family Members. The IU may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, relative, or another person responsible for the care of the individual of the individual's location, general condition, or death.

- If the Individual is Present. If the individual is present or available, and has the capacity to make health decisions, the IU may disclose PHI to a family member, relative or other person identified by the individual, so long as the IU:

    - Obtains the individual's consent;

    - Provides the individual with the opportunity to object to the disclosure, and the individual does not object; or

    - Can reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

- If the Individual is Not Present or the Individual is Incapacitated or in an Emergency Circumstance.

    - If the individual is not present or available, or the opportunity to agree or object to the disclosure is not practicable because the individual is incapacitated or in an emergency circumstance, the IU may, in the exercise of professional judgment, determine whether the disclosure is in the best

interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes.

- The IU may allow a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other items containing similar forms of PHI, even without an Authorization or the individual's express agreement if, in the professional judgment of the IU's administrator or agent, it is in the individual's best interest to allow the practice.

Do **NOT** elect to disclose PHI to a family member, relative or friend of the individual, if the IU has a reasonable belief that:

1. the individual has been or may be subjected to domestic violence, abuse or neglect by such person; or

2. disclosing the PHI could endanger the individual; and the IU, in the exercise of professional judgment, decides that it is not in the best interest of the individual to disclose PHI.

The IU shall maintain a copy of an executed Authorization Enrollment in its records for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

AUTHORIZATION ENROLLMENT
Family Members, Relatives and Friends

I hereby authorize the IU to release my PHI described below to:

☐ All of my family members
☐ Spouse
☐ Mother
☐ Father
☐ Children: _____
☐ Other: _____

Names of specific family members, relatives or friends that I do not want to have access to any PHI (include relation to you e.g., uncle): _____
_____
_____

Information to Be Released: _____

Purpose of Disclosure (explain or indicate "at the request of the individual"):
I understand that the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations (collectively, "HIPAA") govern the terms of this Authorization. I understand that I have the right to revoke this Authorization, at any time prior to the IU's compliance with the request set forth herein, provided that the revocation is in writing. I further understand that additional information relating to the exceptions to the right to revoke and a description of how I may revoke this Authorization is set forth in the IU's Notice of Privacy Practices. I understand that any revocation must include my name, address, telephone number, date of this Authorization and my signature and that I should send it to:

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13[address]

I understand that I am not required to sign this Authorization and that my enrollment in a health plan or treatment cannot be conditioned upon my execution of this Authorization.

I understand that the information used or disclosed pursuant to this Authorization may be subject to re-disclosure by the recipient and, in that case, will no longer be protected by HIPAA.

This Authorization expires within one (1) year, or earlier upon my request. I hereby acknowledge receipt of a copy of this Authorization.

_____
Signature of Individual

_____
Date of Authorization

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **PERSONAL REPRESENTATIVES WITH LEGAL AUTHORITY**

Date Adopted: **February 12, 2014**

Policy:

The IU considers personal representatives with the legal authority (a "Personal Representative") to act on behalf of an individual as though they have "stepped into the shoes" of the individual for purposes of access to and use of the individual's PHI relevant to such personal representation.

Procedures:

Prior to releasing PHI to a person claiming to be a Personal Representative, the IU shall verify the person's authority as follows:

- Request identification from the person to determine whether they have authority to act as a personal representative on behalf of a patient in making decisions related to health care (e.g., Court Order appointing Guardian; Power of Attorney etc.).

- If the documentation is sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, treat such person as a Personal Representative with respect to PHI relevant to the personal representation.

- If the documentation is not sufficient to ensure that the requesting individual is an authorized Personal Representative of the individual, the PHI may not be released to the requesting individual unless: (i) a written Authorization from the individual has been obtained, or (ii) the disclosure is permitted under the Family Member, Relatives and Friends policy.

The IU may not treat a person as a Personal Representative of an unemancipated minor if the minor has the authority to make decisions with respect to PHI pertaining to a health care service under applicable State law. See Minors policy.

Do not treat a person as the Personal Representative of the individual if there is a reasonable basis to believe that:

1. the individual has been or may be subjected to violence, abuse or neglect by the purported Personal Representative; or
2. treating such person as the Personal Representative could endanger the individual and in the exercise of the IU's professional judgment, it is not in the best interest of the individual to treat the person as the individual's Personal Representative.

Contact and notify the HIPAA Privacy Officer in the event a negative determination is made regarding the release of PHI, or the authority of the requesting individual to act as the Personal Representative is questionable.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **DECEDENTS**

Date Adopted: **February 12, 2014**

Policy:

If the individual is deceased (the "Decedent"), the IU may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual who was involved in the Decedent's care or payment for health care prior to the Decedent's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the Decedent that is known to the IU.

If under applicable law, an executor, administrator, or other person has authority to act on behalf of the Decedent or of the Decedent's estate, the IU treats such person as a legal Personal Representative of the Decedent.

Disclosures to any other third party (e.g., coroner; funeral director etc.) of a Decedent's PHI shall be permitted only if handled in accordance with the following procedures.

Procedures:

- Prior to disclosing to a family member, other relative, or a close personal friend of the Decedent, or any other person identified by the Decedent who was involved in the Decedent's care or payment for health care prior to the Decedent's death, PHI of the Decedent that is relevant to such person's involvement, the IU determines whether such a disclosure is inconsistent with any prior expressed preference of the individual that is known to the IU. The IU shall contact and notify the HIPAA Privacy Officer in the event a negative determination is made regarding the release of PHI on the basis that doing so is inconsistent with any prior expressed preference of the individual.

- Prior to releasing the Decedent's PHI, verify the requesting individual's identity to determine whether the person is the executor, administrator, trustee, or other authorized person, who is authorized to act on behalf of the Decedent or the Decedent's estate, or to request information about the Decedent.

- If the requesting individual provides documentation sufficient to ensure that he/she is authorized to receive information regarding the Decedent, treat such person as a Personal Representative with respect to the PHI relevant to the personal representation.

- The Decedent's PHI may be disclosed to a coroner or medical examiner for the purpose of: (i) identifying a deceased person, (ii) determining a cause of death, or (iii) other duties as authorized by law. Obtain verification of the requesting individual's authority.

- The Decedent's PHI may be disclosed to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the Decedent. If necessary for funeral directors to carry out their duties, PHI may be disclosed prior to, and in reasonable anticipation of, the individual's death.

- Document disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **RESPONSE TO SUBPOENAS AND DISCOVERY REQUESTS**

Date Adopted: **February 12, 2014**

Policy:

Where a civil subpoena or discovery request for PHI is not accompanied by a qualified protective order entered by a court of law, the IU requires "satisfactory assurances" from the party seeking the information that reasonable efforts have been made to ensure that the individual about whom the PHI pertains has been given notice of the subpoena/discovery request and has had an opportunity to object.

Procedures:

The IU shall immediately direct any and all subpoenas and discovery requests to the HIPAA Privacy Officer.

The term "subpoena" means a document that directs the IU to appear to give testimony about PHI or to produce records or other documents containing PHI. The term "discovery requests" means other documents used to obtain PHI in a lawsuit, such as interrogatories (written questionnaires used to find out about facts relevant to a litigation).

PHI may be disclosed in the following circumstances only:

- In accordance with a signed Authorization.
- In accordance with an Order of a Court or other "Administrative Tribunal."
- In accordance with a Civil Subpoena/Discovery Request under the following circumstances:
    - The subpoena or discovery request contains one of the two following items:
        - Proof that reasonable efforts have been made to provide written notice to the individual that his or her PHI is being sought; OR
        - Proof that the attorney has applied to the court for a "qualified protective order". In order to satisfy this requirement, it must be shown that:
            - the parties in the lawsuit have agreed to a "qualified protected order" and have presented their agreement to the court; or
            - a "qualified protective order" has been requested from the court that would limit the use of PHI.

The term "qualified protective order" means an order of a court or a stipulation by the parties to the litigation that:

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

In the event that "satisfactory assurances" are not provided, the subpoena/discovery request should be returned and the requesting individual informed that the HIPAA requirements have not been met.

This procedure does not apply to:

- Court orders;
- Court subpoenas (including grand jury subpoenas);
- Search warrants; and/or
- Summonses issued by a court.

Document disclosures made under this procedure pursuant to the Accounting of Disclosures policy and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **LAW ENFORCEMENT REQUESTS**

Date Adopted: **February 12, 2014**

Policy:

PHI may be released to law enforcement officials and for law enforcement purposes if such disclosure is "required by law" and is enforceable in a court of law, and is released only strictly in accordance with this policy. Note that this policy does not apply to investigations that arise out of and are directly related to: (1) the receipt of health care; (2) a claim for public benefits related to health; or (3) qualification for, or receipt of public benefits or services where an individual's health is integral to the claim for benefits or services. In such cases, the policy governing Health Oversight Activities should be followed. Furthermore, if the individual is not the subject of the investigation, the policy governing Health Oversight Activities may be applied.

Procedures:

The IU shall immediately direct any and all requests for PHI made by a law enforcement officer to the HIPAA Privacy Officer.

PHI may be disclosed in compliance with, and as limited by, the relevant requirements of:

- A court order or court-ordered warrants;
- A subpoena or summons issued by a judicial officer;
- A grand jury subpoena; or
- An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand or similar process authorized under law, provided that:
    - The information sought is relevant and material to a legitimate law enforcement inquiry;
    - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
    - De-identified information could not reasonably be used.

Disclosures should comply with the Minimum Necessary policy.

With regard to requests by law enforcement in connection with suspects, fugitives, material witnesses, or missing persons, only the following PHI may be disclosed in response to a law enforcement official's request:

- Name and Address
- Date and Place of Birth
- Social Security Number

- ABO blood type and rh factor
- Type of Injury
- Date and Time of Treatment
- A description of distinguishing physical characteristics, including, height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos
- Date and time of death (if applicable)

The foregoing limited PHI may be provided at the oral or written request of someone acting on behalf of law enforcement (e.g., in response to a radio or television broadcast for assistance in identifying a suspect, "Wanted" posters and other public service announcements).

PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue are not to be disclosed for the purpose described in this policy.

With regard to requests by law enforcement in connection with victims of crime, the individual must be given an opportunity to agree or disagree before any PHI about the individual is released for such purpose. Thus, except as required by law, do not disclose PHI pursuant to a law enforcement official's request for such information about an individual who is, or is suspected to be, a victim of a crime unless it has been determined that the individual agrees to such a disclosure.

If an individual's agreement cannot be obtained because of incapacity or other emergency circumstances, the PHI may still be disclosed provided that:

- the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
- the law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
- the disclosure is in the best interests of the individual as determined by the IU, in the exercise of professional judgment.

This policy does not prevent reporting under state mandatory reporting laws regarding certain crime victims.

Disclosure of PHI concerning victims of abuse, neglect or domestic violence must be in compliance with the IU's Victims of Abuse, Neglect or Violence policy.

With regard to requests by law enforcement in connection with a decedent, PHI may be disclosed to a law enforcement official in order to alert such officials that the death of the individual may have resulted from criminal conduct.

With regard to requests by law enforcement in connection with a crime on the premises, PHI may be disclosed to a law enforcement official if the IU believes, in good faith, it constitutes evidence of criminal conduct that occurred on the premises of the IU.

Document disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **PUBLIC HEALTH ACTIVITIES**

Date Adopted: **February 12, 2014**

Policy:

PHI may be used or disclosed to certain public health or government authorities or to certain individuals for the public health activities and purposes described in this policy.

Procedures:

The IU may use or disclose PHI to the following authorities or persons, for the public health activities and purposes described:

1. To a public health authority or foreign government agency official that is authorized by law to collect or receive the PHI being disclosed, for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions;

2. At the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

3. To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

4. To a person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

    - To collect or report adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

    - To track FDA-regulated products;

    - To enable product recalls, repairs, replacement or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

    - To conduct post-marketing surveillance.

5. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the IU is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation;

6. To an employer, about an individual who is a member of the workforce of the employer, if: (A) the IU is a covered health care provider who provides health care to the individual at the request of the employer (i) to

conduct an evaluation relating to medical surveillance of the workplace or (ii) to evaluate whether the individual has a work-related illness or injury; (B) the PHI that is disclosed consists of findings concerning work-related illness or injury or a workplace-related medical surveillance; (C) the employer needs such findings in order to comply with its obligations under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and (D) the covered health care provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer: (i) by giving a copy of the notice to the individual at the time the health care is provided; or (ii) if the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided;

7. To a school, about an individual who is a student or prospective student of the school, if: (A) The PHI that is disclosed is limited to proof of immunization; (B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and (C) The Covered Entity obtains and documents the agreement to the disclosure from either: (i) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or (ii) The individual, if the individual is an adult or emancipated minor.

Document the use or disclosure for compliance with the IU's Accounting of Disclosures policy. Include as much of the following information as reasonably possible and applicable under the circumstances:

(a) Date and time of the use or disclosure, and whether the use or disclosure was made orally or in writing (a copy of any writing should be kept in the record);

(b) Description of the PHI used or disclosed;

(c) Name, title, and government affiliation of the person(s):

(i) Representing that the use or disclosure is necessary under this policy;

(ii) Requesting the use or disclosure under this policy; and

(iii) Receiving the PHI disclosed under this policy;

(d) The factual basis for the belief that the use or disclosure is necessary, including:

(i) Representations made by a person or entity that caused the IU to believe that the use or disclosure was necessary;

(ii) The IU's basis for believing that the person making the representations had knowledge about the situation; and

(iii) The IU's basis for believing that the person making the request and/or receiving the PHI had the authority to request and/or receive it.

Uses or disclosures under this policy may be made without first obtaining a signed Authorization or giving the individual an opportunity to agree or object.

Except for uses or disclosures that are made pursuant to an Authorization (even though one is not required for disclosures under this Procedure) or made because required by law, uses or disclosures under this policy must comply with the IU's Minimum Necessary policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Document uses and disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years. For public health uses and disclosures that reoccur on a regular basis, documentation may be satisfied by a statement reflecting the "regular reporting schedule" to a particular public healthcare agency.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **AVERTING THREATS TO HEALTH OR SAFETY**

Date Adopted: **February 12, 2014**

Policy:

The IU may use or disclose PHI if, in good faith, it believes:

- the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and
- the use or disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
- the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual:
    - because of a statement by an individual admitting participation in a violent crime that the IU reasonably believes may have caused serious physical harm to the victim; or
    - where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

This policy does not create or establish a legal duty to disclose PHI to prevent a threat to the safety or health of any person.

Procedures:

Use or disclosure of PHI under this policy may be made without the individual's authorization or giving the individual an opportunity to agree or object. Uses or disclosures must comply with the IU's Minimum Necessary policy.

Consistent with applicable law and standards of ethical conduct, PHI may be disclosed in either of the following two circumstances:

- Aversion of serious and imminent threats. When there is a good faith belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the IU is reasonably able to prevent or lessen the threat.
- For law enforcement to identify or apprehend someone. When there is a good faith belief, that the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual:
    - Because of a written or oral statement by an individual admitting participation in a violent crime that the IU reasonably believes may have caused serious physical harm to the victim, subject to the following conditions:

- Use or disclosure not permitted. The IU may NOT use or disclose PHI when the information is learned by the IU:
  - In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or
  - Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.
- Limit on information that may be disclosed. A use or disclosure under these circumstances shall contain only the following:
  - The statement made by the individual admitting participation in the violent crime; and
  - The following PHI:
    - Name and address,
    - Date and place of birth,
    - Social security number,
    - ABO blood type and rh factor,
    - Type of injury,
    - Date and time of treatment,
    - Date and time of death (if applicable), and
    - Description of distinguishing characteristics (such as height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos).

or

- Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

Document disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **VICTIMS OF ABUSE, NEGLECT OR VIOLENCE**

Date Adopted: **February 12, 2014**

Policy:

The IU may disclose PHI about an individual that the IU reasonably believes is a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive such reports. This policy does not affect reports of child abuse that are required by law.

Procedures:

General

- "Individual" or "victim" means the individual that the IU believes to be a victim of abuse, neglect or domestic violence.

- Disclosure under this policy may be made without the individual's authorization and without giving the individual an opportunity to agree or object.

- Disclosure under this policy need not comply with an agreement with an individual to restrict uses or disclosures of PHI.

- Disclosure under this policy must comply with the IU's Minimum Necessary policy (unless disclosure is made because it is required by law).

- Refer also to the IU's policy Disclosure of PHI to Family Patients, Relatives or Friends of the Individual, for guidance on using or disclosing information about an incapacitated victim who is unable to agree or object to those types of disclosures.

- Permitted Disclosures – Other than for child abuse or neglect. Except for reports of child abuse or neglect (which are covered by the IU's Public Health Activities and Required by Law policies), an employee of the IU who, in his/her professional judgment, reasonably believes that an individual has been a victim of abuse, neglect, or domestic violence (such as, for example, a victim of spousal abuse or abuse or neglect of residents of nursing homes or facilities for the mentally incompetent) can disclose PHI about the victim to a government authority that is authorized by law to receive reports of such abuse, neglect, or domestic violence (such as, for example, adult protective or social service agencies, ombudsmen for the aging, and law enforcement or oversight agencies) in the following circumstances:

    - Required by law: If the disclosure is required by law, disclosure is permitted:

        - To the extent it is required by law; and

        - As long as the disclosure complies with and is limited to the requirements of that law.

"Required by law" means that there is some mandate of the law, enforceable in court, that compels the IU to make the disclosure. For example, "required by law" includes statutes and regulations that require the disclosure, court orders and warrants, and subpoenas issued by a court, grand jury or administrative body authorized to require the production of information.

Example: If a disclosure about a victim of abuse, neglect or domestic violence is made in response to a court order, the IU shall limit the PHI disclosed to that required by the order.

- The victim agrees: Disclosure is permitted if the victim agrees to the disclosure. The agreement can be written or verbal; in the case of a verbal agreement, the IU should make a notation in the records about the victim's agreement.

- Authorized by law: Disclosure is permitted to the extent the disclosure is expressly authorized by statute or regulation and:

  - The IU, in the exercise of its employee's professional judgment, believes the disclosure is necessary to prevent serious harm to the victim or other potential victims; or

  - If the victim cannot agree because he or she is incapacitated, when a law enforcement or other public official authorized to receive the report represents to a IU employee that:

    - The victim's PHI will not be used against the victim, and

    - An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the victim is no longer incapacitated.

  Important Note: When a law enforcement or other public official asks the IU to disclose information about a victim, and that disclosure is permitted—but not required—by law, the IU maintains discretion, consistent with professional judgment about the victim's best interest, in deciding whether or not to make the requested disclosure.

Informing the Individual

- At the time of the disclosure

  - When: When the IU makes a disclosure permitted by this policy it must promptly inform the victim, in writing or orally, that such a report has been or will be made, except if, in the exercise of professional judgment:

    - The IU believes that informing the victim would place him or her at risk of serious harm (such as, for example, potential physical or emotional harm from learning that a report was made); or

    - The IU would be informing a personal representative, and the IU reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interest of the victim as determined by the IU.

  - How: When informing a victim that a report of abuse has been made, the IU encourages employees to do so verbally rather than in writing, due to the sensitivity of abuse situations and

the potential for someone other than the victim (particularly the abuser) to learn that the report was made.

- If the victim is informed orally, a notation should be made in the record.
- If the victim is informed in writing, a copy of that writing should be retained in the record.

Upon request for an accounting

- To be provided to the victim. If the victim subsequently requests an accounting of disclosures of PHI, the IU must include an accounting of a disclosure made under this policy.
- To be provided to a personal representative. If the request for an accounting is made by the victim's personal representative and the IU (i) reasonably believes that the person is responsible for the abuse, neglect, or other injury, or that treating that person as a personal representative could endanger the victim, and (ii) in the exercise of professional judgment, decides that informing that person about a report under this policy would not be in the best interest of the victim, then the IU does not have to treat that person as the personal representative and should not provide an accounting of a disclosure under this policy to that person.

Document disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **DE-IDENTIFIED INFORMATION**

Date Adopted: **February 12, 2014**

Policy:

Information has been rendered "de-identified" under HIPAA when there is no reasonable basis to believe that the information can be used to identify an individual. De-identified information is treated by the IU as no longer being covered by HIPAA and the IU's Privacy Policies & Procedures.

Procedures:

In order for PHI to be de-identified, all of the following identifiers related to the individual, the individual's employers, and the individual's household members must be removed:

- Names;
- All geographical subdivisions smaller than a state (thus, indications of street address, city, precinct, zip code, and their equivalent geocodes must be removed);
- All elements of dates (except years) related to an individual, such as dates of birth, admission, discharge, or death. All ages of 90 and above must be removed (and in such cases, the year must be removed); provided, however, that such ages may be described as a single category of "age 90 or older";
- Telephone and fax numbers;
- Electronic mail addresses; Web Universal Resource Locators ("URLs"); and Internet Protocol ("IP") addresses;
- Social security numbers;
- Record numbers (including prescription numbers);
- Health plan beneficiary numbers;
- Account numbers;
- Certificate and license numbers;
- Vehicle identifiers, including serial and license plate numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and

- Any other unique identifying number, code, or characteristic. An illustrative but non-exhaustive list of unique identifiers include:
    - Unusual occupations;
    - Very high salary ranges;
    - Existence/location of unique birthmarks and scars; and
    - That fact that a health condition or injury was the result of an unusual or highly publicized source or event, where there is a reasonable belief that disclosure of such fact would permit identification of the individual (such as, for example, an individual's receipt of anthrax-laden letters or mail bombs or falling victim to acts of terrorism or sniper attacks).

The IU must not have actual knowledge that, after the above-described identifiers have been removed, the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

The IU may disclose de-identified information, and, unless it is re-identified, de-identified information is not subject to the requirements of HIPAA or these Privacy Policies & Procedures.

Upon the issuance of further guidance by the Secretary of Health and Human Services regarding implementation of the requirements for the de-identification of PHI, the IU shall update its policies and procedures related to de-identification.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **REQUIRED BY LAW**

Date Adopted: **February 12, 2014**

Policy:

In general, the IU may use and disclose PHI as required by law, except additional requirements shall be met prior to the release of such information if such disclosure relates to victims of abuse, neglect or domestic violence or is for law enforcement purposes. For disclosures relating to these excepted topics, the IU shall meet the requirements described in the IU's Victims of Abuse, Neglect or Domestic Violence or Law Enforcement Purposes policies.

The IU will limit its use or disclosure of PHI to the relevant requirements of applicable laws.

Procedures:

Routine Uses and Disclosures

Identify current federal and state laws that mandate the IU to make certain routine disclosures of PHI.

The HIPAA Privacy Officer, or his/her designee, shall maintain a list of state and federal laws (statutes and regulations) that require the IU to make routine uses and disclosures of PHI.

The IU employees may consult this list to determine if a disclosure is one that the IU is mandated to make, and, if it is, the PHI may be disclosed as required by law.

Requests to Disclose PHI

Requests for release of PHI that an individual or entity claims is required by law should be directed to the HIPAA Privacy Officer.

The HIPAA Privacy Officer must first determine whether the disclosure is actually mandated (versus merely permitted). If the use or disclosure is mandated, the HIPAA Privacy Officer may disclose PHI in accordance with this policy. If the use or disclosure is merely permitted, the HIPAA Privacy Officer is not permitted to make the use or disclosure under this policy. In such case, the HIPAA Privacy Officer should determine if the use or disclosure is permitted under another policy. If the use or disclosure is not permitted under any other procedure, the IU may not disclose the PHI without first obtaining an Authorization.

Required by law means a mandate of law, enforceable in a court of law, that would compel the IU to use or disclose PHI. Examples of mandates that would be deemed to be required by law include:

- Statutes or regulations that require use or disclosure of PHI;
- Court orders and court-ordered warrants; and
- Subpoenas or summons issued by a court, grand jury or administrative body.

Once the HIPAA Privacy Officer confirms that the request is required by law, the HIPAA Privacy Officer, or employee directed by the HIPAA Privacy Officer may disclose the PHI without having to obtain an Authorization

and without providing the individual with an opportunity to agree or object to the disclosure, provided that the disclosure is made in accordance with this policy and procedure and the HIPAA Privacy Officer, or employee:

- Verifies the authority of the requestor;
- Verifies the identity of the requestor in accordance with the policy governing Verification of Identity for Individuals Requesting PHI; and
- Documents the disclosure in accordance with the IU's policy governing Accounting for Disclosures and maintains this documentation in the individual's record for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **HEALTH OVERSIGHT ACTIVITIES**

Date Adopted: **February 12, 2014**

Policy:

The IU permits the disclosure of PHI to a health oversight agencies for oversight activities authorized by law, including: (1) audits; (2) civil, administrative or criminal investigations; (3) inspections; (4) licensure; (5) disciplinary actions; (6) civil, administrative or criminal proceedings or actions; (7) other activities necessary for appropriate oversight of (a) the health care system; (b) government benefit programs for which health information is relevant to beneficiary eligibility; (c) entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or (d) entities subject to civil rights laws for which health information is necessary for determining compliance.

If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the IU may disclose PHI to a health oversight agency in such instance.

Procedures:

Direct unique requests for release or access to PHI from a health oversight agency to the attention of the HIPAA Privacy Officer.

Assess and confirm that the request is made by a "health oversight agency." A "health oversight agency" includes an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Native American tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether private or public) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Once it is confirmed that the request is made by a health oversight agency, the PHI may be released without having to obtain an authorization and without providing the individual with an opportunity to agree or object to the disclosure.

When the request centers around the individual who is the subject of the investigation, PHI (about that individual) may be disclosed to the requesting health oversight agency only if such investigation or other activity arises out of and is directly related to:

- the receipt of health care; or
- a claim for public benefits related to health; or
- qualification for, or receipt of, public benefits or services, when the individual's health is integral to the claim for public benefits or services.

Where the individual is the subject of an investigation and such investigation or activity does not arise out of and is not directly related to the activities described above, the IU may not disclose PHI under this policy. In such case, the policy governing disclosures of PHI for Law Enforcement Purposes should be followed.

Document disclosures made under this policy pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES AND PROCEDURES

Category: *Use and Disclosure of PHI*

Topic: **EMERGENCY SITUATIONS**

Date Adopted: **February 12, 2014**

Policy:

The IU may disclose PHI to a health care provider without first obtaining a written Authorization from the individual if the disclosure is for the purpose of providing emergency treatment to the individual.

The IU may disclose PHI to the individual's family or other person in an emergency circumstance if the disclosure is in the individual's best interest.

Procedures:

If the Request is from a Physician or other Health Care Provider:

- Verify that the request is for the purpose of providing emergency treatment to the individual.
- In the case of requests from Business Associates, have the Business Associate submit the request in writing on letterhead. Fax requests are acceptable.
- Document the name of the Business Associate and the date of the request.
- Provide the PHI to the requester in the manner specified.
- Do not deny an emergency request simply because the Business Associate has not submitted a written request on hospital or practice letterhead.

If the Request is from a Spouse, Parent, Child or Other Person:

- Disclose PHI to a family member or other person in an emergency circumstance without requiring a signed Authorization as long as the disclosure is in the individual's best interest. The PHI disclosed shall be limited to that which is directly relevant to the person's involvement in the individual's care.

Document disclosures made under this procedure pursuant to the IU's Accounting of Disclosures policy, and retain for six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **MARKETING**

Date Adopted: **February 12, 2014**

Policy:

The IU does not engage in Marketing. The IU reviews any communication that encourages recipients of the communication to purchase products or to use services to determine whether it is Marketing, except if the communication is in the form of:

- A face-to-face communication made by the IU to the individual; or
- A promotional gift of nominal value provided by the IU.

Marketing does not include a communication made:

(A) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the IU in exchange for making the communication is reasonably related to the IU's cost of making the communication;

(B) For the following treatment and health care operations purposes:

(a) for treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual (the "Treatment Exception");

(b) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: (i) the entities participating in a health care provider network or health plan network; (ii) replacement of, or enhancements to, a health plan; and (iii) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits (the "Health Product or Service Exception"); or

(c) for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment (the "Case Management/Care Coordination Exception").

The IU does not receive financial remuneration (meaning any direct or indirect payment from or on behalf of a third party whose product or service is being described) in exchange for making the communications listed in (a), (b), and (c) above. In addition, the IU treats arrangements between the IU and any other entity whereby the IU would be expected to disclose PHI to the other entity in exchange for direct or indirect payment of any kind in order to allow the other entity to communicate about its own product or service to be Marketing, and the IU does not enter such arrangements.

Communications by a Business Associate of the IU that fall within the (a) Treatment Exception; (b) Health Product or Service Exception; or (c) Case Management/Care Coordination Exception are not considered Marketing, as long as:

- The communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment received by the IU in exchange for the communication is reasonably related to the IU's cost of making the communication; or

- The communication is made by a Business Associate on behalf of the IU and the communication is consistent with the written contract (or other written arrangement) between the Business Associate and the IU.

In addition, the following communications are not considered "Marketing":

- Mailings (by the IU, or by Business Associate on the IU's behalf) promoting health in a general manner. For example:

  - information about new developments in health care (e.g., new diagnostic tools);

  - information about health or "wellness" classes;

  - information about support groups; and/or

  - information about health fairs.

- Communications about government and government-sponsored programs such as Medicare, Medicaid, supplemental benefits, or SCHIP.

- Calendars, pens, and the like that display the name of a product or the IU (but only when provided by the IU).

When considering whether, pursuant to the definition contained in this Policy, a communication is Marketing, the IU will consider whether the effect of the communication meets the definition of Marketing under HIPAA. It is irrelevant whether or not the intent of the communication was for marketing purposes.

Direct any questions regarding whether a communication or an activity is Marketing to the HIPAA Privacy Officer.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Use and Disclosure of PHI***

Topic: **SALE OF PHI**

Date Adopted: **February 12, 2014**

Policy:

The IU will obtain an Authorization for any disclosure of PHI which is a sale of PHI. Such Authorization must state that the disclosure will result in remuneration to the IU.

The sale of PHI means a disclosure of PHI by the IU or its Business Associate, if applicable, where the IU or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Sale of PHI does not include a disclosure of PHI:

(i) For public health purposes pursuant to 45 CFR §164.512(b) or § 164.514(e);

(ii) For research purposes pursuant to 45 CFR § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;

(iii) For treatment and payment purposes pursuant to 45 CFR § 164.506(a);

(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to 45 CFR § 164.506(a);

(v) To or by a Business Associate for activities that the Business Associate undertakes on behalf of a covered entity, or on behalf of a Business Associate in the case of a subcontractor, pursuant to 45 CFR §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the Business Associate, or by the Business Associate to the subcontractor, if applicable, for the performance of such activities;

(vi) To an individual, when requested under 45 CFR § 164.524 or § 164.528;

(vii) Required by law as permitted under 45 CFR § 164.512(a); and

(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law ((i) – (viii) each a "Permitted Purpose" and collectively, the "Permitted Purposes").

Procedures:

If the IU, or its Business Associate, is to receive any money, either directly or indirectly, in connection with a specific use or disclosure of an individual's PHI, the IU must determine whether such use and/or disclosure is a Permitted Purpose.

If the use or disclosure is for a Permitted Purpose, no HIPAA Authorization is required.

If the use or disclosure is not for any one of the Permitted Purposes, then obtain the individual's written authorization for receipt of remuneration by using the IU's Authorization to Use and Disclose PHI with Remuneration form.

If a third party has presented a signed "HIPAA-compliant" Authorization from the individual, review and confirm the validity of the that document, which must include the following elements in accordance with HIPAA:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s) or classes of persons, to whom the IU may make the requested use or disclosure;
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
- A statement of the individual's right to revoke the Authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the Authorization;
- A statement that information used or disclosed pursuant to the Authorization may be subject to re-disclosure by the recipient and no longer be protected by HIPAA;
- Signature of the individual and date;
- If the Authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.
- A statement that the IU will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing Authorization for the requested use or disclosure;
- A description of the purpose of the requested use or disclosure;
- A statement that the individual may refuse to sign the Authorization; and
- A statement that the use or disclosure of the requested information will result in direct or indirect remuneration to the IU from a third party.

Provide a copy of the signed Authorization to the individual.

Maintain a copy of the signed Authorization, or an electronic copy, for a period of six (6) years from the date of its creation, or the date when it was last in effect, whichever is later.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

AUTHORIZATION
FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

I hereby authorize LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13 ("Covered Entity") to use and release my Health Information, as designated below, to:

Recipient: _____
Recipient Address: _____
Recipient Telephone Number: _____
Recipient Fax Number: _____

The following Health Information about me may be used and disclosed (check each either "Yes"or"No/NA"):

	Yes"	"No"or N/A
My entire medical or billing record ☐	☐	☐
HIV/AIDS testing. diagnoses and treatment	☐	☐
Sexually Transmitted Disease testing, diagnoses and treatment	☐	☐
Mental Illness diagnoses and treatment	☐	☐
Drug or Alcohol Addiction diagnoses and treatment	☐	☐
Genetic testing and results and genetic information about me	☐	☐
Other: _____	☐	☐

The Health Information checked "yes" above may be used for the following Purpose(s):

☐ At my request, or
☐ For the Purpose of:_____

I understand that the terms of this Authorization are governed by the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, as may be amended from time to time ("HIPAA"). I understand that I have the right to revoke this Authorization, at any time prior to Covered Entity's compliance with the request set forth herein, provided that the revocation is in writing. I further understand that additional information relating to the exceptions to the right to revoke and a description of how I may revoke this Authorization is set forth in Covered Entity's Notice of Privacy Practices. I understand that any revocation must include my name, address, telephone number, date of this Authorization and my signature and that I should send it to: LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13 [address]; Attn: HIPAA Privacy Officer.

I understand that I am not required to sign this Authorization and that Covered Entity may not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on my execution of this Authorization. I understand that the information used or disclosed pursuant to this Authorization may be subject to redisclosure by the Recipient listed above and, in that case, may no longer be protected by HIPAA. This Authorization expires automatically upon Covered Entity's release of my Health Information as needed to fully accomplish the above-described Purpose(s). I hereby acknowledge receipt of a copy of this Authorization.

____/_____/_____ _____ _____

Date | Signature of Individual (or Legal Representative) | Authority of Legal Representative

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Individual's Rights***

Topic: **REQUEST FOR RESTRICTIONS & CONFIDENTIAL COMMUNICATIONS**

Date Adopted: **February 12, 2014**

Policy:

Requests for Restrictions.

The IU permits individuals to request that the IU restrict: (a) uses or disclosures of PHI to carry out treatment, payment, or health care operations; and (b) disclosures for which the IU must provide an individual with the opportunity to agree or to object under 42 CFR § 164.510.

The IU must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if: (A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (B) The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

The IU does not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the IU may use the restricted PHI, or may disclose such restricted PHI to a health care provider, to provide such treatment to the individual.

If the restricted PHI is disclosed to a health care provider for emergency treatment, the IU requires that such health care provider not further use or disclose the PHI.

A restriction agreed to by the IU is not effective to prevent uses or disclosures permitted or required under 45 CFR § 164.502(a)(2)(ii) (required by the Secretary), 45 CFR§ 164.510(a) (for facility directories) or 45 CFR § 164.512 (where an authorization or opportunity to object is not required).

The IU may terminate its agreement to a restriction if: (a) the individual agrees to or requests the termination in writing; (b) the individual orally agrees to the termination and the oral agreement is documented; or (c) the IU informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

Confidential Communications

The IU permits individuals to request and will accommodate reasonable requests by individuals to receive communications of PHI from the IU by alternative means or at alternative locations.

The IU may require the individual requesting the confidential communication to make such request in writing and may condition the provision of a reasonable accommodation on:

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

The IU may require an explanation from the individual that disclosure of all or part of the individual's information to which the request pertains could endanger the individual.

Procedures:

Right of an Individual to Request Restriction of Uses and Disclosures

Afford every individual the right to request that the IU restrict:

- Uses or disclosures of the individual's PHI to carry out treatment, payment, or health care operations; and
- Disclosures for which the IU must provide the individual with the opportunity to agree or to object under 42 CFR § 164.510 (e.g. disclosures to assist in the notification of family members).
- Disclosures to health plans for purposes of carrying out payment or health care operations, and not for purposes of carrying out treatment, when the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

Require requests for restrictions to be submitted in writing. Validate the "author" of the request to determine the author's authority to request such restriction (e.g., in cases of legal representatives).

Requests for restrictions should be forwarded to the HIPAA Privacy Officer for review. If the HIPAA Privacy Officer grants the restriction, the restriction shall be honored by implementing the restriction in the individual's files at the IU by marking the files as "restricted".

If a restriction is in place, do not use or disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the IU may disclose the restricted PHI to a health care provider, to provide emergency treatment to the individual.

The agreed upon restriction may only be terminated if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The IU informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the individual.

Right of an Individual to Request Confidential Communication

- Allow every individual the right to request that confidential communications be received by alternative means or at alternative locations.
- Requests for confidential communications should be made in writing.
- Accommodate reasonable requests.
- The provision of a reasonable accommodation may be conditioned on:
    - When appropriate, information as to how payment, if any, will be handled; and
    - Specification of an alternative address or other method of contact.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Individual's Rights***

Topic: **ACCESS RIGHTS**

Date Adopted: **February 12, 2014**

Policy:

The IU affords each individual the right of access to inspect and obtain a copy of his or her PHI maintained in a designated record set, with the exception of the following:

- "Psychotherapy Notes";
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and
- Information maintained by the IU that is: (i) subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 262a, to the extent the provision of access would be prohibited by law; or (ii) exempt from the Clinical Laboratory Improvement Amendments of 1988, pursuant to 42 CFR 493(a)(2).

The IU will provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form and format as agreed to by the IU and the individual.

If the PHI that is the subject of the request is maintained by the IU in one or more designated record sets electronically and if the individual requests an electronic copy of such PHI, the Copmany shall provide the individual with access to the PHI inin the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the IU and the individual.;The IU must provide the individual with access to the PHI within thirty (30) days after receipt of the request. If the IU grants the request, in whole or in part, it shall provide the acces requested. If the IU denies the request, in whole or in part, it shall do so in accordance with the Denial of Access Procedure, below.If an individual's request for access directs the IU to transmit the copy of the PHI directly to another person designated by the individual, the IU must provide the copy to the person designated by the individual within thirty (30) days. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

Procedures:

If the Individual Appears In Person To Request PHI:

Require the individual to submit the request for access in writing, specifying the scope of information as to which he/she wishes to have access or copies (e.g., all information; billing information; information pertaining to a specific date of treatment).

Request at least one form of identification from the individual, e.g., driver's license, birth certificate or passport.

Verify that all sources that may contain the requested PHI are checked. This includes PHI maintained solely on the IU's computer system and in the IU's business office. The IU shall attempt to provide the individual with the requested PHI as soon as possible.

In the event the IU determines that it will take longer than 30 days to produce the requested information, the HIPAA Privacy Officer shall be contacted immediately.

The IU may charge a per page copying fee provided that the fee is a reasonable, cost-based fee and provided that the fee includes only the cost of copying (including the cost of supplies for and labor of copying and postage when the individual has requested the copy be mailed). The IU will adhere to any additional restrictions under state law on caps for copy charges. The IU may charge an amount not greater than its labor costs in responding to an individual's request for a copy of PHI (or a summary or explanation of such information) in an electronic format.

Member Requests Information by Telephone or Fax

Requests for PHI from an individual made by telephone or fax are acceptable, provided that the request is made on an Authorization to Disclose PHI form.

Have the PHI available for pick-up by the individual or representative of the individual, or mail the information to the individual at the address specified in the Authorization.

Advise the individual that if someone other than the individual is going to pick up the PHI from the IU, the person will need to provide proof of identity and authority for pick-up.

Denial of Access

Requests for access may be denied if:

- the access requested is likely to endanger the life or physical safety of the individual or another person;
- the PHI makes reference to another person, and it has been determined that the release of the information could lead to harm to that other person;
- the request is made by a personal representative of the individual, and it has been determined that permitting the access could cause harm to the individual;

In addition, the following information may be excluded:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and
- Information maintained by the IU that is: (i) subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 262a, to the extent the provision of access would be prohibited by law; or (ii) exempt from the Clinical Laboratory Improvement Amendments of 1988, pursuant to 42 CFR § 493(a)(2).

If an individual is denied access to PHI, the IU must:

- Explain to the individual why he/she is being denied;
- Document the denial in the individual's file; and
- Allow the individual the right to have the denial reviewed by a health care professional who is designated by the IU to act as the reviewing official and who did not participate in the original decision to deny the request.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Individual's Rights***

Topic: **AMENDMENT OF PHI**

Date Adopted: **February 12, 2014**

Policy:

The IU affords each individual the right to amend his or her PHI in a Designated Record Set ("DRS") for as long as the PHI is maintained in the DRS by the IU. The IU may deny an individual's request for amendment if it determines that the PHI or record that is the subject of the request:

- Was not created by the IU, unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment;
- Is not part of the DRS;
- Would not be available for inspection; or
- Is accurate and complete.

Procedures:

The IU shall permit individuals to submit a request to amend PHI in a DRS maintained by the IU.

The IU shall require that all such requests be made in writing and include a reason to support the requested amendment.

The IU shall act on requests for amendment no later than 60 days* after receipt of the request as follows:

- Immediately upon receipt of a written request, determine whether the IU is obligated to make the requested amendment and, in the event the IU determines to deny the request, provide a written denial to the individual.
    - Making the Amendment. If the IU accepts the requested amendment, in whole or in part:
        - Identify the records in the DRS that are affected by the amendment and append the amendment to the original record or otherwise provide a link to the location of the amendment.
        - Inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the IU notify the relevant persons with which the amendment needs to be shared.
        - Make reasonable efforts to inform and provide the amendment within a reasonable time to:
            - Persons identified by the individual as having received PHI needing the amendment; and

- Persons, including Business Associates, that the IU knows have PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

- Denial of the Request for Amendment. If the IU determines to deny the requested amendment, in whole or in part:

  - The denial must be based on the IU's determination that the record or PHI that is the subject of the request:

    - Was not created by the IU, unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested amendment;

    - Is not part of the DRS;

    - Would not be available for inspection; or

    - Is accurate and complete.

  - Provide the individual with a timely, written denial. The denial must use plain language and contain:

    - The basis for the denial, in accordance with the immediately preceding square bullet point;

    - An individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

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

    - A description of how the individual may complain to the IU pursuant to the complaint procedures established by the IU. Include the name, title, and telephone number of the HIPAA Privacy Officer.

- Statement of Disagreement. Permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Forward all written statements of disagreement to the HIPAA Privacy Officer immediately upon receipt.

- Rebuttal Statement. Prepare a written rebuttal to the individual's statement of disagreement, and provide the same to the individual.

- Recordkeeping. Identify the record or PHI in the DRS that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the IU's denial of the request, the individual's statement of disagreement, if any, and the IU's rebuttal, if any, to the DRS.

- Future Disclosures. If a statement of disagreement has been submitted by an individual, include the material appended in accordance with Recordkeeping immediately above, or, at the election of the IU, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates. If the individual has not submitted a written statement of

disagreement, the IU must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action in accordance with the second square bullet point under Denial of the Request for Amendment above.

- When any subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the IU may separately transmit the material required by these procedures to the recipient of the standard transaction.

*If the IU is unable to act on the request for amendment within 60 days, the IU, with the approval of the HIPAA Privacy Officer, may extend the time for such action by no more than 30 days provided that the IU provides the individual, within the initial 60 day time period, with a written statement of the reasons for the delay and the date the IU will complete its action on the request. The IU may have only one such extension of time for action on a request for an amendment. However, any shorter timeframes specified under state law must be adhered to.

Implementation Specification

Upon receipt of notice by the IU from another Covered Entity of an amendment to an individual's PHI, append the amendment to the original record or otherwise provide a link to the location of the amendment.

Document the titles of the persons and/or offices responsible for receiving and processing requests for amendments and retain such documentation for a period of at least six (6) years.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***Individual's Rights***

Topic: **ACCOUNTING OF DISCLOSURES**

Date Adopted: **February 12, 2014**

Policy:

The IU affords each individual the right to receive an accounting of disclosures made by the IU of his or her PHI over the preceding six (6) years, except the following are excluded from such accounting requirement:

- Those made to carry out treatment, payment or healthcare operations, except when disclosures of PHI are made by the IU through an Electronic Health Record (EHR), the IU affords each individual the additional right to receive an accounting of disclosures of his or her PHI for health care operations, payment and treatment made by the IU (or its Business Associate) through an EHR for a period of three (3) years prior to the date the individual requests the accounting;

- Those made to the individual themselves;

- Those that are merely incidental to another permissible use or disclosure;

- Those made as a result of a listing in the facility directory;

- Those made to friends and family members, provided that the individual agreed to the disclosure, did not object to the disclosure or which were made based on professional judgment that the disclosure was necessary;

- Those made pursuant to a valid Authorization;

- Those made for national security or intelligence purposes;

- Those made to corrections institutions or law enforcement officials having custody of inmates;

- Disclosures made as part of a Limited Data Set; and

- Those made prior to April 14, 2003.

Procedures:

Upon written request by the individual, the IU shall provide either an accounting of disclosures of PHI by the IU and by a Business Associate acting on behalf of the IU, or an accounting of disclosures by the IU and a list of all Business Associates acting on behalf of the IU, including contact information for the Business Associates, such as mailing address, phone, and e-mail address of Business Associate (and, upon a request made by an individual to a Business Associate of the IU, the Business Associate shall provide a written accounting that includes:

- Date of each disclosure;

- Name of each entity or person who received the PHI, and if known, the address of such entity or person;

- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or
    - A copy of the individual's authorization; or
    - A copy of a written request for a disclosure.

Any person in the IU's workforce who makes a "non-excepted" disclosure shall make a notation in the accounting log (or through an equivalent documentation mechanism) of the date, name of the person who received the PHI, a brief description of the PHI disclosed and a brief statement of the purpose of the disclosure.

Disclosures to the following persons/entities must be documented by the IU and available for an accounting (note that this is not an exhaustive list):

Non-excepted Disclosures Include:

- Release of PHI to an "authorized individual" (i.e., any governmental authority authorized by law to receive reports of abuse, neglect or domestic violence such as protective or social services agencies, state survey and certification agencies, ombudsmen for the aging for those in long-term care facilities, law enforcement or oversight) about victims of abuse, neglect or domestic violence;
- Release of PHI for Public Health Activities to Public Health Authorities authorized by law to collect or receive information in order to prevent or control disease, injury or disability, including reporting disease, injury, vital events such as birth or death and conducting public health surveillance, investigations and interventions and to report cases of child abuse or neglect, including the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention and state and local public health departments;
- Release of PHI for Health Oversight Activities (e.g., oversight of health care plans, oversight of health benefits plans, oversight of health care providers, oversight of health care and health care delivery, oversight of activities that involve resolution of consumer complaints, oversight of pharmaceuticals, medical products and devices, and a health oversight agency's analysis of trends in health care costs, quality, health care delivery, access to care, health insurance coverage for health oversight purposes, audits, civil, administrative or criminal investigations, inspection, licensure or disciplinary actions and civil, administrative or criminal proceedings and actions) to health oversight agencies (e.g., an agency or authority of the U.S., a State, a territory or political subdivision of a State or territory or an Indian Tribe that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance or to enforce civil rights laws for which health information is relevant. Examples include: State insurance commissions, State health professional licensure agencies, Offices of Inspector Generals, the Department of Justice, State Medicaid fraud control units, the Health and Human Services Office for Civil Rights, the Office of the Attorney General and the FDA);
- Release of PHI to Avert a Serious Threat to Health or Safety to a Person or the Public;
- Release of PHI to a Person/Entity Responsible for Payment of Worker's Compensation Benefits to the Individual;
- Release of PHI to Funeral Directors/Homes;
- Release of PHI to the Medical Examiner or Coroner;

- Release of PHI to Law Enforcement; and
- Release of PHI Related to Organ Donation Activities.

For routine disclosures (those where the IU has made multiple disclosures of PHI to the same person or entity for a single purpose or pursuant to a single authorization), the accounting may provide:

- The information required above for the first disclosure during the accounting period;
- The frequency or number of disclosures made during the accounting period; and
- The date of the last disclosure during the accounting period.

The IU must act on the individual's request for an accounting no later than 60 days after receipt of the request. In the event the IU is unable to provide an accounting within 60 days, the IU may extend the time to provide the accounting for no more than 30 days, provided that the IU advises the individual with a written statement of the reasons for the delay and date by which it will provide the accounting. The IU may only have one such extension.

The IU must provide one accounting per year without charge. Thereafter, the IU may impose a reasonable, cost-based fee for each subsequent request within a 12-month period, provided that the individual is informed in advance of the cost.

The HIPAA Privacy Officer shall be notified of each request for an accounting, shall direct the process of the accountings and shall review each response prior to its provision to the individual. The HIPAA Privacy Officer shall direct that a copy of the accounting be maintained in the individual's file.

The IU must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official if the agency/official provides the IU with a written statement that: 1) such an accounting to the individual would be reasonably likely to impede the agency's activities; and 2) specifying the time for which the suspension is required. If the agency or official statement is made orally: (1) document the statement, including the identity of the agency or official making the statement; (2) temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (3) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Accounting for Electronic Health Record Disclosures.

If the IU acquired an EHR system prior to or by January 1, 2009:

- Starting on January 1, 2014, the IU shall afford each individual the right to receive an accounting of disclosures of PHI through an EHR made by the IU, covering a period of three (3) years preceding the request.

If the IU acquired and EHR system after January 1, 2009:

- Starting on January 1, 2011 or the date that the IU acquires an EHR, whichever date is later, the IU shall afford each individual the right to receive an accounting of disclosures of PHI through the EHR made by the IU, covering a period of three (3) years preceding the request.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***State-Specific Procedures***

Topic: **HIV-AIDS INFORMATION**

Date Adopted: **February 12, 2014**

Policy:

Any and all PHI which contains identifying information about an individual who has or is suspected of having Acquired Immune Deficiency Syndrome ("AIDS") or HIV (which means an infection with the human immunodeficiency virus or any other related virus identified as a probable causative agent of AIDS) (collectively, the "HIV/AIDS Records") is maintained by the IU in the highest of confidence.

Specific informed written consent of the individual is required prior to any episodic use and disclosure of HIV/AIDS Records, except for the limited treatment purposes described in the next paragraph.

In the event the prior written consent of such individual is not obtained, the IU permits HIV/AIDS Records to be disclosed only under the following limited conditions:

- To qualified personnel for the purpose of conducting scientific research, but a record shall be released for research only following review of the research protocol by an Institutional Review Board constituted pursuant to federal regulation 45 CFR § 46.101 et seq. Note that the individual who is the subject of the record shall not be identified, directly or indirectly, in any report of the research and research personnel shall not disclose the individual's identity in any manner;

- To qualified personnel for the purpose of conducting management audits, financial audits or program evaluation, but the personnel shall not identify, directly or indirectly, the individual who is the subject of the record in a report of an audit or evaluation, or otherwise disclose the individual's identity in any manner. Identifying information shall not be released to the personnel unless it is vital to the audit or evaluation;

- To qualified personnel involved in medical education or in the diagnosis or treatment of the person who is the subject of the record. Disclosure is limited to personnel directly involved in the medical education or in the diagnosis and treatment of the person;

- To the State Department of Health as required by State or federal law;

- As permitted by rules and regulations adopted by the State Commissioner of Health for the purposes of disease prevention and control;

- In all other instances authorized by State or federal law; or

- By court order which is granted pursuant to an application showing "good cause."

These limits on disclosure of HIV/AIDS Records shall continue to apply for as long as such records are maintained by the IU.

Procedures:

Prior to any use and disclosure of HIV/AIDS Records, obtain the individual's prior written consent.

Prior to disclosing HIV/AIDS Records as permitted under this policy, without an individual's prior written consent, notify and consult with the IU's HIPAA Privacy Officer. In any matter referred to or otherwise being resolved by the HIPAA Privacy Officer, the HIPAA Privacy Officer together with counsel shall evaluate the request for PHI in light of all relevant policies and laws, and shall determine whether the disclosure of the PHI may be made.

Document all requests for HIV/AIDS Records under this procedure, the actions taken to determine whether the disclosure could be made, the IU's decision regarding the request and, if a disclosure was made, a description in the log in accordance with the IU's Accounting of Disclosures policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***State-Specific Procedures***

Topic: **DRUG & ALCOHOL TREATMENT INFORMATION**

Date Adopted: **February 12, 2014**

Policy:

The IU maintains any and all PHI which contains identifying information regarding the diagnosis, prognosis or treatment of an individual for alcohol and/or drug abuse, which is received from a drug or alcohol treatment facility (collectively, the "Alcohol/Drug Abuse Records") in the highest confidence.

Alcohol/Drug Abuse Records shall not be disclosed for any reason whatsoever, unless the IU obtains the specific informed written consent of the individual, who is the subject of the Alcohol/Drug Records, prior to the disclosure.

In the event the prior written consent of such individual is not obtained, the Alcohol/Drug Records may only be disclosed under the following limited conditions:

- To medical personnel to the extent necessary to meet a bona fide medical emergency;
- To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual in any report of such research, audit, or evaluation, or otherwise disclose individual identities in any manner; or
- If authorized by an appropriate court order granted upon a showing good cause.

Except for disclosure by court order, Alcohol/Drug Abuse Records may not be used or disclosed (without an individual's prior written consent), to initiate or substantiate any criminal charges against an individual or to conduct any investigation of an individual.

The limits on disclosure of Alcohol/Drug Abuse Records shall continue to apply for as long as such information is maintained by the IU.

Procedures:

Prior to the use and disclosure of Alcohol/Drug Abuse Records, obtain the individual's specific prior written consent.

The foregoing restrictions are not meant to prevent an individual from accessing his or her own records, including the opportunity to inspect and copy any records that the IU maintains about the individual.

Each disclosure of Alcohol/Drug Abuse Records made with the individual's written consent must be accompanied by the following written statement:

NOTICE TO RECIPIENT OF INFORMATION

> "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any individual for alcohol or drug abuse."

Prior to disclosing Alcohol/Drug Abuse Records without an individual's prior written consent, notify and consult with the IU's HIPAA Privacy Officer. There are specific requirements under federal law, which govern how disclosures of Alcohol/Drug Abuse Records are to be handled in the event of medical emergencies (e.g., how such disclosures are to be documented); disclosures in the course of audit and evaluation activities (e.g., when Alcohol/Drug Abuse Records may be copied or removed); and presentment of a court order (e.g., whether the IU should comply with the court order. Note that a court order does not compel disclosure, unless a subpoena or other similar legal mandate is issued to compel disclosure).

In any matter referred to or otherwise being resolved by the HIPAA Privacy Officer, the HIPAA Privacy Officer together with counsel shall evaluate the request for PHI in light of all relevant policies and laws, and shall determine whether the disclosure of the PHI may be made.

Document all requests for Alcohol/Drug Abuse Records, the actions taken to determine whether the disclosure can be made, the IU's decision regarding the request and, if a disclosure was made, a description in the log in accordance with the IU's Accounting of Disclosures policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
PRIVACY POLICIES & PROCEDURES

Category: ***State-Specific Procedures***

Topic: **MINORS**

Date Adopted: **February 12, 2014**

Policy:

In general, the IU may use or disclose PHI regarding a minor individual ("Minor Records") to the minor individual's parent, guardian, or other person acting in loco parentis (collectively, the "Parent"), and may treat the Parent as the minor's "personal representative" with respect to the Minor Records.

However, in certain situations, where minors are authorized under applicable law to consent to a particular health care service, the IU will not treat the Parent as the personal representative, and the minor (not the Parent) can consent to and authorize any use and disclosure of their individual information.

The IU recognizes that under Pennsylvania law, minors can consent to and authorize disclosure of their Minor Records if:

(1) Married;

(2) Pregnant (and seeking health care services related to the pregnancy or the minor individual's child);

(3) Being treated for Alcohol or Drug Abuse;

(4) Being treated for Venereal Disease or Sexual Assault;

(5) The minor is 12 years old or older, and his or her individual information relates to AIDS or HIV infection; or

(6) Emancipated (18 years old or older).

TheIU routinely checks for any changes in state law with respect to the foregoing.

Notwithstanding the foregoing, the ultimate decision to provide or deny access to Minor Records is made by the minor's treating physician, in the exercise of professional judgment. This means that the treating physician of the minor individual may (but is not required to), (i) deny the Parent access to the Minor Records; (ii) not treat the Parent as the personal representative of the minor individual; and (iii) inform the Parent of the minor individual's treatment for health care services (including treatment for venereal disease and alcohol/drug abuse).

Procedures:

Prior to disclosing Minor Records to a Parent without a minor individual's prior written consent, determine whether the Minor has sought medical treatment independently with authority under State law, and whether the minor must be treated as the individual with authority to control access and disclosure to his or her PHI.

Notify and consult with the minor individual's treating physician to assess whether the Minor's Records should be withheld or provided to a Parent.

The Minor's treating physician (and HIPAA Privacy Officer, as necessary) shall evaluate the request for Minor's Records in light of all relevant policies and laws, and shall determine whether the disclosure of PHI may be made.

The IU must document all requests for individual Information under this procedure, the actions taken to determine whether the disclosure can be made, the IU's decision regarding the request and, if a disclosure was made, a description in the log in accordance with the IU's Accounting of Disclosures policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13

HIPAA COMPLIANCE PROGRAM:

SECURITY POLICIES & PROCEDURES

* Unless otherwise defined in these Security Policies and Procedures, the terms used herein shall have the meanings and definitions assigned to such terms in the HIPAA Privacy and Security Regulations, 45 C.F.R Part 160, 162 and 164 *

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Technical Safeguards***

Topic: **ACCESS CONTROLS**

Date Adopted: **February 12, 2014**

Policy:

The IU maintains technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those person or software programs that have been granted access rights. To accomplish this, the IU has implemented the following:

- A unique user identification system that assigns a unique name and/or number for identifying and tracking identity. (Required).
- Emergency access procedures for obtaining necessary e-PHI during an emergency. (Required).
- "Reasonable and appropriate" electronic procedures that terminate an electronic session after a predetermined time of inactivity (e.g., automatic logoff). (Addressable).
- "Reasonable and appropriate" mechanisms to encrypt and decrypt e-PHI. (Addressable)

Procedures:

Assessment & Evaluation

- Identify the applications and systems that require access controls. The focus shall be on the applications or systems housing e-PHI (e.g., stand-alone PC, network).
- With respect to all applications, systems and data where it has been determined that access control is required, determine the scope and degree of access control needed. (Consider how the systems are being accessed: Is the data and/or system being accessed remotely? Is the data being viewed only? Is the data being modified? Is new date being created and stored on the system? Consider whether passwords are being used and if so, whether they are unique to the individual.)

Unique Identifier

- Assign a unique identifier to all systems users.
- Ensure that system activity can be traced to a specific user.
- Ensure that the necessary data is available in the system logs to support audit and other related business functions.

Develop Access Control Policy

- Establish a formal policy for access control that will guide the development procedures.
- Implement access control procedures using selected hardware and software.

- Implement electronic procedures that terminate an electronic session after a predetermined period of inactivity (e.g., "automatic logoff"). If it is not "reasonable and appropriate" to implement automatic logoff procedures, the reasons why and a reasonable alternative shall be documented. (See attached form).

- Implement mechanisms to encrypt and decrypt e-PHI. If it is not "reasonable and appropriate" to implement mechanisms for encryption and decryption, the reasons why and a reasonable alternative shall be documented. (See attached form).

Emergency Access

- Identify a method of supporting continuity of operations in the event that the normal access procedures become disabled or unavailable due to system problems.

- Emergency access procedures should be activated when: _____
_____

- The HIPAA Security Officer is authorized to make the decision to activate emergency access procedures.

- Emergency access procedures will be supported by individuals designated to support this process.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

APPENDIX

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Automatic Logoff***

(a) It is not "reasonable and appropriate" to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity because:

_____
_____
_____

Provider shall use the following reasonable alternative to implementing such procedures: _____
_____
_____
_____

(b) If it is not "reasonable and appropriate" to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity and there are no reasonable alternatives the reasons why are: _____
_____
_____
_____
_____

2. Encryption and decryption

(a) It is not "reasonable and appropriate" to implement mechanisms to encrypt and decrypt e-PHI because: _____
_____
_____

Provider shall use the following reasonable alternative to implementing such mechanisms:

_____
_____
_____

If is not "reasonable and appropriate" to implement mechanisms to encrypt and decrypt e-PHI and there are no reasonable alternatives, the reasons why are:

_____
_____
_____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Technical Safeguards***

Topic: **AUDIT CONTROLS**

Date Adopted: **February 12, 2014**

Policy:

Activity in the IU's information systems that contain or use e-PHI are recorded and examined by hardware, software and/or procedural mechanisms.

Procedures:

- Identify the systems or activities that the IU will track or audit. The focus shall be on the e-PHI that is most at risk. Determine the appropriate scope of system audits.

- Use the results of the risk assessment to determine which systems and activities should be tracked and audited. Monitor, create, read, update and delete.

- The audit record should include user ID, event type/date/time. These shall be reviewed periodically and suspect activity reported to the HIPAA Security Officer.

- Existing system capabilities and tools for tracking shall be evaluated and changes or upgrades shall be made as necessary.

- Determine how decisions on audits and reviews and shall be made, and who is responsible for the overall audit process and results, the frequency of audits, how they will be analyzed, the sanction policy for employee violations and maintenance of audit information.

- Train the workforce on how the review/audit policy could affect them.

- Address how the exception reports will be reviewed, where the monitoring reports will be filed and maintained, whether there is a formal process in place to address system misuse, abuse and fraudulent activity and how appropriate employees will be notified regarding suspect activity.

- The effectiveness of the audit/system activity review process shall be reviewed annually and revised if necessary.

- Audits shall include processes for detecting any potential Security Breach of PHI (including electronic, paper or oral), as more particularly described in the IU's Security Breach Notification Policies and Procedures. The HIPAA Security Officer and HIPAA Privacy Officer shall coordinate investigating, evaluating and responding to any instance where a potential Security Breach is detected through a security audit, all in accordance with the IU's Security Breach Notification Policies and Procedures.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Technical Safeguards***

Topic: **INTEGRITY**

Date Adopted: **February 12, 2014**

Policy:

The IU protects e-PHI from improper alteration or destruction through implementation of "reasonable and appropriate" mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner. If it is not "reasonable and appropriate" to implement such mechanisms for corroborating that e-PHI has not been altered or destroyed in an unauthorized manner, the reasons why and a reasonable alternative are documented. (See attached form).

Procedures:

- Identify all users who have been authorized to access e-PHI. Identify all approved users with the ability to alter or destroy data.
- Identify any possible unauthorized sources that may be able to intercept the information and modify it, including identifying scenarios that may result in modification to the e-PHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).
- Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.
- Implement procedures to address these requirements. Identify which methods will be used to protect the information from modification. Identify tools and techniques to be developed or procured that support the assurance of integrity.
- Monitor process to assess and "audit" effectiveness of integrity safeguards.
- Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Electronic Corroboration***

(a) It is not "reasonable and appropriate" to implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner because: _____

_____

_____

Provider shall use the following reasonable alternative to implementing such mechanisms: _____

_____

_____

(b) If it is not "reasonable and appropriate" to implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner and there are no reasonable alternatives the reasons why are: _____

_____

_____

_____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Technical Safeguards***

Topic: **PERSON/ENTITY AUTHENTICATION**

Date Adopted: **February 12, 2014**

Policy:

The IU authenticates persons or entities seeking to access e-PHI

Procedures:

- Identify technological methods available for authentication. Authentication is the process of establishing the validity of a transmission source or verifying an individual's authorization claim for specific access privileges to information and information systems.
- Evaluate authentication options available. Weigh the relative advantages and disadvantages of commonly used authentication approaches. There are four commonly used authentication approaches available:
    - Something a person knows, such as a password;
    - Something a person has or is in possession of, such as a token (smart card, ATM card, etc.);
    - Some type of biometric identification a person provides, such as a fingerprint; or
    - A combination of two or more of the above approaches.
- Select and implement the authentication method most appropriate for the IU.
- Evaluate methods as needed, but at least annually, and update or revise as needed.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Technical Safeguards***

Topic: **TRANSMISSION SECURITY**

Date Adopted: **February 12, 2014**

Policy:

The IU guards against unauthorized access to e-PHI that is being transmitted over an electronic communication network through the implementation of "reasonable and appropriate" security measures to ensure that electronically transmitted e-PHI is not improperly modified without deletion until disposed of. If it is not "reasonable and appropriate" to implement such security measures, the reasons why and a reasonable alternative are documented. (See attached form).

The IU uses "reasonable and appropriate" mechanisms to encrypt e-PHI whenever deemed appropriate. If it is not "reasonable and appropriate" to implement a mechanism for encrypting e-PHI, the reasons why and a reasonable alternative are documented. (See attached form).

Procedures:

- Identify possible unauthorized sources that may be able to intercept and/or modify e-PHI. Identify scenarios that may result in modification to the e-PHI by unauthorized sources during transmission (e.g., hackers, disgruntled employees, business competitors).

- Develop and implement a formal (written) set of requirements for transmitting e-PHI.

- Implement procedures for transmitting e-PHI using hardware/software if needed, identify methods of transmission that will be used to protect e-PHI. Identify tools and techniques that will be used to support the transmission security policy.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Transmission***

(a) It is not "reasonable and appropriate" to implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without deletion until disposed of because:_____

Provider shall use the following reasonable alternative to implementing such measures: _____

(b) **It** is not "reasonable and appropriate" to implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without deletion and there are no reasonable alternatives the reasons why are: _____

2. ***Encryption***

(a) **If** is not "reasonable and appropriate" to implement mechanism to encrypt e-PHI whenever deemed appropriate because:_____

Provider shall use the following reasonable alternative to implementing such a mechanism: _____

(b) **If** is not "reasonable and appropriate" to implement mechanism to encrypt e-PHI whenever deemed appropriate and there are no reasonable alternatives the reasons why are: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Physical Safeguards***

Topic: **FACILITY ACCESS CONTROLS**

Date Adopted: **February 12, 2014**

Policy:

The IU limits physical access to electronic information systems and the facility in which such systems are housed, while ensuring that properly authorized access is allowed.

This is accomplished through:

- Maintenance Records: Implementing "reasonable and appropriate" procedures to document repairs and modifications to the physical components of the facility which are related to security (e.g., hardware, walls, doors and locks). (Addressable).

- Facility Security Plan: Implementing "reasonable and appropriate" procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft. (Addressable).

- Access Control and Validation: Implementing "reasonable and appropriate" procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision. (Addressable).

- Contingency Operations: Establishing "reasonable and appropriate" procedures that allow facility access in support of restoration of lost data under disaster recovery plan and emergency mode operations plan. (Addressable).

Procedures:

Conduct an Analysis of Physical Security Vulnerabilities

- On a periodic basis, identify and conduct an analysis of existing physical security vulnerabilities and create a "facility inventory." [Consider the following: Are non-public areas locked? Are cameras utilized? Are workstations protected from public viewing? Are entrances/exits secure? What is the threat to the particular environment? What are the current policies and procedures regarding access to and use of facilities and equipment?]

- Based on the inventory, assign degrees of significance to each vulnerability identified (e.g., high, medium, low). Highest priority should be assigned to: (1) data centers, (2) peripheral equipment locations, (3) IT staff offices, and (4) workstation locations.

Identify Corrective Actions

- Based on the list created, identify the measures and activities necessary to correct any deficiencies.

- Review all policies and procedures governing the assessment, identification and corrective measure for deficiencies to determine whether they need revision, and maintain them for easy review.

- Ensure that necessary repairs, upgrades, and/or modifications are made to the appropriate physical areas of the IU on a regular basis and as needed.

- All physical components that require maintenance and/or are subject to repair shall be identified and maintenance logs shall be kept. Examples of physical components include:

    - Grounds security (gates, alarms, communication, systems);

    - Building security (doors, walls, hardware, locks, fireproofing, sprinkler systems, smoke detection);

    - Equipment and devices used by security personnel (televisions, monitors, CB radios, pagers);

    - Information system security (computers, servers, back-up systems).

- Maintain physical maintenance records, which shall include history of changes, upgrades and other modifications.

- If it is not "reasonable and appropriate" to document repairs and modifications to the physical components of the facility that are related to security, document the reasons why and provide a reasonable alternative. (See attached form).

- Retain maintenance records for six (6) years.

Facility Security Plan and Access Control

- Develop a "Facility Security Plan" that addresses the physical security protection of e-PHI in the IU's possession.

- If it is not "reasonable and appropriate" to implement procedures to safeguard a particular location at the facility and or certain equipment therein from unauthorized physical access, tampering and theft, document the reasons why and a reasonable alternative. (See attached form).

- Develop facility access control procedures to limit and control access to e-PHI by staff, contractors, visitors and probationary employees. If it is not "reasonable and appropriate" to establish procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision and document the reasons why and provide a reasonable alternative. (See attached form).

Contingency Operations

- The Disaster Recovery Plan and Emergency Mode Operations Plans ("EMOP") shall generally control during emergency mode operations (see Security policy and procedure: "Contingency Plans"). However, under emergency circumstances, authorized entry must be provided to certain emergency response personnel.

- Any personnel and/or individuals that must be provided access to the e-PHI in the event of an emergency or a disaster shall be identified and listed in a contingency plan. The individual responsible for implementing the contingency plans in each department/unit etc. shall be identified in the contingency plan.

- The HIPAA Security Officer, and his or her designee, shall be responsible for developing the contingency plan for facility access to the IU in the event of an emergency or disaster.

- If it is not "reasonable and appropriate" to establish procedures that allow facility access in support of restoration of lost data under the disaster recover plan and emergency mode operations plan, document the reasons why and a reasonable alternative (See attached form).

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Facility Security Plan***

(a) It is not "reasonable and appropriate" to implement procedures to safeguard the IU and the equipment therein from unauthorized physical access, tampering and theft because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **It** is not "reasonable and appropriate" to implement procedures to safeguard the IU and the equipment therein from unauthorized physical access, tampering and theft and there are no reasonable alternatives the reasons why are: _____

2. ***Repairs and Modifications to Facility***

(a) It is not "reasonable and appropriate" to implement procedures to document repairs and modifications to the physical components of the IU which are related to security because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) If is not "reasonable and appropriate" to implement procedures to document repairs and modifications to the physical components of the IU which are related to security and there are no reasonable alternatives, the reasons why are: _____

3. ***Control and Validation of Access Based on Role or Function***

(a) It is not "reasonable and appropriate" to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision and there are no reasonable alternatives the reasons why are: _____

4. ***Contingency Operations***

(a) It is not "reasonable and appropriate" to implement procedures that allow facility access in support of restoration of lost data under disaster recovery plan and emergency mode operations plan because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures that allow facility access in support of restoration of lost data under disaster recovery plan and emergency mode operations plan and there are no reasonable alternatives the reasons why are: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Physical Safeguards***

Topic: **WORKSTATION USE**

Date Adopted: **February 12, 2014**

Policy:

It is the policy of the IU regarding workstation use that: (1) only proper functions are to be performed; (2) the manner in which those functions are to be performed are understood and executed by its workforce; and (3) physical attributes of the surroundings of a specific workstation or class of workstation that can access e-PHI are safeguarded.

Procedures:

- Identify all workstations, their functions and uses.
- Classify workstations based on the capabilities, connections and allowable activities for each workstation used.
- Identify the expected performance of each type of workstation. Develop specific workstation procedures related to the proper use and performance of particular stations.
- Analyze the physical surroundings and review the risks associated with a workstation's surroundings.
- Implement procedures that will prevent or preclude unauthorized access of unattended workstations and limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.
- Train employees on the use requirements based on workstations used by such employees.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Physical Safeguards***

Topic: **WORKSTATION SECURITY**

Date Adopted: **February 12, 2014**

Policy:

The IU utilizes physical safeguards for all workstations that access e-PHI to restrict access to unauthorized users.

Procedures:

- Identify all methods of physical access to workstations (including workstations located in public areas and laptops that are used as workstations).
- Identify which physical safeguards are in place (e.g., locked doors, screen barriers, cameras, guard etc.) and identify any gaps.
- Analyze the risk associated with each type of access and determine what type of access holds the greatest threat to security.
- Add additional physical safeguards to minimize the risk to security of e-PHI at workstations.
- If none of the identified physical safeguards will sufficiently minimize the risk to security of e-PHI, workstations shall be relocated to enhance physical security.
- Periodically train employees on workstation security.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Physical Safeguards***

Topic: **DEVICE & MEDIA CONTROLS**

Date Adopted: **February 12, 2014**

Policy:

The receipt and removal of hardware and electronic media that contain e-PHI into and out of the IU and the movement of these items within the IU are safeguarded through implementation of:

- Procedures to address the final disposition of e-PHI and/or the hardware or electronic media on which it is stored;
- Procedures for removal of e-PHI from electronic media before the media are made available for reuse;
- A "reasonable and appropriate" system for keeping maintenance records that document the movement of hardware and electronic media and any person responsible therefore. (Addressable); and
- "Reasonable and appropriate" methods to create a retrievable exact copy of e-PHI, when needed, before movement of equipment. (Addressable).

Procedures:

Disposal & Reuse of e-PHI

- Identify all e-PHI maintained by the IU and the location(s) where data is maintained.
- Evaluate and review the methods for disposal of e-PHI for each location identified.
- Determine and document the approved methods to dispose of hardware, software, and the data itself. This shall include selected processes for destroying data on hard drives and file servers.
- Ensure that e-PHI is properly destroyed and cannot be recreated through location-specific procedures governing disposal.
- Implement procedures for how to reuse electronic media. Turn over to IT, as appropriate.
- Ensure that e-PHI previously stored on electronic media cannot be accessed and reused.
- Identify all removable devices, and review and approve all permitted uses. If certain devices cannot be removed off premises, specify such information on the device.
- Select the individual(s) and/or department that is responsible for coordinating the disposal of data, and the reuse of the hardware and software.
- Train all employees on the security and risks to e-PHI when reusing software and hardware.

Equipment Relocation – Accountability & Backup

- Records relating to hardware, media and personnel shall be maintained.

- Ensure that e-PHI is not inadvertently released or shared with any unauthorized party.

- A record of the movements of hardware and electronic media, and the person responsible therefore, shall be maintained ("Equipment Relocation History"). If it is not "reasonable and appropriate" to maintain a record of the movements of hardware and electronic media and any person responsible therefore, document the reasons why and a reasonable alternative. (See attached form).

- Develop and implement backup procedures to ensure that the integrity of e-PHI will not be jeopardized during equipment relocation.

- Retain and protect an exact, retrievable copy of the data until equipment relocation is completed. If it is not "reasonable and appropriate" to create a retrievable, exact copy of e-PHI when needed, before movement of equipment, document the reasons why and a reasonable alternative (See attached form).

- Develop and implement a contingency plan procedure to control in the event of a failure of data backup.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Equipment Relocation – Accountability***

(a) It is not "reasonable and appropriate" to maintain a record of the movements of hardware and electronic media and any person responsible therefore because: _____

The IU shall use the following reasonable alternative to maintaining Equipment Relocation History: _____

(b) **If** is not "reasonable and appropriate to maintain a record of the movements of hardware and electronic media and any person responsible therefore and there are no reasonable alternatives, the reasons why are: _____

2. ***Equipment Relocation – Backup***

(a) It is not "reasonable and appropriate" to create a retrievable, exact copy of e-PHI when needed, before movement of equipment because: _____

The IU shall use the following reasonable alternative to creating retrievable, exact copies of e-PHI when needed, before movement of equipment: _____

(b) If is not "reasonable and appropriate" to create a retrievable, exact copy of e-PHI when needed, before movement of equipment and there are no reasonable alternatives, the reasons why are: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **SECURITY MANAGEMENT PROCESS**

Date Adopted: **February 12, 2014**

Policy:

The IU strives to prevent, detect, contain and correct all security violations. To accomplish this, the IU:

- Performs a risk analysis whereby the potential risks and vulnerabilities to confidentiality, integrity, and availability of e-PHI are assessed (Required);
- Implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level (Required);
- Applies sanctions against workforce who fail to comply with security policies and procedures (Required); and
- Implements procedures to regularly review records of information system activity, such a audit logs, access reports and security incident tracking reports (Required).

Procedures:

- Identify relevant information systems that store e-PHI, either temporarily or permanently. Include all hardware and software that are used to collect, store, process, or transmit e-PHI.
- Analyze business functions and verify ownership and control of information system elements as necessary. The following should be considered:
    - Who or what organization is responsible for the specific hardware or software.
    - Whether the current information system configuration documents, including connection to other systems?
    - Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated?
- Conduct a risk assessment and determine:
    - What is the system characterization (e.g., hardware, software, system interfaces, data and information, and people)?
    - What is the system mission?
    - Are there vulnerabilities or weaknesses in security procedures or safeguards?
    - Are there any events that can negatively impact security?
    - What are the controls in place?

- What is the potential impact that a security breach could have on the IU's operations or assets, including loss of integrity, availability or confidentiality.

- What are the recommended security controls for the information and the system, including all the technical and non-technical protections in place to address security concerns?

- What is the residual risk?

- Document output and outcomes from the risk assessment.

- Determine whether additional hardware, software and/or services may be needed to adequately protect e-PHI and, if so, make appropriate selections taking into consideration: (1) applicability of the IT solution to the environment; (2) sensitivity of data; (3) the IU's Security policies; procedures and standards; and (4) resources available for operation, maintenance and training.

- Document the decisions concerning the management, operational, and technical controls selected to mitigate identified risks.

- Identify individuals or officers responsible for the implementation of each control.

- Develop and implement procedures to be followed to accomplish particular security related tasks.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **ASSIGNED SECURITY RESPONSIBILITY**

Date Adopted: **February 12, 2014**

Policy:

The IU's HIPAA Security Officer is responsible for developing, implementing, monitoring and assuring enforcement of the IU's Security Policies and Procedures.

Procedures:

- The IU shall select and approve an individual who is able to assess effective HIPAA security and to serve as the point of contact for security policy, implementation, and monitoring. The individual shall be identified by name, title or both. A resolution appointing the individual will be signed by the governing body.

- Document the HIPAA Security Officer's responsibilities in a written job description reflecting assigned security duties and the responsibilities of the security official.

- Review the job description periodically.

- Make the identity of the appointed HIPAA Security Officer known to the entire organization so that employees at the IU know who to contact in the event of a HIPAA security problem.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **STANDARD WORKFORCE SECURITY**

Date Adopted: **February 12, 2014**

Policy:

It is the policy of the IU that all members of the workforce who need to access e-PHI have appropriate access to e-PHI, and those who do not are prevented from obtaining access.

Procedures:

Authorization and Supervision

- The HIPAA Security Officer, in conjunction with the HIPAA Privacy Officer and Human Resources, shall establish security roles and responsibilities for all job functions.

- Develop a table assigning each job function the appropriate levels of security oversight, training, and access.

    - Relevant definitions related to this process are:

"Limited" means, with respect to:

> Access & Oversight: is not permitted to access any e-PHI without first obtaining approval and oversight by an individual who has at least "Full" access rights with that department from which e-PHI is sought.

"Basic" means, with respect to:

> Access & Oversight: is permitted to access some e-PHI within the department he or she works; is not permitted to access any e-PHI kept in a separate department without first obtaining approval and oversight from an individual working in that "other department" who has at least "Full" access rights in that department

"Full" means, with respect to:

> Access & Oversight: (1) is permitted to access any and all e-PHI within the department he or she works; (2) is permitted to access some e-PHI in a separate department, which is "directly related to" treatment that must be provided or functions that must be performed for the department he or she works; (3) is not Permitted to access any other e-PHI kept in a separate department without first obtaining approval and oversight from an individual working in that "other department" who has at least "Full" access rights in that department.

"Unlimited" means, with respect to:

> Access: "is permitted to access any and all types of e-PHI maintained, received or Created by any department at the IU without any approval and/or oversight.

"Scope of Rights" defines whether an individual may view, retrieve, store and/or amend e-PHI.

- Identify which members of the workforce have the business need, and which have been granted permission, to view, alter, retrieve, and store e-PHI, and at what time, under what circumstances, and for what purposes.

- If it is not "reasonable and appropriate" to implement procedures allowing for the authorization and/or supervision of workforce members who work with e-PHI or in location where it might be accessed, document the reasons why and a reasonable alternative. (See attached form).

Workforce Clearance Procedures

- Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles, e.g., positions involving access to and use of sensitive information.

- Prospective employees shall be questioned with respect to their knowledge about privacy and security requirements.

- Complete employment and educational reference checks, as well as appropriate background checks.

- If it is not "reasonable and appropriate" to implement procedures allowing for the IU to determine that the access of a workforce member to e-PHI is appropriate, document the reasons why and a reasonable alternative. (See attached form).

Termination Procedures

- Develop (with Human Resources) a standard set of procedures to be followed to recover access control devices (e.g., identification badges, keys, access cards, etc.) when employment ends as a result of voluntary termination (e.g., retirement, promotion, change of employment) or involuntary termination (e.g., termination for cause, reduction in force, involuntary transfer, and criminal or disciplinary actions).

- The HIPAA Security Officer shall work with the HIPAA Privacy Officer and Human Resources to create a standard checklist for items to be completed when an employee leaves. The checklist shall include:

    - Return of access devices

    - Deactivation of logon accounts

    - Delivery of needed data solely under the employee's control.

- The HIPAA Security Officer shall be responsible for assuring that mechanisms are in place to deactivate computer access accounts (e.g., disable user IDs and passwords).

- If it is not "reasonable and appropriate" to implement procedures for terminating access to e-PHI when the employment of a workforce member ends, document the reasons why and provide a reasonable alternative. (See attached form).

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Authorization and Supervision***

(a) It is not "reasonable and appropriate" to implement procedures allowing for the authorization and/or supervision of workforce members who work with e-PHI or in location where it might be accessed because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures allowing for the authorization and/or supervision of workforce members and there are no reasonable alternatives, the reasons why are: _____

2. ***Workforce Clearance Procedures***

(a) It is not "reasonable and appropriate" to implement procedures allowing for the IU to determine that the access of a workforce member to e-PHI is appropriate because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures allowing for the IU to determine that the access of a workforce member to e-PHI is appropriate and there are no reasonable alternatives, the reasons why are: _____

3. ***Termination Procedures***

(a) It is not "reasonable and appropriate" to implement procedures for terminating access to e-PHI when the employment of a workforce member ends because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures for terminating access to e-PHI when the employment of a workforce member ends and there are no reasonable alternatives, the reasons why are: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **INFORMATION ACCESS MANAGEMENT**

Date Adopted: **February 12, 2014**

Policy:

The IU maintains policies and procedures to determine access authority to e-PHI.

Procedures:

Access Authorization

- Determine how access to workstations, transactions, programs, processes and other mechanisms will be determined.
- Determine restrictions on access, which can be identity-based, role-based, location-based, or some combination.
- Establish standards for granting access. Formal authorization should be obtained from the HIPAA Security Officer, or her/his designee, before access to sensitive information is permitted to any user. Only the minimum necessary e-PHI should be made available to each employee based on their job requirements.
- If it is not "reasonable and appropriate" to implement procedures to govern granting access to e-PHI, document the **reasons why and a reasonable alternative shall be provided. (See attached form).**

Access Establishment and Modification

- Evaluate access controls already in place or implement new access controls as appropriate.
- Evaluate access controls and policies routinely and as needed.
- The HIPAA Security Officer shall coordinate with other existing management, operational, and technical controls, such as policy standards and personnel procedures, maintenance and review of audit trails, identification and authentication of users, and physical access controls.
- Members of the workforce shall receive security training upon hire and shall receive at least annual updates. Confirmation of this training shall be maintained by the HIPAA Security Officer with a copy sent to the IU's Human Resources Department.
- If it is not "reasonable and appropriate" to implement procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process, document the reasons why and a reasonable alternative (See attached form).

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Access Authorization***

(a) It is not "reasonable and appropriate" to implement procedures to govern granting access to e-PHI because: _____

_____

_____

_____

The IU shall use the following reasonable alternative to implementing such procedures: _____

_____

_____

_____

(b) **If** is not "reasonable and appropriate" to implement procedures to govern granting access to e-PHI and there are no reasonable alternatives, the reasons why are: _____

_____

_____

_____

2. ***Access Establishment and Modification***

(a) It is not "reasonable and appropriate" to implement procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process because: _____

_____

_____

_____

The IU shall use the following reasonable alternative to implementing such procedures: _____

_____

_____

_____

(b) **If** is not "reasonable and appropriate" to implement procedures that establish, document, review and modify a user's right of access to a workstation, transaction, program or process and there are no reasonable alternatives, the reasons why are: _____

_____

_____

_____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **TRAINING**

Date Adopted: **February 12, 2014**

Policy:

HIPAA security awareness and training is provided to all members of the workforce, including management. The content and scope of the training is appropriate to the IU and will include, but not be limited to, training affected employees on the IU's:

- Procedures for guarding against, detecting, and reporting malicious software;
- Procedures for monitoring log-in attempts and reporting discrepancies; and
- Procedures for creating, changing and safeguarding passwords.

In addition, the IU disseminates "reasonable and appropriate" periodic security updates and reminders. (Addressable).

Procedures:

Awareness and Training

- Assess employees knowledge of the IU's HIPAA Security policies and procedures (e.g., interviewing, written assessment etc.)
- Determine whether there are any gaps in employees' understanding, and what are the training needs that exist.
- Create a training strategy by identifying the specific HIPAA Security policies that require awareness and training and documenting them in a written "Security Awareness and Training Plan. (See sample attached).
- Prepare, update and use training materials.
- Schedule and conduct training as outlined in the Security Awareness and Training Plan. Focus on training appropriate to the individual, department, etc. given their access to e-PHI.
- Implement reasonable techniques to disseminate the security messages and updates at the IU. Newsletters, screensavers, videotapes, e-mail messages, teleconferencing sessions, staff meetings, and computer-based training may be used to disseminate information. If it is not "reasonable and appropriate" to disseminate periodic security updates and reminders, document the reasons why and a reasonable alternative. (See attached form).
- Keep the security awareness and training program fresh and current and conduct training whenever changes occur in the technology and practices, as appropriate.

- Monitor the training program implementation to ensure employee participation.

- Implement and document corrective action when problems arise.

Related Procedures

- Implement "reasonable and appropriate" procedures for guarding against, detecting, and reporting malicious software (e.g., viruses), and if not document the reasons why and a reasonable alternative (See attached form). (Addressable).

- Implement "reasonable and appropriate" procedures for monitoring log-in attempts and reporting discrepancies, and if not document the reasons why and a reasonable alternative. (See attached form). (Addressable).

- Implement "reasonable and appropriate" procedures for creating, changing and safeguarding passwords, and if not document the reasons why and a reasonable alternative. (See attached form). (Addressable).

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Awareness and Training***

(a) It is not "reasonable and appropriate" to disseminate periodic security updates and reminders because: _____

The IU shall use the following reasonable alternative to such updates and reminders: _____

(b) **If** is not "reasonable and appropriate" to disseminate periodic security updates and reminders and there are no reasonable alternatives, the reasons why are: _____

2. ***Guarding Against Malicious Software***

(a) It is not "reasonable and appropriate" to implement procedures for guarding against, detecting, and reporting malicious software because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures for guarding against, detecting, and reporting malicious software and there are no reasonable alternatives, the reasons why are: _____

3. ***Monitoring Log-In Attempts***

(a) It is not "reasonable and appropriate" to implement procedures for monitoring log-in attempts and reporting discrepancies because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures for monitoring log-in attempts and reporting discrepancies and there are no reasonable alternatives, the reasons why are: _____

4. ***Passwords***

(a) It is not "reasonable and appropriate" to implement procedures for creating, changing and safeguarding passwords because: _____

The IU shall use the following reasonable alternative to implementing such procedures: _____

(b) **If** is not "reasonable and appropriate" to implement procedures for creating, changing and safeguarding passwords and there are no reasonable alternatives, the reasons why are: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

SAMPLE
SECURITY AWARENESS AND TRAINING PLAN

The Security Awareness and Training Plan should outline the following:

- the plan
- the scope of awareness and training program
- the goals
- the target audiences
- the learning objectives
- the deployment methods, evaluation, & measurement techniques
- the frequency of training

Security Training Category: GENERAL:
Scope of Training: ENTIRE WORKFORCE (including management)
Training Responsibility:
Training Frequency: Upon Hire, and Annual

1. The Plan: _____

2. Goals: _____

3. Learning objectives:

   (a) Security Reminders

   (b) How to protect and guard the system from malicious software.

   (c) How to monitor log-in attempts and report discrepancies

   (d) Password Management

   (e) Incident reporting

   (f) Other: _____

4. Deployment methods: _____

5. Evaluation & measurement techniques to be Used: _____

Security Training Category: SPECIFIC:
Scope of Training: IT
Training Responsibility:
Training Frequency: Upon Hire, and Annual

1. The Plan: _____

2. Goals: _____

3. Learning objectives: _____

4. Deployment methods: _____

5. Evaluation & measurement techniques to be Used: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **SECURITY INCIDENT PROCEDURES**

Date Adopted: **February 12, 2014**

Policy:

The IU treats HIPAA security incidents with the highest concern and regard, and takes action to respond and address such matters as soon as reasonably possible.

Procedures:

- A "Security Incident" in the IU's environment includes, but is not limited to, the following: a "Security Breach" or an attempted "Hack."

- Determine first whether the Security Incident may also be a "Security Breach" which could trigger required notices and specific actions. Refer to the IU's Security Breach Notification Policy and Procedure first.

- All Security Incidents should be reported to the HIPAA Privacy and HIPAA Security Officer(s).

- The HIPAA Security Officer, in conjunction with the IU's [SPECIFY SUBSET OF IU?], may assemble a "Security Incident Response Team" to respond to reported Security Incidents. Such a team may be comprised of, but not limited to, the following individuals:

Response Team Member	Responsibility
Departmental Supervisor	- Intake of Security Incident Report - Coordination with HIPAA Security Officer
HIPAA Security Officer	- Intake of Security Incident Report - Oversight of Investigation and Outcome Report - Required Notifications
IU CEO	- Media Intervention - Law Enforcement Intervention - Business Partners Intervention
General Counsel	- Provide counsel for all third party Notifications and Interventions (e.g., media; law enforcement etc.)
IT Supervisor	- IT Intervention
Human Resources	- Employee Intervention (i.e., Sanctions)

- Develop and implement incident response procedures to guide the Incident Response Team. The procedures should be updated as required based on changing needs of the IU.

- Following the resolution of a Security Incident, the HIPAA Security Officer shall provide direct technical assistance to the IU, advise vendors of the weaknesses to assist them with the resolution of product-related problems, and provide liaisons to legal and criminal investigative groups, as needed.

- Document the information and outcome of each Security Incident, and retain for at least six (6) years. Use the attached Security Incident Report Form for this purpose.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

SECURITY INCIDENT RESPONSE OUTCOME

Responsible Incident Response Team Representative: _____
Date of this Outcome Report: _____

1. Assessment of Security Incident(s): _____

2. Source(s) of Assessment (e.g., report form; interviews; consultants feedback): _____

3. Actions Taken: _____

4. If Law Enforcement was notified, document the identity of the law enforcement official: _____

   Name: _____ Title: _____
   Precinct: _____ Phone #: _____

5. Outcome: _____

Note: Confidentiality is to be strictly observed except where report disclosure is determined to be required for further action and resolution.

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **CONTINGENCY PLANS**

Date Adopted: **February 12, 2014**

Policy:

The IU maintains a contingency plan for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure or natural disaster) that can damage systems containing e-PHI.

An established and implemented "Data Backup Plan" provides a plan by which retrievable exact copies of e-PHI are created and maintained. (Required). An established and implemented "Disaster Recovery Plan" provides for a mechanism by which lost data may be restored. (Required).

An established "Emergency Mode Operation Plan(s)" enables the continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode. (Required).

"Reasonable and appropriate" periodic testing of contingency plans are conducted and related procedures will be revised accordingly. (Addressable). "Reasonable and appropriate" periodic assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components will be conducted. (Addressable).

Procedures:

Applications and Data Criticality Analysis

- Identify the activities and materials that are critical to daily business operations.
- Identify the automated processes that support the critical services or operations (e.g., hardware, software, power supply, and IT personnel).
- Determine the amount of time the IU can tolerate power outages, disruption of services and/or loss of capability.
- Identify the practical and feasible preventive measures for each defined scenario that could result in loss of a critical service operation.
- Establish cost-effective and timely strategies for recovering the identified critical services, data or processes.

Data Backup and Disaster Recovery Plan

- Develop and implement a "Data Backup Plan" to provide for the creation and maintenance of retrievable exact copies of all e-PHI. (See attached sample.)
- Backed up e-PHI shall be retrievable in accordance with the Data Backup Plan.

- Develop and implement a "Disaster Recovery Plan" to providing for the restoration of any data lost as a result of a system "interruption" (e.g., fire, vandalism, natural disaster, system failure). (See attached sample.)

Emergency Mode Operation Plan

- Develop and document one or more Emergency Mode Operation Plan(s) (or "EMOPS") in the event of an emergency (e.g., system failure, blackout, fire, vandalism, natural disaster) to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode.

- An EMOP should be activated when an emergency that may impact critical business processes is reasonably anticipated, as well as during an actual emergency. The determination to activate an EMOP can be made by [employee/supervisor] of the IU who believes that such action shall protect the security of e-PHI. In the event of uncertainty as to whether a EMOP should be activated, the HIPAA Security Officer and HIPAA Privacy Officer should be contacted.

- An emergency call list shall be made available to all employees of the IU.

- Personnel and/or individuals that must be provided access to the e-PHI of the IU in the event of an emergency or a disaster shall be listed in the EMOP.

- Ensure that all appropriate agreements are in place with outside vendors key to the disaster recovery plan.

- Train all appropriate employees as to their responsibilities in each EMOP.

Testing and Revision of Procedures

- Test all procedures at least annually. Testing should be conducted in accordance with the testing procedures outlined in the respective EMOP and documented. If possible, outside vendors will be involved in testing exercises. If it is not "reasonable and appropriate" to conduct periodic testing of contingency plans and revise related procedures accordingly, document the reasons why and a reasonable alternative (See attached form).

- Assess the relative criticality of specific applications and data in support of other contingency plans. Consider the following components: (1) network architecture diagrams and system flowcharts showing structure, equipment and system interdependencies; (2) critical business processes and their associated outage tolerance; (3) key applications and systems used to support critical business processes; (4) other:_____

- Maintain a list of key applications and systems and their recovery time objectives. If it is not "reasonable and appropriate" to conduct periodic assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components, document the reasons why and a reasonable alternative. (See attached form).

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Documentation Requirement for
"Addressable" Implementation Standards:

1. ***Periodic Testing Of and Revisions To Contingency Plans***

(a) It is not "reasonable and appropriate" to conduct periodic testing of contingency plans and revise related procedures accordingly because: _____

The IU shall use the following reasonable alternative to periodic testing of contingency plans and revision of procedures: _____

(b) **If** is not "reasonable and appropriate" to conduct periodic testing of contingency plans and revise related procedures accordingly and there are no reasonable alternatives, the reasons why are: _____

2. ***Periodic Assessment & Analysis of Relative Criticality of Specific Applications & Data***

(a) It is not "reasonable and appropriate" to conduct periodic assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components because: _____

The IU shall use the following reasonable alternative to conduct periodic assessment and analysis of the relative criticality of specific applications and data: _____

(b) **If** is not "reasonable and appropriate" to conduct periodic assessment and analysis of the relative criticality of specific applications and data in support of other contingency plan components and there are no reasonable alternatives, the reasons why are: _____

DATA BACKUP PLAN

Type of e-PHI	Location of e-PHI	Data Backup Strategy or Mechanism Utilized	How Backed up e-PHI is Retrieved

DISASTER RECOVERY PLAN

Type of e-PHI	Location of e-PHI	Data Backup Strategy or Mechanism Utilized	How to Restore Lost e-PHI

TESTING PROCEDURES

1. Determine whether it is feasible to actually take down functions/services for the purposes of testing.

2. Determine whether testing should be done during normal business hours or during off hours.

3. If a real operational scenario shall be staged, including actual restoration of primary data lost, make key decision regarding how the testing will occur. Designate a team of individuals to conduct the testing or involve external entities (vendors, alternative site/service providers) in testing exercises).

4. "Tabletop" exercises will be conducted in lieu of real operational scenarios when real scenario testing would not reasonable.

This Disaster Recovery Plan was last tested on: _____

Coordinator who manages, maintains and updates this Disaster Recovery Plan is: _____

LANCASTER-LEBANON INTERMEDIATE UNIT NO. 13
PROVIDER HIPAA COMPLIANCE PROGRAM:
SECURITY POLICIES & PROCEDURES

Category: ***Administrative Safeguards***

Topic: **EVALUATIONS**

Date Adopted: **February 12, 2014**

Policy:

The IU performs regular periodic technical and non-technical evaluations, using standards implemented under the Security Rule and standards adopted in response to environmental or operational changes affecting the security of the e-PHI, to determine the extent to which its operations meet implemented HIPAA Security policies and procedures and the HIPAA Security Rule.

Procedures:

- Arrange periodic evaluations and determine whether internal staff resources or external consultants should be engaged to conduct such. Internal resources shall be used to supplement external resources when the knowledge maintained by the internal resources is unique.

- To the extent possible, evaluation strategies that have substance and can be tracked (e.g., questionnaires, checklists, audits) shall be used. The evaluations shall be distributed to all department identified by the HIPAA Security Officer. The evaluations may also be effected through the use of interviews, output of automated tools (e.g., access control auditing tools, system logs, penetration testing). These tools shall be maintained by the HIPAA Security Officer for six (6) years.

- The data from the evaluations shall be used to create a report on the level of compliance or effectiveness of a security safeguard. The results of the evaluation shall be analyzed and provided to the other top level administration at the IU, including compliance staff. Security weaknesses shall be identified, documented and addressed in a priority plan.

- Evaluations shall take into account prior reports or documentation and should incorporate, as may be appropriate, follow-up questions relating to prior weak areas.