UNION HOSPITAL

Policy Number:	HIPAA-106
Effective Date:	04/2005

Hospital Policies and Procedures

HIPAA Security Oversight

Developed / Edited By:	Robin Emrick, Anne Lara	Date:	01/2015
Reviewed By:	HIM Committee	Date:	02/2015
Approved By:	Laurie Beyer, CFO	Date:	02/2015
		Established Date:	04/2005
Departments Affected:	All		
Reviewed Dates:	08/2012, 02/2012		
Revised Dates:	01/01/2015, 08/2012, 02/2012, 02/2015		
TJC Standard(s):			
HIPAA Standard(s):	164.308(a)(1)(ii)(c), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(5), 164.316(a-b)		

PURPOSE:

To provide for the appropriate development, implementation, and oversight of Union Hospital's efforts toward compliance of the HIPAA security regulations

POLICY:

In accordance with the standards set forth in the HIPAA Security Rule, Union Hospital is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (e-PHI) it creates, receives, maintains, and/or transmits. Union Hospital has a HIPAA Security Officer [164.308(a)(2)] responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward HIPAA security compliance [164.316(a-b)].

Responsible for Implementation:
Administration and HIPAA Security Officer

Applicable To:
HIPAA Security Officer, leadership, workforce members, and others as assigned

Key Definitions:
Electronic Protected Health Information (e-PHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information that identifies an individual, or

provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Workforce: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Procedures:

1) **HIPAA Security Officer Responsibilities**. The HIPAA Security Officer, in collaboration with the HIPAA Privacy Officer (if not held by the same individual), is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Union Hospital's efforts to be compliant with the HIPAA Security Regulations. The intent of all oversight activities includes those necessary to maintain the confidentiality, integrity, and availability of e-PHI. These responsibilities are included in the HIPAA Privacy/Security Officer's job description (see Compliance and Privacy Practices) and include, but are not limited to the following:
   a) Oversees and enforces all activities necessary to comply with the Security rule and verifies the activities are in alignment with the requirements.
   b) Establishes and maintains written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.
   c) Updates policies and procedures as necessary and appropriate to comply with the Security rule and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.
   d) Facilitates audits to validate Security compliance efforts throughout the organization.
   e) Documents all activities and assessments completed to comply with the Security rule and maintain it for six years from the date of creation or date it was last in effect, whichever is later.
   f) Provides copies of the policies and procedures to management, and has them available to review by all other workforce members to which they apply.
   g) Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security of e-PHI.
   h) Reviews annual training for all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions
   i) Develops and provides periodic security updates to the Affinity Health Institute for reminder communications for all workforce members.
   j) Implements procedures for the authorization and/or supervision of workforce members who work with e-PHI or in locations where it may be accessed.
   k) Maintains a program promoting workforce members to report non-compliance with established Security rule policies and procedures. (See Occurrence Reporting Process AG-240)
      i) Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
      ii) Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Union Hospital.

iii) Mitigates to the extent practicable, any harmful effect known to Union Hospital of a use or disclosure of e-PHI in violation of Union Hospital's policies and procedures or business associates.

l) Reports security efforts and incidents to administration in a timely manner.

m) Assists in the administration and oversight of business associate agreements.

2) **Workforce Training**.

a) The HIPAA Security Officer facilitates the training of all workforce members as follows:

i) Supplies to Human Resources necessary materials for New Employee Orientation

ii) Supplies to the Affinity Health Institute department the material for annual competency training.

iii) Notification to workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective.

b) Ensure that workforce members sign into the training session.

c) Ensures that Human Resources and/or department manager retains documentation of the training session materials and attendees for a minimum of six years.

d) The training session focuses on, but is not limited to, the following subjects defined in Union Hospital's security policies and procedures (such as the System Access policy and Communication of PHI policy):

i) Auditing. Union Hospital may monitor access and activities of all users

ii) Workstations may only be used to perform assigned job responsibilities

iii) Users may not download software onto Union Hospital's workstations and/or systems without prior approval from the HIPAA Security Officer

iv) Users are required to report malicious software to the HIPAA Security Officer immediately

v) Users are required to report unauthorized attempts, uses of, and theft of Union Hospital's systems and/or workstations

vi) Users are required to report unauthorized access to facilities

vii) Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation)

viii) Users may not alter e-PHI maintained in a database, unless authorized to do so as a part of their job responsibilities

ix) Users are required to understand their role in Union Hospital's contingency plan

x) Users may not share their user names nor passwords with anyone

xi) Requirements for users to create and change passwords

xii) Users must set all applications that contain or transmit e-PHI to automatically log off after 10 minutes of inactivity.

xiii) Managers are required to report terminations of workforce members and other outside users.

xiv) Managers are required to report a change in a user's title, role, department, and/or location

xv) Procedures to dispose of discs, cd, hard drives, and other media containing e-PHI.

xvi) Procedures to re-use electronic media containing e-PHI.

xvii) Email encryption procedures

e) The HIPAA Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:

i) Latest malicious software or virus alerts

ii) Union Hospital's requirement to report unauthorized attempts to access e-PHI

iii) Changes in creating or changing passwords

f) Additional training is provided to workforce members in the information services department. This training is specific in nature, as to the Union Hospital's requirements for their involvement in areas such as the following:

i) Data backup plans
ii) System auditing procedures
iii) Redundancy procedures
iv) Contingency plans
v) Virus protection
vi) Patch management
vii) Media Disposal and/or Re-use
viii) Documentation requirements

3) **Supervision of Workforce**. Although the HIPAA Security Officer is responsible for implementing and overseeing all activities related to compliance with the Security rule, it is the responsibility of all leaders (i.e. team leaders, supervisors, managers, directors, etc.) to supervise all workforce members and any other user of Union Hospital's systems, applications, servers, workstations, etc. that contain e-PHI.

a) Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
b) Leaders assist the HIPAA Security Officer to ensure appropriate role-based access is provided to all users.
c) Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Union Hospital's security policies and procedures.

4) **Sanctions**. All workforce members and other users report non-compliance of Union Hospital's policies and procedures to the HIPAA Security Officer or other individual as assigned by the HIPAA Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence. (Refer to HR-323 Anti-Retaliation Policy and Compliance and Privacy Practices for additional information).

a) The HIPAA Security Officer promptly facilitates a thorough investigation of all reported violations of Union Hospital's security policies and procedures. The HIPAA Security Officer may request the assistance from others such as Human Resources, the workforce member's or users' leader, other workforce members, and/or other users.
   i) Complete an audit trail/log to identify and verify the violation and sequence of events.
   ii) Interview any individual that may be aware of or involved in the incident.
      (1) All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
      (2) Provide individuals suspected of non-compliance of the Security rule and/or Union Hospital's policies and procedures the opportunity to explain their actions.
   iii) The investigators thoroughly documents the investigation is as the investigation occurs.
b) Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations. Refer to Union Hospital's Constructive Discipline Policy.
   i) The table below describes the sanctions that will be applied based on access offense:

Access Offense	First Offense	Second Offense
Personal Record	24 working hours suspension without pay	Termination
Other Access (e.g. family member, unassociated patient, employee, minor and emancipated)	Written warning and 24 working hours suspension without pay	Termination

ii) Union Hospital reserves the authority to depart from the guidelines when, in its sole discretion, the violation is especially egregious or reflects a pattern of inappropriate behavior.

c) The HIPAA Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
d) The HIPAA Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.