UNIVERSITY HOSPITAL
Newark, New Jersey

UNIVERSITY HOSPITAL POLICY

SUBJECT:	COMPLIANCE AND PRIVACY	**TITLE:**	BREACH NOTIFICATION POLICY		
CODING:	831-200-847	**ADOPTED:**	July 1, 2013	**AMENDED/ REVIEWED:**	

Purpose: To provide guidance for breach notification by covered entities when improper or unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

Background:

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media.

Definitions:

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

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of

the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means any impermissible use or disclosure of PHI that the Covered Entity (CE) or Business Associate (BA) cannot demonstrate through sufficient written documentation poses a low probability that the PHI was compromised.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. Any inadvertent disclosure by a person who s authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

3. A disclosure of PHI where CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Covered Entity (CE): A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Organization: For the purposes of this policy, the term "organization" shall mean the CE to which this Policy and breach notification applies.

Protected Health Information (PHI): means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information: PHI that is not rendered **unusable, unreadable, or indecipherable to unauthorized individuals through the use of** technology or methodology specified by the Secretary in the 13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
    A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
    B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Security Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation; 800-77, Guide to IPsec VPNs; or 800-133, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
    A. Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
    B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce: Workforce mean 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 CE.

Policy Statements:

1. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to University Hospital, or, by existing reasonable diligence would have been known to University Hospital (includes breaches by the organization's business associates). University Hospital shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of University Hospital. Following the discovery of a potential breach, the breach shall be reported to the Chief Compliance and Privacy Officer for University Hospital to coordinate an investigation with the University Hospital Compliance Investigator, and conduct a risk assessment, where based on the results of the risk assessment, can begin the process of notifying each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach. The Chief Compliance and Privacy Officer shall also begin the process of determining what external notifications are required or should be made (e.g. Secretary of Department of Health and Human Services (HHS), media outlets, law enforcement officials, etc.).

2. Breach Investigation: The Chief Compliance and Privacy Officer for University Hospital shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordination of the response in conjunction with the requisite University Hospital entities. All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS Secretary under breach notification requirements, University Hospital will perform a risk assessment to determine if there is a low probability that the PHI has been compromised. The University Hospital Chief Compliance and Privacy Officer shall document the risk assessment as part of the investigation in the direct intake report form noting the outcome of the risk assessment process. The Chief Compliance and Privacy Officer has the burden of proof to demonstrate that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, University Hospital's Chief Compliance and Privacy Officer will determine the need to move forward with the breach notification. The risk assessment and the supporting documentation shall be fact specific and address:
    A. The nature and extent of the protected health information involved including the type and amount of PHI disclosed.

B. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
C. Whether the protected health information was actually acquired or viewed.
D. The extent to which the risk to the PHI has been mitigated.

4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the CE involved or the business associate involved. It is the responsibility of the CE to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the CE that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the CE shall:
    A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
    B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
    A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    B. A description of the types of unsecured PHI involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, diagnosis, disability code or other types of information).
    C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
    D. A brief description of what the CE is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
    E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

7. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

A. Notice to Individual (s): Notice shall be provided promptly and in the following form:

1. Written notification by certified mail to the individual at the last known address of the individual. The notification shall be provided in one or more mailings as information is available. If the CE knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by certified mail to the next of kin or person representative shall be carried out.

2. Substitute Notice: In the case of insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

    a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
    b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the CE's website, or a conspicuous notice in a major print or broadcast media in the CE's geographic area where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

3. If University Hospital's Chief Compliance and Privacy Officer determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying Covered Entities involved in all breaches in which the **unsecured** PHI of more than 500 patients is accessed, acquired, used, or disclosed.
   1. For breaches involving 500 or more individuals, the CE shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
   2. For breaches involving less than 500 individuals, the CE will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (Logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

8. Maintenance of Breach Information Database/Log: As described above and in addition to the reports created for each incident, University Hospital's Chief Compliance and Privacy Officer shall maintain a log of all breaches of unsecured PHI by entering those incidences into the University Hospital Accounting Disclosure Database regardless of the number of patients affected. The following information should be collected for each breach.

   A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
   B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
   C. A description of the action taken with regard to notification of patients regarding the breach.
   D. Resolution steps taken to mitigate the breach and prevent future occurrences.

Business Associate Responsibilities: The Business Associate (BA) of University Hospital that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, notify, in writing, the CE when the BA discovers a breach of unsecured PHI. A breach is deemed to have been discovered by a BA as of the first day on which the BA (by its employee, officer, or other agent, other than the person committing the breach), knows or would have known of such breach by exercising reasonable diligence. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide University Hospital with any other available information that University Hospital is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available.

9. Employee Training: University Hospital shall train all employees on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Employees shall also be trained as to how to identify and report breaches within the organization.

10. Complaints: Privacy complaints concerning patient privacy policies and procedures or compliance with such policies and procedures should be reported immediately to the Ethics Helpline at 1-800-215-9664 or directly to the University Hospital's Chief Compliance and Privacy Officer. Individuals have the right to complain about the organization's breach notification processes without adverse employment actions being taken against them.

11. Sanctions: University Hospital shall apply appropriate sanctions against employees who fail to comply with patient protected health information privacy and security policies and procedures.

12. Retaliation/Waiver: University Hospital shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. University Hospital shall not require individuals to waive their privacy rights under or as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Applicable Federal/State Regulations:

- ARRA Title XIII Section 13402 – Notification in the Case of Breach
- FTC Breach Notification Rules – 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules

APPROVALS BY:	NAME:	SIGNATURE:
President/CEO	James R. Gonzalez	
Interim Chief Compliance and Audit Officer	John W. Ras	
General Counsel	Paul Wermuth	
Director of Health Information Management	Irene Szczech	