Adirondack Health Institute

Collaboration Catalyst Community

POLICY AND PROCEDURE

Title: Breach Notification Policy

Department: Compliance

Effective Date: 9/2016

Annual Review Date: 9/2017

Date Revised:

Policy

It is the policy of Adirondack Health Institute (AHI), to establish the processes and procedures for the workforce members responsible for assessing and responding to a confirmed or suspected breach that occurs within AHI's facilities or database of client/patient protected health information ("PHI").

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, for individuals whose unsecured PHI has been accessed, acquired, or disclosed as a result of a privacy or security breach, if AHI determines that a breach poses a risk of financial, reputation or other compromise.

Definitions

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

Breach: 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 poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at 45 CFR §164.514(e)(2) of HIPAA Privacy Rule, limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

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 is 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 a 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: A health plan, health care clearinghouse, or a health care 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: That 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 or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; 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 covered entity to which the policy and breach notification apply.

Personally Identifiable Information (PII): any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. One example is a person's Social Security Number.

Protected Health Information (PHI): Protected health information 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: 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 guidance issued under section 13402(h)(2) of Pub. L.111-5 on the Department of Health and Human Services (HHS) website.

1. Encryption Guidelines:

   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 Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

2. Media Destruction:

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 Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce: Workforce means employees, board members, volunteers, trainees, interns, vendors, independent contractors 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.

Procedure

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 the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization's business associates). The organization 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 the organization. Following the discovery of a potential breach, the Compliance Officer (CO) and/or their designee shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been, accessed, acquired, used, or disclosed as a result of the breach. The CO will determine 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 Compliance Officer, and/or designee, will act as the investigator of the breach. The investigator(s) shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordination with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, communications, legal counsel, etc.) The investigator(s) shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained in the Compliance Department for a minimum of six years.

3. ***Risk Assessment to Determine Probability of Compromise:*** Upon the discovery of a breach, the Compliance Department will undertake a fact specific assessment as to whether the unauthorized acquisition, access, use, or disclosure of unsecured PHI compromises the security or privacy of the information. This assessment will determine whether the breach poses a significant risk of financial, reputation or other the harm to the affected patient/client. It includes the following considerations:

    - Was the PHI acquired or viewed?
    - Did the breach result from an impermissible use?
    - Who impermissibly used or disclosed the PHI?
    - To whom was the PHI impermissibly disclosed?
    - Is it possible to obtain the recipient's assurances that the PHI will not be further used or disclosed, or will be destroyed?
    - Was the PHI returned prior to it being accessed for an improper purpose?
    - What is the nature and extent of the PHI at issue?
    - To what extent has the risk to the PHI has been mitigated?

    The Compliance Department will maintain documentation of this assessment for each breach discovered. If the Compliance Department determines that the risk posed by the breach is more than a low probability of compromise, the patient/client will be notified.

Notification Procedures

1. ***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 organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

2. ***Notice to Individuals:*** Within sixty (60) days of discovery of a breach, AHI must provide notice via first class mail to the affected person's last known address. In the case of a minor or someone who otherwise lacks legal capacity, notice will be sent to the person's parent or personal representative if known. For known decedents, notice will be sent to either the next of kin or personal representative.

The notice must include:

(A) A description of what happened, the date of the breach and the date of the breach's discovery (if known);

(B) A description of the types of unsecured information involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(C) The steps a person should take to protect himself or herself from the potential harm resulting from the breach;

(D) A description of AHI's efforts to investigate the breach, to mitigate the harm to individuals and to protect against future breaches; and

(E) Contact procedures for individuals to ask questions including AHI's toll free telephone number, an email address, a website or postal address.

If AHI does not have sufficient contact information for an individual or if ten (10) or less notices are returned as undeliverable, a substitute notice such as an email or telephone call will be provided. If more than ten (10) notices are returned, notice will be posted on the AHI website home page for ninety (90) days.

A log of these notifications will be kept and maintained for six (6) years.

3. ***Notice to Local Media*:** Any case in which 500 or more persons who are residents of the same state are affected by a breach, AHI must provide notice to major local media outlets within sixty (60) days of discovery.

4. ***Notice Required to HHS:*** AHI is required to disclose all breaches to the Department of Health and Human Services ("HHS"). Notice of breaches affecting 500 or more individuals must be made to HHS concurrently to the notices provided to affected persons. Breaches affecting fewer than 500 individuals must be reported annually to HHS. This report will be sent within sixty (60) days after the end of the calendar year.

5. ***Notice Required to NYS:*** AHI is required to disclose any unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of private information to the New York State Attorney General as per the NYS Information Security Breach and Notification Act; New York Attorney General Security Breach Notification Guidance available at: http://www.ag.ny.gove/consumer-frauds/new-yor-state-information-security=breach-and-notification-act.

6. ***Delay of Notification Authorized for Law Enforcement Purposes:*** If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, AHI 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.

7. ***Maintenance of Breach Information/Log:*** As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged 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/clients 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/clients regarding the breach.

   D. Resolution steps taken to mitigate the breach and prevent future occurrences.

8. ***Business Associate Responsibilities:*** The business associate (BA) of AHI that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. 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 AHI with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, AHI will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals.

Policy Compliance

Workforce members who discover a breach should report the breach immediately to the Compliance Department either by phone at 518-480-0111 x109 or by email at ahicompliance@ahihealth.org. Any incident reported in good-faith is protected under AHI's whistleblower policy.

The Compliance Department will verify compliance to this policy through various methods, including but not limited to, internal and external audits or any other necessary means of investigation.

POLICY AND PROCEDURE

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or services. In cases where local, state, or federal laws have been violated, workforce members may also face prosecution.

Distribution

Upon final approval, all policies are emailed to staff and are then made available for future access through placement on the AHI server [z drive] in the All Employees Policies and Procedure folder.

All recipients of this policy must acknowledge their receipt and understanding of the policy by referring any questions or problems with the policy within ten (10) days of the issue date to the Compliance Department. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

Contact Person: Corporate Compliance Coordinator

Responsible Person: Compliance Officer

Approved by: CEO/Board of Directors