Privacy Policy - HIPAA Incident Response and Reporting and Breach Determination

Policy Purpose

Organization takes the privacy, security and integrity of individuals' data seriously. Organization also has legal responsibilities to protect PHI under HIPAA, to identify and respond to suspected incidents, mitigate harm, require its workforce members to report incidents, and to determine when there is a reportable breach of an individual's PHI.

The purpose of this Incident Response and Reporting and Breach Determination Policy is to meet Organization's responsibilities and to provide guidance to Organization workforce members regarding recognizing and reporting a privacy or security incident involving Member health information. Organization will review all reported incidents and will follow the procedures set forth to determine if there has been a breach (an acquisition, access, use, or disclosure of the Member's unsecured PHI in a manner not permitted under HIPAA).

Policy

This policy establishes guidelines for Organization to:

- Require the reporting of suspected privacy and security incidents (any attempted or successful unpermitted or unauthorized access, use, disclosure, modification, interference or destruction of unsecured PHI in any form). All workforce members must report any suspected incident to the Compliance, Privacy or Security Officer as soon as possible, and may report anonymously through The Guard if preferred. Workforce members who fail to promptly report incidents will be subject to discipline. See Privacy Policy - Sanctions/Discipline for additional details;
- Identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Organization will handle any complaint that is potentially a privacy or security incident under this policy, or any similar Security policy, instead of Privacy Policy - Complaints to the Organization;
- Determine if there has been a breach of unsecured PHI ("PHI") after analyzing potential exceptions and performing a risk analysis or requiring any involved business associate to do so and then reviewing their determination; and
- Document the incidents, responses and breach determinations and retain the documentation for at least six years.

Procedures

Reporting of Security Incidents

Organization will train all workforce members on HIPAA privacy and security requirements. All Organization workforce members must report to their supervisor and/or Organization's Compliance, Privacy Officer or Security Officer as soon as possible and in no event later than 24 hours after discovering any suspected, known, or potential privacy or security incident. Supervisors must notify the Privacy and Security Officers immediately upon notification of potential, known or suspected Incidents. Organization workforce members are subject to discipline for failure to promptly report any suspected, known, or potential breach of unsecured PHI.

Organization will require business associates to report privacy and security incidents promptly and will enforce contract requirements.

Monitoring for Privacy and Security Incidents

Organization shall employ tools and techniques to monitor events, detect attacks and provide identification of unauthorized use of the systems that contain electronic protected health information (*ePHI*) and also periodically review access, integrity, use and disclosure of all PHI, in whatever form, to identify any potential breaches.

Treatment of Recurring and Expected Unsuccessful HIPAA incidents

Organization acknowledges the ongoing existence or occurrence of attempted but "*unsuccessful security incidents*" including but not limited to, pings, and other broadcast attacks on firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above. As long as no such unsuccessful security incident results in unauthorized access, use or disclosure, inappropriate denial of access or harm to the integrity of ePHI, they will be reviewed, and the reports kept but Organization will not undertake a full factual investigation or breach determination analysis for each such unsuccessful attempt. Unsuccessful security incidents will also be reviewed for heightened frequency and considered in the development, implementation of and improvements to safeguards. Organization will perform a thorough analysis of any suspicious circumstances or unusual activity found during reviews.

Perform and Document a Factual Investigation of the Incident

Organization will perform a factual investigation of any reported potential privacy or security incident. At a minimum, Organization will seek information and documentation sufficient to

- perform an analysis of whether there was any attempted or successful *unauthorized access*, use, disclosure, modification, or destruction of information in any form
- determine if any unsecured information was involved
- determine if any *PHI* was involved
- determine if any exception to an assumption of a *Breach* of *PHI* exists
- perform the risk of *PHI* compromise analysis and
- determine the number of *individual*s impacted.

If Organization has a separate investigations policy, it will follow that policy. Organization may retain outside resources for the completion of some or all of the investigation, especially if a forensic investigation is desirable.

Should the Privacy or Security incident occur through a business associate, Organization may rely on the Business associate to conduct an investigation but may also conduct an independent investigation if it so chooses. Organization must review the Business associate's findings and underlying facts prior to deciding on whether or not to rely solely on the Business associate's investigation or to perform its own investigation.

Determine Need and Implement Reasonable Mitigation Measures

Following the report or discovery of any HIPAA incident, Organization will assess whether any immediate or future safeguards or changes to process or practice are required to address the incident or its potential reoccurrence. Organization should determine whether to involve law enforcement on a case-by-case basis. For mitigations specific to security incidents, please refer to Security Policy for examples.

Determine if There Was Any Attempted or Successful Unauthorized Access, Use, Disclosure, Modification, or Destruction of Information in Any Form

Following a standard procedure and utilizing the HIPAA Breach Risk Assessment Record and Unsecured PHI Job Aid or similar documentation when applicable, Organization will determine whether

1. there was any attempted or successful access, use, disclosure, modification or destruction of information,
2. whether the information involved was unsecured,
3. whether such information was PHI or ePHI,
4. whether such access, use, disclosure, modification, or destruction was unauthorized or unpermitted and
5. whether any of the exceptions to a determination of a breach applies.

Organization will first use the Unsecured PHI Job Aid or a similar standard assessment tool to decide if any information involved in the incident was unsecured. Organization will then determine if the information involved in the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information was PHI. For example, if the information involved a deceased individual, Organization will establish if the individual been deceased for more than fifty years.

Next, Organization will determine if access, use, disclosure, modification, or destruction was unauthorized or unpermitted by establishing if the use or disclosure was authorized or permitted under HIPAA. For example, Organization will analyze if it was authorized by the individual, required by law, or permitted as incidental. Finally, the Organization will analyze if there is an exception to concluding a breach occured by determining if an exception applies.

Determine if there is an Applicable Exception to a Breach Determination

As part of its breach determination, Organization will review the three exceptions to the definition of *breach* published in 45 CFR § 164.402 to analyze whether an exception applies to the specific fact pattern of each privacy or security incident. Organization will determine and record its determination as to whether any of these three exceptions applies to the incident:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, 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 subpart E of this part (Subpart E sets forth allowable uses of PHI). An example of when this exception applies: someone at a business associate was looking for a record they needed to perform their responsibility, they inadvertently accessed Mary B's record instead of Mary A's record and they did not further disclose information from Mary B's record.
2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information *at the same covered entity or business associate, or organized health care arrangement* in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part (Subpart E sets forth allowable uses of PHI). An example of when this exception applies: Dr. Brown requests an individual's record to perform his job responsibilities, Mary delivered the record to Dr. Black instead. So long as all of them work at the same CE, BA or within an organized health care arrangement and Dr. Black did not further disclose the information, there is no breach.
3. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. Example of this exception: a nurse hands the wrong discharge papers to a patient and notices the error right away, taking back the papers before the patient could read them.

If an exception applies, Organization will record its findings in the incident record and the incident can be closed. If no exception applies, there is a presumption that a breach has occurred. Organization may either perform a risk analysis according to the procedure set forth below or forego performing that analysis and follow the process for notifications under Privacy Policy - Breach Notification.

Perform an Analysis of Risk of Compromise to Unsecured PHI Utilizing the Four Required Factors and Other Pertinent Information

If Organization has determined that there is a presumption of a breach, Organization has the option of performing a risk of compromise assessment. If choosing to make this assessment, Organization will use at least the following four required factors to determine if there is a low probability that PHI has been compromised that rebuts the presumption of a breach:

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

Organization may also consider other factors in its analysis that might support a finding of a low probability of risk including but not limited to the time the information may have been accessible or accessed, the likelihood the information was accessed, whether any complaints were received, how difficult or likely access was even if there was accessibility and any professional or legal requirements applicable to the person who received the information (does a legal privilege apply, was the person who received the information in healthcare and trained on HIPAA privacy requirements). The HIPAA Incident Assessment Tool may be useful in completing and documenting the risk of compromise assessment.

If the Breach occurred through a business associate, Organization may rely on a business associate to perform the risk of compromise assessment but must review the findings and underlying facts prior to deciding on whether to perform its own assessment.

Record Keeping

Organization will create and maintain a HIPAA incident log for all reported incidents, regardless of whether they are determined to be Breaches. Organization shall review this log periodically to determine areas that may require additional training. Organization will keep records concerning all reports of security or privacy incidents, any finding of an exception to the Breach definition, all analyses of risk of compromise to unsecured PHI, and the factual investigations and documentation supporting the analysis and findings. These records will be kept for a minimum of six years following the conclusion of the Breach determination for the incident(s). Where Organization has found an applicable exception to a Breach or made a finding of a low probability of compromise to PHI, Organization's records must sufficiently demonstrate the application of any exception or support a finding that there is a low probability of compromise to the PHI.

Enforcement and Reporting

Organization's Compliance Officer and Organization's *HIPAA* Privacy and Security Officers or their designees, along with human resources, are responsible for managing, updating, and enforcing this policy. Violations of this policy must be immediately reported.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
- 45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
- 45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
- 45 CFR 402 *Definitions: Breach*