Subject: HIPAA Security Policies & Procedures **Policy #: ??-?**

Title: Response and Reporting **Page 1 of 10**

Effective Date of This Revision: February 4, 2010

Contact:	HIPAA Chief Security Officer "Insert Addressee Here" "Insert Street Address Here" "Insert Phone Number Here"	Responsible Department:

HIPAA REGULATORY INFORMATION: Integrity Standard

Category:	☐ Administrative Safeguard ☐ Physical Safeguard ☒ Technical Safeguard	**Type:**	☐ Standard ☒ Implementation Specification ☒ Required ☐ Addressable

Applies to:	☒ Officers ☒ Other agents	☒ Staff/ Faculty ☒ Visitors	☒ Student clinicians ☒ Contractors	☒ Volunteers

---

BACKGROUND:

The Health Insurance Portability and Accountability Act of 1996 *(HIPAA)* requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI *(ePHI)* data. According to the law, all "Covered Entity's Name" officers, employees and agents of units within a "Covered / Hybrid" Entity must preserve the integrity and the confidentiality of individually identifiable health information *(IIHI)* pertaining to each patient or client.

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

PURPOSE:

Each Unit of "Covered Entity's Name" health care component (HCC), which handles ePHI, will implement the ability to authenticate, which is the process used to validate data integrity, verify that the data sent is the same data that is received, and ensure the integrity of data stored and retrieved.
Who is affected by this policy is documented in Policies, Procedures, and Documentation policy ("Policy Number")

This policy provides guidance for *"Covered Entity's Name" 's Security Office* in adopting the Security Incident Procedures standard *[45 CFR 164§.308(a)(6)(i)]*.

POLICY:

Each Unit of "Covered Entity's Name" HCC responsible for ePHI will include, as appropriate, in its documented process for promptly identifying security incidents, the following:

- ☑ Risk analysis of ePHI Systems, as set forth in "Covered Entity's Name" 's Risk Analysis implementation specification ("Policy Number")
- ☑ On the basis of the risk analysis, identify what events constitute a security incident in the context of "Covered Entity's Name" 's operations.
- ☑ Process for identifying a security incident.

Each Unit of "Covered Entity's Name" HCC responsible for ePHI will organize a Security Incident Response Team (SIRT) primarily responsible for security incident reporting and response will perform an investigation when evidence shows that a security incident has occurred and will respond promptly to the security incident. Each Unit of "Covered Entity's Name" HCC responsible for ePHI will document its process for promptly responding to security incidents.

Each Unit of "Covered Entity's Name" HCC responsible for ePHI will include, as appropriate, in its documented process for promptly reporting security incidents, a procedure for "Covered Entity's Name" 's workforce members to report a security incident to the appropriate identified management personnel.

A "Covered Entity's Name" workforce member will not prohibit or otherwise attempt to hinder or prevent another "Covered Entity's Name" workforce member from reporting a security incident to the SIRT and will cooperate fully with security incident investigations.

Each Unit of "Covered Entity's Name" HCC responsible for ePHI will include training and awareness for workforce members, as appropriate, in its documented process for promptly identifying, reporting, tracking, and responding to security incidents in accordance with "Covered Entity's Name" 's security policies and procedures.

ACTION:

General Requirements & Investigation:

1. It is the responsibility of all members of "Covered Entity's Name"'s workforce to report any security or privacy incidents or suspected security or privacy incidents to the "Covered Entity's Name" security officer or designee and the "Covered Entity's Name" privacy officer or designee as soon as the incident or suspected incident is discovered.
2. The PSIRT will be formed and appropriately trained and membership shall include the security officer, the privacy officer, "Covered Entity's Name" or designee, an information technology (IT) representative and legal counsel [*additional members may be assigned depending on the size and complexity of the organization*].
3. The PSIRT is responsible for investigating and mitigating any identified security or privacy incidents or suspected incidents. This includes investigation, mitigation, breach notification if appropriate, implementation or update of security and privacy controls and reporting findings and actions taken to "Covered Entity's Name" or designee in a timely manner.
4. PSIRT's responsibilities include:
    a. Respond to all security and/or privacy incidents or suspected incidents
    b. Convene within one hour of notification of a potential incident
    c. Identify affected critical systems, policies or practices
    d. Assess damage and scope of the incident
    e. Control and contain the breach/intrusion
    f. Collect and document all evidence relating to the incident according to established forensic procedures
    g. Contact additional support members as necessary for investigation of a given incident
    h. Confer with legal counsel to determine appropriate course of action regarding notification, if appropriate, of patients, law enforcement, etc.
    i. Provide liaison to proper criminal and legal authorities under the direction of "Covered Entity's Name" or designee
    j. Initiate breach notification, if appropriate
    k. Contact communications officer and provide details of the incident and PSIRT's response
    l. Implement new or strengthen existing privacy and security controls to prevent a future like incident
    m. Document the investigation, mitigation and future prevention activities

5. Security or privacy incidents can arise at any time of day and on any day of the week. Often attacks happen during non-business hours. In order to react swiftly to minimize damages at least one member of the PSIRT must be available 24 hours a day, seven days a week.
6. Each core PSIRT member must be on call to respond to an incident page immediately.
7. The PSIRT will be made up of:
    a. Security Officer (co-team lead)
    b. Privacy Officer (co-team lead)
    c. "Covered Entity's Name" or designee
    d. IT representative
    e. [*other members to be defined depending on the size and complexity of the organization*]
8. All security and privacy incidents will be reported to the PSIRT member on call. The PSIRT member on call will make a quick evaluation of the information available and determine whether PSIRT activation is warranted. If so PSIRT members will be paged.
9. PSIRT members will report to [*indicate location*] as soon as possible after the page is received, but within no longer than 60 minutes from the initial page.
10. If the PSIRT member is not physically able to join the team [*indicate location*], he/she shall call the PSIRT member on call and provide a number where he/she can be conferenced in to the initial problem assessment meeting.
11. At the time the incident is reported PSIRT members are required to:
    a. Determine if the incident warrants further investigation/action
    b. Categorize the security or privacy incident
    c. Determine what, if any, outside workforce members/managers should be called
    d. Make sure all proper procedures are followed for the investigation to reasonably ensure evidence and nature of the incident is preserved
    e. Document the investigative steps taken and evidence gathered
    f. Provide a detailed analysis of the incident to the security and privacy officers, if warranted, senior management
    g. Recommend further actions/sanctions
    h. Contact legal counsel if action considered criminal and/or needs to be reported to law enforcement
    i. Provide liaison with appropriate law enforcement agencies as appropriate and under the direction of the security and privacy officers
12. If management is called in their responsibilities include:
    a. Participate with PSIRT members in investigation and evidence gathering related to a reported incident
    b. Make recommendations to prevent future like incidents
13. Security and privacy incidents will be classified as follows:
    a. Class 1 incidents which require immediate SIRT activation
        i. Attacks against a firewall
        ii. Virus attacks
        iii. Internet abuse
        iv. Attacks against a server
        v. Attacks against any system containing PHI

vi. Inappropriate release of PHI
vii. Loss or theft of devices or media containing PHI
viii. Use of PHI for personal use (not related to required business activities) or gain

b. Class 2 incidents are those referred to PSIRT after investigation within a specific department or by IT representatives or another support group. The following require PSIRT review but may not be emergency situations and may be addressed by the PSIRT during normal business hours
   i. Suspected password misuse
   ii. Theft of property containing information assets (not including PHI)
   iii. Request from management to review activity of a particular member of the "Covered Entity's Name" workforce
   iv. Accidental release of PHI to an unauthorized party
   v. Fax of PHI to an incorrect number
   vi. Unintentional inappropriate access to PHI

14. Security and privacy incidents may be escalated depending on the nature of the incident. A class 2 incident can be raised to a class 1 incident in the following ways:
    a. The PSIRT co-team leaders (the security and privacy officers) determine, based on the initial investigation of a class 2 incident, that it is more widespread or severe than previously suspected
    b. At the request of "Covered Entity's Name" or designee
15. All reports regarding security or privacy incidents or suspected security or privacy incidents shall be retained for six years following the conclusion of the investigation.

Mitigation & Breach Notification:

In addition to the preceding, mitigation shall include patient breach notification as appropriate. If the patient's full name or first initial and last name along with any PHI, especially including the patient's social security number, drivers license number, passport number or credit card and PIN, are inappropriately disclosed, the patient will be notified of the breach [*Oregon Identity Theft Protection Act only requires notification if full name or first initial plus last name and social security number or drivers license number or passport number or credit card number and PIN are inappropriately disclosed; notification if any PHI is inappropriately disclosed is sound business practice, limits liability and assists in preserving the organization/Provider's reputation*].

It is the responsibility of the "Covered Entity's Name", designee or communications officer to initiate appropriate notification processes if deemed appropriate. Breach notification will not occur until the incident and the data breached is reviewed by legal counsel to determine if notification is required. Also, notification may be delayed if law enforcement is notified and law enforcement requests a delay in notification to assist with the investigation process.

Notification is not required if the breach included only data that was encrypted. Such data, whether at rest or in transit has been rendered unreadable by any unauthorized individuals or entities. See **Secure Transmission** policy. Also, notification is not required if the data inappropriately released is in a non-