Company Name or Logo[1]	Policy and Procedure
Title: Breach Notification	**P&P #:**
Approval Date: Date[4]	**Review:** Biannually
Effective Date: Date[5]	**Approval Signature:**

Purpose:

This policy establishes [PRACTICE NAME] framework for addressing a breach of unsecured protected health information (PHI) that occurs notwithstanding [PRACTICE NAME] recognition of the importance of information security and its reasonable efforts to prevent such a breach.

Scope:

This policy applies to all [PRACTICE NAME] workforce members.

Definitions:

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

Breach means the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. (For exceptions to the definition of breach, please consult 45 CFR § 164.402.)

Discovered means the first day on which the breach is known or would have been known to a [PRACTICE NAME] workforce member by exercising reasonable diligence.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Law enforcement official means an officer or employee of any agency or authority of the United States, a state or territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to:

a. Investigate or conduct an official inquiry into a potential violation of law; or
b. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Protected health information (PHI) generally means identifiable or potentially identifiable health information that is transmitted or maintained in electronic media or any other form or medium. (For the complete definition, please consult 45 CFR § 160.103).

Unsecured protected health information means PHI that is not secured through the use of a technology or methodology specified by the Secretary that renders the PHI unusable,

unreadable, or indecipherable to unauthorized individuals.

Policy:

1. **General**. [PRACTICE NAME] shall outline its process for evaluating and reporting known or suspected privacyviolations or security incidents. This process shall include a Key Contact List indicating to whom reports of such incidents should be made; who shouldbe involved in determining if a breach of unsecured PHI has occurred; and if affectedindividual(s) should be notified.

2. **Reporting incidents and complaints**

   a. [PRACTICE NAME] workforce members shall immediately report known or suspected privacy violations or security incidents to the [PRACTICE NAME] Compliance Officer and complete a ***Security Incident Report.***

   b. The HIPAA Compliance Officer may need to quickly decide on steps to contain or mitigate the potential spread or damage from the incident. For instance, deciding whether to isolate or remove the affected device from the network. Decide who needs to be contacted on the Key Contacts List.

   c. Upon receipt of a Security Incident Report, an investigation into the incident shall be initiated. The ***Security Incident Investigation Report*** should be completed as thoroughly as possible by the Incident Handler and Investigators.

   d. As soon as possible, but not later than forty-five (45) calendar days following discovery of an incident, the [PRACTICE NAME] Compliance Officer shall complete a risk assessment using the ***Risk Assessment Analysis Tool and/or Privacy Breach Assessment*** to determine the probability that PHI has been compromised and attach it to the report,. The risk assessment shall include:

      i. The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification.

         A. Was PHI involved ;

         B. Type of PHI;

         C. Does the incident meet the definition of breach; and

         D. Likelihood of re-identification.

      ii. The person who used the PHI or to whom the disclosure was made.

         A. Did the recipient have an obligation to protect the privacy and security of Pill;

         B. Was the acquisition, access, or use of PHI by a workforce member or person acting under the authority of [PRACTICE NAME];

         C. Was such acquisition, access, or use made in good faith;

         D. Does the recipient have the ability to re-identify the PHI;

         E. Was the acquisition , access, or use within the recipient 's scope of authority; and

         F. Did the acquisition, access, use, or disclosure result in further use or

disclosure in amanner **not** permitted by the Privacy Rule.

iii. A determination of whether the PHI was actually acquired or viewed, or rather, the opportunity to acquire or view existed, but was not acted upon.

A. Was the PHI encrypted using at least 128 bit encryption or destroyed by an acceptable method of destruction?

B. Following a forensic examination, did evidence establish that the information was not accessed?

iv. The extent to which the risk to the PHI has been mitigated.

A. A satisfactory assurance has been received from the recipient stating that the PHI hasor will not be further used or disclosed.

B. The efficiency of the mitigation effectively limited availability to the PHI;

C. Does an exception to the notification requirement exist; and

D. Do the affected individuals need to be notified?

e. Answers to the questions listed above may not always be available.

3. **Evaluating an incident or complaint.** The reporting obligation for [PRACTICE NAME] is triggered when a breach of unsecured PHI occurs. In order to have a breach of unsecured PHI, there must be **PHI + a violation of the HIPAA Privacy Rule + compromise of the privacy and security of the PHI + unsecured PHI + no exceptions**. Sections 3.a.-c. Below may be utilized to accurately evaluate a privacy incident or complaint.

a. PHI involved. Ifno PHI is involved, there is no breach of unsecured PHI and no obligation tonotify.

b. Violation of the Privacy Rule. If the [PRACTICE NAME] Compliance Officer determines that the violation compromises the privacy and the security of PHI, then the violation is a "breach."

c. Ability of [PRACTICE NAME] to mitigate the risk of harm. The risk of harm may depend upon the ability of [PRACTICE NAME] to mitigate the effects of the breach.

4. **Securing PHI through encryption or destruction.** [PRACTICE NAME] shall utilize one of the two following methods for "securing" PHI:

a. Encryption. [PRACTICE NAME] shall encrypt PHI using a NIST recommended algorithm and procedure. To comply with encryption standards and ensure the encryption keys are not obtained, [PRACTICE NAME] shall keep encryption keys on a separate device.

b. Destruction. Paper, film, or other hard copy media shall be shredded or destroyed in a mannerthat the PHI cannot be read or otherwise reconstructed.

5. **Law enforcement notification delay.** [PRACTICE NAME] may delay its notification to

affected individuals for a criminal investigation or for national security purposes.

a. If a law enforcement official informs [PRACTICE NAME] that notice to an individual, to the Secretary ofthe U.S. Department of Health and Human Services (DHHS), or to the media would impede acriminal investigation or cause damage to national security, [PRACTICE NAME] shall request that the lawenforcement official make an official written request that [PRACTICE NAME] delay such notification. The written request shall include:

   i. The law enforcement official's full name;

   ii. The law enforcement official's title and badge number;

   iii. The law enforcement organization's name;

   iv. The reason for the delay; and

   v. The proposed number of days to delay.

b. All oral requests for a notification delay shall be evaluated on a case by case basis and only granted in the most urgent and serious circumstances. If [PRACTICE NAME] receives an oral request, such request shall be documented.

6. Notification

a. If the [PRACTICE NAME] Compliance Officer determines a breach of unsecured PHI has occurred, the practice shall provide notice of the breach and maintain documentation of such notice.

b. Notice to the affected individual(s). Unless contrary instructions from law enforcement are received, a written notice of breach shall be provided to each affected individual whose unsecured PHI has been breached, or is reasonably believed to have been breached, as follows:

   i. Timing of notice. The notice shall be provided no later than sixty (60) calendar days after [PRACTICE NAME] discovers the breach. The breach is considered "discovered" on the first day a [PRACTICE NAME] workforce member or agent knows, or by exercising reasonable diligence, would have known, of the breach.

   ii. Manner of notice. The written notice shall be:

      A. Sent by first-class mail addressed to the affected individual's last known address;

         I. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn;

      B. Provided to the individual's personal representative, if the individual is deceased, andif [PRACTICE NAME] has the personal representative's address; or

      C. Provided in one or more mailings as additional information becomes available.

   iii. Content of notice. The notice shall be written in plain language and shall contain the following information:

      A A brief description of the incident, including the date of the breach and the

date of thediscovery of the breach, if known;

B. A description of the types of unsecured PHI involved in the breach;

C. Any steps the individual should take to protect him or herself from harm that couldresult from the breach;

D. A brief description of the steps [PRACTICE NAME] is taking to investigate the breach, to mitigate the harm to the individual , and to protect against future occurrences; and

E. Contact information, including a toll-free telephone number, an e-mail address, website, or postal address for the individual to ask questions or learn additional information.

iv. Substitute notice. If insufficient or out-of-date contact information for an individual precludes written notice to such individual, the [PRACTICE NAME] shall provide notice reasonably calculated to reach the individualas soon as reasonably possible after such determination, as described below.

A. If there is insufficient or out-of-date contact information for fewer than ten (10)

individuals, notice may be provided by e-mail, telephone, or other means.

B. If there is insufficient or out-of-date contact information for ten (10) or more individuals, notice shall:

I. Be in the form of either a conspicuous posting for ninety (90) calendar days on the [PRACTICE NAME] internet home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside; and

II. Include a toll-free number that remains active for at least ninety (90) calendar days so that the individual can learn whether his or her unsecured PHI was included in the breach.

C. Substitute notice need not be provided if the affected individual is deceased and the[PRACTICE NAME] has insufficient or out-of-date contact information for the next of kin or personal representative of the individual.

v. Urgent notice. If [PRACTICE NAME] determines that potential for imminent misuse of the unsecured PHI in connection with a breach exists, [PRACTICE NAME] may provide information regarding the breach to individuals by telephone or other means, as appropriate, in addition to providing the required written notice as describedabove.

c. Notice to DHHS. Unless contrary instructions from law enforcement are received, [PRACTICE NAME] shall notify DHHS of the breach of unsecured PHI. Such notification shall be provided as follows:

i. If the breach involves 500 or more individuals, [PRACTICE NAME] shall notify DHHS in a manner specified by DHHS on its website of the breach contemporaneously with providing the notice to the individual.

ii. If the breach involves less than 500 individuals, the [PRACTICE NAME] shall maintain a log or similar documentation of the breach of unsecured PHI and shall report the information specified by DHHS on its website no later than February 28 of the following year

d. Notice to media. Unless contrary instructions from law enforcement are received , and a breach involves more than 500 residents of one state or jurisdiction , the [PRACTICE NAME] shall notify prominent media outlets serving the state or jurisdiction in addition to notifying the individual and DHHS. Such notice shall be provided no later than sixty (60) calendar days after discovery of the breach. The notice shall contain the same information included in the notice to the individua1.

e. Communications with the media or outside agencies. With the exception of the [PRACTICE NAME] Compliance Officer, Public Information Officer, or designee, [PRACTICE NAME] workforce members are not authorized to speak on behalf of [PRACTICE NAME] to media personnel or representatives of other outside agencies concerning a breach.

f. Retention of breach notice documentation. The [PRACTICE NAME] shall record and maintain thorough records of all activities related to breaches of unsecured PHI, the provision of notice to individuals, DHHS, or the media, and communications from law enforcement related to delayed notification, if applicable, for at least six (6) years from the date the incident was closed or notice was provided, whichever date is the latest.

g. Reporting of incidents to [PRACTICE NAME] by its business associates

1. In the event of a breach of unsecured PHI, a [PRACTICE NAME] business associate (BA) is required to:

   A. Notify [PRACTICE NAME] no later than seven (7) business days following discovery of an incident involving [PRACTICE NAME] PHI. The BA shall provide to the [PRACTICE NAME] Compliance Officer the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been breached and any other available infornation that [PRACTICE NAME] is required to provide to the individual for further processing in accordance with this policy.

   B. Complete a riskassessment no later than seven (7) business days following discovery of an incident involving [PRACTICE NAME] PHI to determine whether there has in fact been a breach. If definite answers to all of the questions above are not available at the time the incident is reported, the BA shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from a breach is on [PRACTICE NAME] - not the BA. Therefore, a BA should not have the discretion to determine whether notification will occur.

2. [PRACTICE NAME] shall:

   A. Include appropriate language in all contracts with BAs to reflect the BA's responsibilities.

References:

45 CFR 164 Subpart D

NIST SP-800-111, Guide to Storage Encryption Technologies for End User Devices NIST SP-800-88, Guidelines for Media Sanitization

Attachments:

Security Incident Report

Security Incident Investigation Report

Risk Assessment Analysis Tool

Security Incident Privacy Breach Assessment

Security Incident Report Log