SEPA Labs	**Policy & Procedure** **BREACH NOTIFICATION**	**FUNCTION** **NUMBER** 4g **PRIOR ISSUE** **EFFECTIVE DATE** January 1, 2014

BREACH NOTIFICATION POLICY

1. PURPOSE

The purpose of this Breach Notification Policy is to provide guidance to the staff of SEPA Labs when there is a breach an acquisition, access, use, or disclosure of SEPA Labs patients' unsecured protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996 and its implementing rules and regulations, which compromises the security or privacy of the Protected Health Information (PHI). HIPAA requires that SEPA Labs notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances, SEPA Labs must also report such breaches to the Secretary of HHS and through the media. SEPA Labs breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 and its implementing rules and regulations, each as may be amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013), collectively "HIPAA."

2. DEFINITIONS

2.1 Breach. Breach means the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information. Breach excludes:

- 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 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 HIPAA.
- Any inadvertent disclosure by a person who is authorized to access protection health information at a covered entity or business associate to another person authorized to access PHI 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 HIPAA.
- 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.

2.2 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.

2.3 Unsecured Protected Health Information (Unsecured PHI). Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

2.4 Workforce. Workforce means employees, volunteers, trainees, and other persons under the direct control of SEPA Labs, whether or not they are paid by SEPA Labs.

3. POLICY AND PROCEDURES

In summary, HIPAA requires that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. The notification requirements only apply to breaches of unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.

3.1 Discovery of Breach. A breach shall be treated as discovered as of the first day on which such breach is known to SEPA Labs or, by exercising reasonable diligence, would have been known to SEPA Labs or any person, other than the person committing the breach, who is a workforce member or agent of SEPA Labs.

Workforce members who believe that patient information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify his/her supervisor, SEPA Labs senior management (Dr. Godbey, Mr. Coor, Ms. Drury), or SEPA Labs privacy officer (Dr. McIntire).

Following the discovery of a potential breach, SEPA Labs shall begin an investigation, conduct a risk assessment, and, based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by SEPA Labs to have been, accessed, acquired, used, or disclosed as a result of the breach. SEPA Labs shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services (HHS), media outlets, or law enforcement officials.

3.2 Breach Investigation. If a breach is thought to have occurred, then SEPA Labs shall name an individual to act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in SEPA Labs as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel.) SEPA Labs' entire workforce is expected to assist management in this investigation as requested. The investigator shall be the key facilitator for all breach notification processes.

3.3 Risk Assessment. For breach response and notification purposes, a breach is presumed to have occurred unless SEPA Labs can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

3.3.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
- 3.3.1.1 Social security numbers, credit cards, financial data
- 3.3.1.2 Clinical detail, diagnosis, treatment, medications
- 3.3.1.3 Mental health, substance abuse, sexually transmitted diseases, pregnancy

3.3.2 The unauthorized person who used the PHI or to whom the disclosure was made.
- 3.3.2.1 Does the unauthorized person have obligations to protect the PHI's privacy and security?
- 3.3.2.2 Does the unauthorized person have the ability to re-identify the PHI?

3.3.3 Whether the PHI was actually acquired or viewed.
- 3.3.3.1 Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?

3.3.4 The extent to which the risk to the PHI has been mitigated.
- 3.3.4.1 Can SEPA Labs obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, SEPA Labs will determine the need to move forward with breach notification. The investigator must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years.

3.4 Notification: Individuals Affected. If it is determined that breach notification must be sent to affected individuals, SEPA Labs' standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. SEPA Labs also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if SEPA Labs so chooses. Notice to affected individuals shall be written in plain language and must contain the following information, which elements are included in SEPA Labs' standard breach notification letter:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

- A description of the types of unsecured protected health information that were 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).
- Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what SEPA Labs is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

This letter will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If SEPA Labs knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. If 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, by telephone, or by other means. If 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 SEPA Labs' website, or a conspicuous notice in major print or broadcast media in SEPA Labs' geographic areas 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.

Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If SEPA Labs 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 the methods noted above. It is the responsibility of SEPA Labs to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

A copy of all patient correspondence shall be retained by SEPA Labs in accordance with state law record retention requirements.

3.5 Notification: HHS. In the event a breach of unsecured PHI affects 500 or more of SEPA Labs' patients, HHS will be notified at the same time notice is made to the affected individuals, in

the matter specified on the HHS website. If fewer than 500 of SEPA Labs' patients are affected, SEPA Labs will maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.

3.6 Notification: Media. In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

3.7 Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official states to SEPA Labs or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, SEPA Labs shall:

3.7.1 If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

- If the statement is made orally, document the statement, including the identify 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.

This applies to notices made to individuals, the media, HHS, and by business associates.

3.8 Maintenance of Breach Information. SEPA Labs 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 for each breach:

3.8.1 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.

3.8.2 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, other).

- A description of the action taken with regard to notification of patients regarding the breach.
- Steps taken to mitigate the breach and prevent future occurrences.

3.9 Business Associate Responsibilities. SEPA Labs' business associates shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI, notify SEPA Labs of such breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The business

associate shall provide SEPA Labs with any other available information that SEPA Labs 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 business associate of discovery of a breach, SEPA Labs will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals.

3.10 Workforce Training. SEPA Labs shall train all members of its workforce on SEPA Labs' policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within SEPA Labs.

3.11 Complaints. SEPA Labs provides a process for individuals to make complaints concerning SEPA Labs' patient privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about SEPA Labs' breach notification processes.

3.12 Sanctions. Members of SEPA Labs' workforce who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

3.13 Retaliation/Waiver. SEPA Labs may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

3.14 Burden of Proof. SEPA Labs has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.