Policy & Procedure

POLICY: #908 – Breach Notification and Oversight

SECTION: Corporate Compliance

MAINTAINED BY: Compliance/Privacy Officer

APPLIES TO:
- ☒ OnPoint Board of Directors
- ☒ OnPoint Staff
- ☒ Contracted Providers
- ☐ Other: _____

Approved By: _____
Chief Executive Officer

Approved By: _____
Medical Director (if applicable)

First Effective: 02/2017
Last Revised: 05/2026

PURPOSE
To outline how OnPoint shall comply with Federal and State regulations concerning responding to impermissible uses and/or disclosures of Protected Health Information.

DEFINITIONS
Refer to Attachment 901.5 Compliance Related Definitions and Terms
Access via OnPoint Intranet at: Policies & Procedures- Compliance
Access via OnPoint Website at: Providers – OnPoint

POLICY
As per HIPAA and 42 CFR Part 2 requirements, OnPoint shall provide notification to individuals whose unsecured Protected Health Information (PHI) has been impermissibly accessed, acquired, used or disclosed when such impermissible access compromises the security or privacy of PHI.

NOTE: Effective 2/16/26, Part 2 programs are required to notify the Sec of HHS if a breach of unsecured Part 2 records occurs (42 CFR 2.16 Ib)). The breach notification framework mirrors HIPAA's and will follow the same notification requirements outlined and referenced in this policy.

I. PROCEDURE(S)
   A. Breach Requirement
      1. A breach notification is required when a breach of unsecured PHI has occurred. Unsecured PHI is PHI that is not encrypted or has not been otherwise physically destroyed (by shredding, burning etc.).
      2. A breach is defined as the impermissible acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is *presumed* to be a breach unless OnPoint or a Business Associate of OnPoint demonstrates that there is a low probability that the PHI has been compromised.
      3. A breach of PHI shall be "discovered" on the first day the breach is known (including breaches by a Business Associate) by any person, other than the person committing the breach that is an employee, officer, or agent of OnPoint and knows or reasonably should have known of the breach.
      4. A breach shall not be deemed to have occurred if:
         i. The acquisition, access, or use of PHI was unintentional, was made by an employee or individual acting under the authority of OnPoint or Business Associate, was made in in good faith and within the scope of authority, and does not result in further use or

disclosure in an unauthorized manner (a manner not permitted by the privacy rule);

ii. The disclosure was inadvertent, was made by a person authorized to access the PHI at OnPoint or Business Associate, was made to another person authorized to access PHI at OnPoint or Business Associate or organized health care arrangement in which OnPoint participates, and does not result in further use or disclosure in an unauthorized manner (a manner not permitted by the privacy rule); or

iii. It is determined that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

B. Reporting Obligation

1. All individuals who become aware of any breaches or other confidentiality issues must report them to OnPoint Privacy Officer, member of the Compliance Committee and/or the Compliance Officer. Failure to report by individuals or entities are subject to disciplinary action.
2. A Business Associate shall notify OnPoint's Privacy and/or Compliance Officer of any breach immediately and in any event prior to the deadline for notification of individuals which is 60 days after the discovery of the breach. Such notice shall include all information needed to assess and monitor the breach. OnPoint Privacy Officer or Compliance Officer will notify all affected individuals unless the Business Associate previously agreed to provide notification in case of a breach. However, OnPoint is still responsible for such notification and must still ensure and document such notification.

C. Breach Investigation

1. If a breach has occurred, an investigation shall be conducted by the Privacy Officer, ~~or~~ Compliance Committee, and/or Compliance Officer to determine what information has been breached, when the breach occurred, and how many individuals have been affected.
2. An investigation may consist of interviews, documentation collection and review, and requiring mitigating action to prevent further impermissible uses or disclosures of PHI. All reports will be reviewed by the OnPoint Compliance Committee at its next regularly scheduled meeting.
3. The OnPoint Compliance Officer and Compliance Committee members will work collaboratively with the OnPoint Office of Recipient Rights and Security Officer on HIPAA privacy and/or security issues reported and/or being investigated whenever an issue involves a recipient of services to ensure that all Recipient Rights issues are being addressed as well as the HIPAA privacy and security requirements.
4. Also refer to OnPoint policy #904 *Compliance Inquires and Investigations*.

D. Breach Risk Assessment

1. OnPoint's Privacy Officer, the Compliance Committee, and or Compliance Officer will complete a Breach Risk Assessment for all impermissible uses and/or disclosures that do not fall under an exception.
2. The Breach Risk Assessment will be used to assist in determining if a breach compromises the security or the privacy of PHI and poses a significant risk to financial, reputation, or other harm to consumers served or entity to the extent that it requires notification to the affected individual(s).
3. The Breach Risk Assessment is to address the following factors:
   a. Whether an unauthorized PHI disclosure has occurred.
   b. The level of probability the PHI in question was compromised, based on consideration of at least the following factors:

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
ii. The unauthorized person who used the PHI or to whom the disclosure was made.
iii. Whether the PHI was actually acquired or viewed.
iv. The extent to which the risk to the PHI has been mitigated.

c. Whether the notification under the Breach Notification Rule is required.
d. Whether corrective action is necessary to address business processes, employee behavior, or other elements that factored into the impermissible disclosure.

E. Breach Notification

If breach notification is required, a notice to the individual(s), HHS, and the media, as applicable, shall be made no later than 60 calendar days after the discovery, or within required time frames, of the breach by OnPoint or Business Associate.

1. If a law enforcement official states that a notification would impede a criminal investigation OnPoint shall:
   a. Delay notification as specified by the official in writing, or
   b. If the statement is made orally, document the statement and delay notification no longer than 30 days from the date of the oral statement, unless a written statement is delivered during that time.
2. The notice to the individual(s) must contain the following information:
   a. Brief description of what happened, including the date of the breach and the date of the discovery of the breach.
   b. A description of the type of unsecured information involved in the breach (Social Security number, name, address, patient ID number, etc.).
   c. How the breach may affect the individual.
   d. Any steps the individual should take to protect themselves from the breach.
   e. A description of what is being done to investigate the breach to mitigate harm to the individual(s), and to protect against further breaches.
   f. Contact information for individuals to ask questions or learn additional information, which include a toll-free telephone number, email address, website, or postal address.
3. Notice to individuals shall be provided by first class mail to the individual at their last known address, or if agreement has been given by the individual, by e-mail. Additional information should be provided as it becomes available.
   a. If the individual is deceased, information should be provided to the next-of-kin, if known.
   b. If contact information for the individual is available and the individual and OnPoint have previously agreed, OnPoint may notify the individual via telephone or verbally.
   c. OnPoint will document the conversation.
   d. The verbal or telephonic notice must not simply be for the administrative convenience of OnPoint.
4. Notice shall be provided to the media when the breach of unsecured PHI affects more than 500 individuals. Notice shall be provided in the form of a press release.
5. Notice shall be provided to the Secretary of the Department of Health and Human Services through the use of a form posted at www.hhs.gov, or by letter to the Secretary notifying the Secretary of the breach.
   a. For breaches affecting 500 or more individuals, OnPoint will notify the Secretary within 60 days as instructed at www.hhs.gov;
   b. For breaches involving less than 500 individuals, OnPoint and Business Associates shall maintain a log and submit this log annually to the Secretary, no later than 60 days following the end of each calendar year in which the breach was discovered. Instructions

for submitting the log are provided at www.hhs.gov.

c. Regardless of the number of individuals affected, OnPoint Privacy Officer will keep a log documenting all breaches of unsecured PHI.

6. Breach Substitute Notice: In the case in which there is insufficient or out-of-date contact information that precludes notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided.
   a. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
   b. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
   c. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the covered entity involved or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside and will include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

II. Training

HIPAA Breach Identification, Reporting, and Notification Training is provided to OnPoint staff and provider staff via in-person and/or online training platforms (e.g., Relias).

REFERENCE(S)

Section 13400 of the HITECH Act (codified at 42 U.S.C. 17921) defined the term "Breach".
Section 13402 of the HITECH Act (codified at 42 U.S.C. 17932) enacted breach notification requirements.
45 CFR 164.400-414
42 CFR Part 2
#903 Compliance Inquires and Investigations.

ATTACHMENT(S)

908.1 Breach Notification Letter_Template_v.012026