Policy & Procedure

POLICY: #905 –Privacy and Security

SECTION: Corporate Compliance

MAINTAINED BY: Privacy and Security Officers

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

Approved By: _____
Chief Executive Officer

Approved By: _____
Medical Director (if applicable)

First Effective: 01/1999
Last Revised: 05/2026

PURPOSE

To assure the privacy and security of Protected Health Information (PHI) and Individually Identifiable Health Information (IIHI) in accordance with applicable federal and State laws.

DEFINITIONS

Refer to Attachment 900.4 Compliance Related Definitions and Terms
Access via OnPoint Intranet at: Policies & Procedures- Compliance
Access via OnPoint Website at: Providers – OnPoint

POLICY

OnPoint will safeguard Protected Health Information (PHI) and other confidential information from intentional or unintentional uses or disclosures. Such safeguards will include a variety of physical, administrative, and technical safeguards including but not limited to security of centralized paper record storage facilities, logical security of agency owned electronic devices and the Electronic Medical Record which are enforced via software rules, use of password-protected screensavers, and rules on retention and disposal of discarded documents containing PHI.

OnPoint Personnel and Contract Providers shall comply with the provisions of HIPAA (Health Insurance Portability and Accountability Act) Privacy (45 CFR 160 and Subparts A and E of Part 164) and Security (45 CFR Part 106 and Subparts A and C of Part 164) rules, the HITECH Act (Health Information Technology for Economic and Clinical Health Act), the Michigan Mental Health Code (Public Act 258 of 1974) and 42 CFR Part 2 Final Rule as it relates to privacy of substance use disorder records and related provisions within contracts with the Michigan Department of Health and Human Services (MDHHS), the Lakeshore Regional Entity (LRE) and OnPoint to preserve the privacy and security of PHI/IIHI.

PROCEDURE(S)

I. Personnel Designation

A. Privacy Officer – OnPoint's designated Privacy Officer works closely with the Office of Recipient Rights on matters related to privacy and confidentiality as the Michigan Mental Health Code and 42 CFR Part 2 are more stringent than HIPAA privacy on a number of matters. The Privacy Officer will also keep the Compliance Officer apprised of privacy breaches and issues needing to be addressed.

B. Security Officer – OnPoint's designated Security Officer works closely with the Privacy Officer on matters that cross over with privacy and keeps the Compliance Officer apprised of security breaches and issues needing to be addressed.
C. Compliance Officer – OnPoint's designated Compliance Officer may receive privacy or security reports and will refer and/or work with the Privacy or Security Officer and/or the Recipient Rights Director as necessary.
D. Compliance Committee – The Privacy and Security Officers are members of the OnPoint Compliance Committee and coordinate, collaborate, and keep the compliance committee apprised of privacy and security issues.
E. Refer to policy *903 Corporate Compliance Structure and Oversight Policy* for the overall structure and oversight of compliance, which includes the HIPAA Privacy and Security Officers, Compliance Officer, and the Compliance Committee.

II. Privacy Standards

A. Notice of Privacy Practices (NPP)
   1. Content of Notice
      a. Everyone receiving services has the right to receive adequate Notice of Privacy Practices (NPP) in plain language that describes:
         i. How OnPoint may use and disclose Protected Health Information (PHI) about an individual.
         ii. The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the agency.
         iii. OnPoint's legal duties with respect to the information, including a statement that OnPoint is required by law to maintain the privacy of PHI.
         iv. Whom the individual can contact for further information about OnPoint's privacy policies.
         v. The NPP must include an effective date.
         vi. OnPoint is required to promptly revise and distribute its (NPP) whenever it makes material changes to any of its privacy practices.
B. Providing the Notice
   1. When Opening a New Case
      a. OnPoint and Contracted Providers who admit clients directly must:
         i. Provide the notice to the client no later than the date of first service delivery and, except in an emergency treatment situation, make a good faith effort to obtain the client's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.
         ii. When first service delivery to a client is provided over the Internet, through email, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the client's first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the client in response to receiving the notice.
         iii. OnPoint may email the notice to a client if the client agrees to receive an electronic notice [45 CFR 164.520(c)) and in accordance with OnPoint policy.
C. In Emergency Treatment Situations – OnPoint will provide the NPP as soon as it is reasonably practicable to do so after the emergency has ended. In these situations, it is not required to make a good faith effort to obtain a written acknowledgment from individuals.
D. OnPoint and Contract Providers will also:
   1. Make its notice available to any person who asks for it.
   2. Post and make available its notice on any web site it maintains that provides information about

its customer services or benefits.

3. Make the latest notice available at OnPoint's office for client's who request to take with them and post it in a clear and prominent locations at the office.
4. Post a revised NPP as soon as it becomes effective.
5. Ensure that, except when required by law, a material change to any term of the NPP will not be implemented prior to the effective date on the NPP.

III. Security Standards

A. OnPoint's security standards address the HIPAA security rule as well as other reasonable and appropriate administrative, physical, and technical safeguards for protecting PHI.

B. The HIPAA Security Rule protects a subset of individually identifiable health information, referred to as **electronic protected health information** (ePHI), which is protected health information that is maintained in or transmitted by electronic media. Unlike the Privacy and Breach Notification Rules, the Security Rule does not apply to PHI that is maintained or transmitted on paper or verbally. However, this policy does also apply to PHI maintained or transmitted on paper or verbally, as appropriate.

C. OnPoint will ensure:
   1. The confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.
   2. Protection against reasonably anticipated threats to the security or integrity of the information.
   3. Protection against reasonably anticipated, impermissible uses or disclosures.
   4. Compliance by OnPoint personnel.

D. Administrative Safeguards include security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency planning, evaluation, and business associate agreements and other arrangements. See referenced policies for more detail.

E. Physical Safeguards include:
   1. Facility Access and Control
      a) Due to the confidential nature of our business and PHI, visitors are to be limited to those that are business related. Personal guests should be limited and must be accompanied by a staff member who will be responsible for safeguarding PHI.
      b) All building access doors are to remain locked at all times except the primary entrances which are open during normal hours of operations. Other staff access is available through an issued building key card.
      c) The primary entrances of each building are staffed by a receptionist, which are the only points to enter the building by clients and visitors. The receptionist will grant access to the locked (private) office areas as per the individual's need to enter and ensure the individual is accompanied by an OnPoint staff person at all times.
      d) PHI must be locked when staff are not present; paper documents must be in a locked file cabinet when office doors are not locked.
      e) Refer to policy #*1404* on *Building Security* for additional details.
   2. Workstation Use and Security - Refer to Policy 1201 Information Technology and 1201.1 IT Confidentiality and Use Agreement.
   3. Device and Media Controls - Refer to Policy 1201 Information Technology and 1201.1 IT Confidentiality and Use Agreement.
   4. Technical Safeguards - Refer to Policy 1201 Information Technology and 1201.1 IT Confidentiality and Use Agreement.

IV. Transporting Confidential Information

A. If possible, confidential information should not be transported in paper form. Agency owned electronic media (e.g., laptop, tablet) which is password protected is generally a preferred means of

transporting confidential information. Every effort must be made to assure the security of the Information at all times when in personnel's possession.

B. An employee is expected to obtain a lock box or case through the IT department and use it if they are transporting confidential information in paper or electronic form. When transporting, the lock box or case must be placed in the trunk of the staff's car, or somewhere out of sight.
C. Staff are to be keenly aware of their surroundings when accessing confidential information outside of OnPoint. This includes assuring that no other parties have access to any confidential information or has the ability to see any confidential information.
D. Staff are required to immediately report to the Security, Privacy, or Compliance Officer any stolen property and/or confidential information who will follow up as necessary.

V. Reporting and Breach Notification

A. All individuals who become aware of any privacy or security violation or incident must report them to OnPoint Privacy Officer, Security Officer, and/or Compliance Officer. Failure to report by an individual is subject to disciplinary action.
B. All Business Associates, including OnPoint Contract Providers, must notify OnPoint 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 outlined in the #908 Breach Notification and Oversight Policy.
C. Privacy and security incidents may be reported by calling 866-951-0063, online at https://bit.ly/4snF72Y or by scanning the QR code below. Reports may be made anonymously.
D. OnPoint will conduct or cause to be conducted a breach risk assessment and provide notification for each breach of unsecured PHI. Refer to policy *#908 Breach Notification and Oversight* for additional information.

VI. Discipline and Sanctions – OnPoint staff who fail to comply with privacy and security policies will be disciplined utilizing the guidelines outlined in applicable Compliance and HR Policy.

VII. Contracts with Third Parties/Business Associate Agreements (BAAs) – OnPoint contracts with various outside entities and organizations to perform functions or provide services on behalf of OnPoint. The policy of OnPoint is to obtain written assurances from Business Associates (BAs) that they will appropriately safeguard any PHI they create or receive on OnPoint's behalf. Such written assurances will be in place before OnPoint discloses PHI to the Business Associate. Each Business Associate must comply with HIPAA Privacy and Security Standards and OnPoint policy and is subject to the same penalties as a covered entity.

VIII. No Retaliation/Reprisal – Under no circumstances is retaliation for submitting a privacy, security, or compliance issue or inquiry acceptable for reporting in good faith. This includes but is not limited to questions and concerns an employee may discuss with an immediate supervisor, the OnPoint CO, a member of the OnPoint Compliance Committee, the OnPoint CEO, or the LRE CO. Any individual reporting, in good faith, suspected FWA is protected under the Whistleblowers' Protection Act 469 of 1980. https://www.legislature.mi.gov/documents/mcl/pdf/mcl- Act-469-of-1980.pdf. Clients may also file a complaint with Recipient Rights if they believe retaliation or harassment has occurred.

IX. Training

A. OnPoint Personnel will complete the following trainings at time of hire/appointment/contract and

annually thereafter:

1. Privacy
2. Security
3. Recipient Rights
4. Compliance

B. OnPoint Contract Providers and provider staff will complete the following trainings at time of contract or hire and annually thereafter:

1. Privacy
2. Security
3. Recipient Rights
4. Compliance

X. Documentation Retention

A. OnPoint will maintain, in paper or electronic form, investigative records for at least six (6) years from date of creation or last date in effect, or as required by law or OnPoint policy whichever is longer.

B. Behavioral health records will be maintained as outlined in policy on Records Retention and Disposal for further information on this area.

REFERENCE(S)

- Health Insurance Portability and Accountability Act of 1996 – Privacy and Security Rules - 45 C.F.R. Part 160 - PDF, Part 162 - PDF, and Part 164 - PDF.
- Health Information Technology for Economic and Clinical Health Act of 2009 (**HITECH** Act)
- Michigan Mental Health Code
- PIHP/LRE Contract with OnPoint
- Policy #708 Provider Contract Compliance
- Policy #904 Compliance Inquiries and Investigations
- Policy #907 Confidentiality, Use and Disclosure of PHI
- Policy #908 Breach Notification
- Policy #909 Records Retention and Disposal
- Policy #911 Reporting Responsibilities for Compliance Violations and Wrongdoing
- Policy #1201 Information Technology/System
- 1201.1 IT Confidentiality and Use Agreement
- Policy #1404 on Building Security and Safety

ATTACHMENT(S)

900.4 Compliance Related Definitions and Terms
903 Corporate Compliance Structure and Oversight Policy
905.1 Notice of Privacy Practices (Brochure)