<table>
<tr><td colspan="1">POLICY/PROCEDURE TITLE: HIPAA-Privacy and Security

POLICY/PROCEDURE #: 902

Section: Corporate Compliance and HIPAA</td><td colspan="2">Approved By: [signature]
(Chief Executive Officer)
Approved By: ______________________
(Medical Director; as applicable)</td></tr>
<tr><td rowspan="4">Developed and maintained by: Corporate Compliance Officer

Scope: ☒ OnPoint Staff ☒ MH/IDD ☒Housing ☒SUD
☒ Integrated Health ☒ OnPoint Contract Providers
☒ Other ______________________</td><td colspan="2">DATES</td></tr>
<tr><td>First Effective</td><td>01/1999</td></tr>
<tr><td>Revised</td><td>03/2025</td></tr>
<tr><td>Reviewed</td><td>03/2025</td></tr>
</table>

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

POLICY

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) and the Lakeshore Regional Entity (LRE) to preserve the privacy and security of PHI/IIHI.

STANDARDS AND PROCEDURES

A. Personnel Designation
   1. 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 is 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.
   2. Security Officer
      OnPoint's designated Security Officer keeps the Compliance Officer apprised of security breaches and issues needing to be addressed.
   3. 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.
   4. Compliance Committee
      The Privacy and Security Officers are members of the OnPoint Compliance Committee and coordinate and collaborate privacy and security issues with the other Compliance Committee members.

5. Refer to policy *901.3 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.

B. Notice of Privacy Practices

1. Everyone receiving services has the right to receive adequate "Notice of Privacy Practices" (NPP) in plain language that:
    - identifies how OnPoint may use and disclos~~ure~~ ~~of~~ Protected Health Information (PHI) about an individual.
    - describes 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.
    - describes OnPoint's legal duties with respect to the information, including a statement that OnPoint is required by law to maintain the privacy of PHI.
    - Lists who the individual can contact for further information about OnPoint's privacy policies.
2. The notice must include an effective date.
3. OnPoint is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices.

C. Opening Cases

1. OnPoint will offer a copy of the NPP at the first scheduled appointment for services. The notice is included as a part of the access/intake orientation meeting with individuals/parents/guardians. Documentation of good faith effort and/or written acknowledgement of acceptance, or if the individual declines, a copy will be a part of the clinical record on the checklist included on the Consent for Treatment.
2. When first service delivery to an individual is provided via telemedicine, OnPoint will provide adequate NPP either by U.S. mail or send an electronic NPP (with proper consent) prior to first date of service. OnPoint will make a good faith effort to obtain a return receipt or other confirmation from the individual in response to receiving the notice.

D. Emergency Treatment Situations

In an emergency treatment situation, 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.

E. Other ways OnPoint will make information about the use/disclosure of PHI available to individuals/parents/guardians include:

1. The current NPP will be posted in a clear and prominent place within all OnPoint sites.
2. Upon request, copies will be available at all OnPoint sites.
3. If requested and if the individual has signed a consent for e-mail, the NPP will be sent to an individual via e-mail.
4. Revisions to the NPP will be prominently indicated as they relate to changes to uses or disclosures, the individual's rights, legal responsibilities, or other privacy practices in the notice.
5. Whenever a NPP is revised, the revised NPP will be posted as soon as it becomes effective. 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.

F. Workforce Training
OnPoint requires upon hire HIPAA Compliance and Recipient Rights trainings. Annual, training must be completed in Corporate Compliance, HIPAA security, Privacy, and Recipient Rights.

G. Access to Building
1. 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.
2. 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.
3. The primary entrances of each building are staffed by a receptionist, which are the only points to enter the building by consumers and visitors. The receptionist will grant access to the locked (private) office areas as per the individuals need to enter and ensure the individual is accompanied by an OnPoint staff person at all time.
4. Refer to policy #*1404* on *Building Security* for additional details.

H. Transporting Confidential Information
1. 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. When it is necessary every effort must be made to assure the security of the Information.
2. 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.
3. 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.
4. Staff are required to immediately report to the Security, ~~or~~ Privacy, or Compliance Officer any stolen property and/or confidential information who will follow up as ~~required~~ necessary.

I. Confidentiality and Disclosure
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 Electronical Medical Record which are enforced via software rules, use of password-protected screensavers, and rules on retention and disposal of discarded documents containing PHI.

J. Complaints/Incidents/Breach Investigations
1. All individuals who become aware of any HIPAA 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.
2. 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.
3. Incidents may be reported verbally and/or in writing. OnPoint *#903.1 Compliance Report*

Form may be completed for submitting a written report of HIPAA violation or incident.

4. 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.
5. Complaints or incidents may be routed to the OnPoint Privacy, ~~or~~ Security, or Compliance Officer as outlined in Policy #911 Reporting Responsibilities for Compliance Violations and Wrongdoing and attachment *#901.4 Compliance Poster.* If complaints or incidents are routed through Recipient Rights, they will forward and/or coordinate with the OnPoint Privacy or Security Officer any HIPAA Privacy or Security related issues for documentation and follow-up.

K. 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.

L. 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 ~~this~~ OnPoint policy and is subject to the same penalties as a covered entity.

M. Mitigation
In the event of a privacy breach OnPoint will mitigate, to the extent practicable, any harmful effects that are known to have occurred.

N. No Retribution
OnPoint Personnel will not intimidate, threaten, coerce, harass, discriminate against, or take other retaliatory action against individuals for exercising any of their HIPAA privacy rights or taking any action such as filing a complaint or participating in an investigation. A consumer may file an additional complaint with Recipient Rights if they believe harassment or retaliation has occurred. Refer to Section G No Retaliation/Reprisal in Policy *#903 Compliance Inquires and Investigations Policy* for additional information.

O. Documentation Retention
1. OnPoint will maintain, in paper or electronic form, documentation required by HIPAA privacy law including policies and procedures, records of complaints, Consent to Share Behavioral Health Information (MDHHS-5515), accountings of disclosures provided to individuals, former versions of the Privacy Notice, and any other documentation as required. Such documentation will be maintained for at least six (6) years from date of creation or last date in effect, whichever is longer.
2. Refer to policy #909 on *Records Retention and Disposal* for further information on this area.

REFERENCES

- 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 #903 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 Acceptable Use of Information Technology
- Policy #1404 on Building Security and Safety