OnPoint

Caring for Allegan County

CORPORATE COMPLIANCE PLAN – FY26

October 1, 2025

(Reviewed and approved by Board of Directors annually, updated as needed)

OnPoint Compliance Committee Approval – 1/6/2025
OnPoint Board Executive Committee Recommended Approval – 1/16/2026
Approved by OnPoint Board – 1/20/2026

Contents

Introduction 1
Purpose of the OnPoint Compliance Program 1
Application of OnPoint Corporate Compliance Program 2
Legal Basis for Compliance Plan 3
Fundamental Elements of OnPoint's Compliance Program 4
Element 1 – Compliance Standards and Procedures 4
Element 2 – Compliance Program Leadership and Oversight 4
Element 3 – Effective Training and Education, Credentialing and Due Diligence 5
Element 4 – Effective Lines of Communication with the Compliance Officer and Disclosure Programs 5
Reporting 6
Non-Retaliation 7
Element 5 – Enforcing Standards: Consequences and Incentives 8
Element 6 – Risk Assessment, Auditing, and Monitoring 9
Element 7 – Responding to Detected Offenses and Developing Corrective Action Initiatives 9
Element 8 - Compliance Program Effectiveness Review **10**
Confidentiality and Privacy **10**
Reporting Contacts **11**
Attachment A – OnPoint Personnel Compliance Attestation 12
Attachment B – OnPoint Contract Provider Compliance Attestation 13
Attachment C – 901.5 Compliance Related Defiition and Terms **14**

Introduction

The OnPoint Corporate Compliance Plan provides a high-level overview of the Corporate Compliance Program and outlines OnPoint's commitment to ensuring compliance with applicable federal, state, and regional statutory, regulatory, and contractual requirements. The Compliance Plan provides a formal statement of OnPoint's intent to conduct itself ethically regarding business operations, adherence to applicable regulations, and providing services and care. It includes the fundamental elements of an effective compliance plan, which provides the overall strategy on how the agency will address fraud, waste, and abuse and other potential non-compliance.

To the extent that the OnPoint Corporate Compliance Plan conflicts with, or misstates any applicable regulation, statute or contractual requirement, the regulation, statute, and/or contractual requirement controls.

The overview of the OnPoint's compliance standards and practices are outlined in policy 901, Corporate Compliance Program and this document, (901.1 OnPoint Corporate Compliance Plan). Other compliance policies, procedures, and standards can be found in section 9 of the OnPoint policy and procedure manual.

Purpose of the OnPoint Compliance Program

Ultimately, the purpose of a corporate compliance program is to protect the organization. The benefits of a strong program go well beyond regulatory and legal compliance to also include operational benefits. A well-balanced corporate compliance program, along with a continuous quality improvement approach, will help ensure that the agency's organizational structure, people, processes, and technology are working in harmony to manage risks, improve stakeholder satisfaction, optimize the use of limited resources, oversee providers, and achieve strategic and operational goals. The purpose of the OnPoint Compliance Program is to also:

1. Encourage the highest level of ethical and legal behavior from all OnPoint Personnel and Contract Providers.
2. Educate all OnPoint Personnel, Contract Providers, and other applicable stakeholders on their responsibilities and obligations to comply with applicable federal, state, and local laws.
3. Communicate to all OnPoint Personnel and Contract Providers, and other applicable stakeholders OnPoint's Corporate Compliance Program structure to promote understanding and encourage communication.
4. Minimize organization risk and improve compliance with applicable federal, state, and regional statutory, regulatory, and contractual requirements; service provision, documentation standards; and Medicaid, and coding and billing requirements.
5. Maintain adequate internal controls throughout all programs.
6. Promote a clear commitment to compliance by taking actions and showing good faith efforts to uphold applicable federal, State, and regional regulations and contractual requirements.
7. Provide oversight and monitor functions to reduce the possibility of misconduct, and violations through prevention and early detection and minimize exposure to civil and criminal sanctions as well as non-compliance with applicable federal and state statutory, regulatory, and

contractual requirements; service provision; documentation standards; and Medicaid coding and billing requirements.

8. OnPoint's Compliance Program further supports the organization's Mission, Vision and Values which are:
    8.1. **Mission** – To improve the lives of people in Allegan County through exceptional behavioral health and homelessness services.
    8.2. **Vision** – An inclusive community with integrated behavioral health services and safe, affordable housing for all.
    8.3. **Values** – Integrity, Inclusivity, Honor, Equality, Humility, Innovation, Teamwork, Cultural Competence.

Application of OnPoint Corporate Compliance Program

The OnPoint Corporate Compliance Plan is intended to provide the framework for OnPoint to comply with all applicable laws, regulations, contracts, and program requirements. It is OnPoint's intent that all its compliance policies and procedures promote integrity, support objectivity, and foster trust throughout the service region. The OnPoint Corporate Compliance Plan applies to all OnPoint day-to-day activities, including those activities that come within Federal, State, and regional oversight of CMHSPs.

OnPoint personnel are subject to the requirements of the OnPoint Corporate Compliance Plan as a condition of employment/appointment/individual contract. All OnPoint personnel are required to fulfill their duties in accordance with the OnPoint Corporate Compliance Plan, policies, and procedures to promote and protect the integrity of OnPoint. Failure to do so will result in disciplinary action, up to and including termination of employment/contract, depending on the egregiousness of the offense. Disciplinary action may also be taken against a supervisory staff member, who directs or approves a staff member's improper conduct, is aware of the improper conduct, and does not act appropriately to correct it, or who fails to properly exercise appropriate supervision over a staff member.

OnPoint may contract for services and/or supports with external organizational providers. The OnPoint Corporate Compliance Plan applies to Network Providers receiving payment through OnPoint and/or through LRE managed care functions. All Network Providers, including their officers, employees, contractors, servants, and agents, are subject to the requirements of OnPoint Corporate Compliance Plan as applicable to them and as stated within the applicable contracts. Failure to follow the OnPoint Corporate Compliance Plan and cooperate with the OnPoint Corporate Compliance Program will result in corrective action plans, remediation, and contract action, as needed.

The OnPoint Corporate Compliance Plan, standards, policies, and procedures included or referenced herein are not exhaustive or all inclusive. All OnPoint personnel and Network Providers are required to comply with all applicable laws, rules, regulations, and policy including those that are not specifically addressed in the OnPoint Corporate Compliance Plan.

OnPoint's Compliance Officer and/or Compliance Committee may recommend modifications, amendments, or alterations to the written Corporate Compliance Plan and will communicate any changes to all OnPoint Personnel and Network Providers, as necessary.

This document is not intended, nor should be construed, as a contract or agreement and does not grant any individual or entity employment or contract rights.

Legal Basis for Compliance Plan

Numerous laws establish compliance requirements for the OnPoint and Contract Providers. However, in formalizing OnPoint's Corporate Compliance Program, the legal basis for OnPoint's Corporate Compliance Program centers around the following primary legal and regulatory standards. (For a more extensive list of compliance related laws and regulations see the list of Federal and Michigan Laws under "References" of Policy *#901 Corporate Compliance Program*.)

1. Affordable Care Act
   This ACT requires agencies to have a written and operable compliance program capable of preventing, identifying, reporting, and ameliorating fraud, waste, and abuse. All OnPoint Personnel and Contract Providers fall within the scope of the OnPoint Compliance Plan.

2. Anti-Kickback Statute.
   This Act (42 U.S.C. § 1320a–7b(b)) prohibits the offer, solicitation, payment, or receipt of remuneration, in cash or in kind, in return for or to induce a referral for any service paid for or supported by the Federal government or for any good or service paid for in connection with the delivery of services.

3. Civil Monetary Penalties Law
   The Civil Monetary Penalties Law (42 U.S.C. § 1320a–7a) allows HHS-OIG to seek civil monetary penalties and/or exclusion for many offenses. Penalties can range from several hundred to multimillion dollars based on the violation(s) cited.

4. Exclusion Statute
   Under the Exclusion Statute (42 U.S.C. § 1320a-7), HHS-OIG must exclude individuals or entities from participation in all federal healthcare programs when certain offenses are committed.

5. False Claims Acts (Federal and Michigan).
   The *Federal False Claims Act* (31 U.S.C. §§ 3729–3733) applies when an agency or individual knowingly presents or causes to be presented a false or fraudulent claim for payment; knowingly uses or causes to be used a false record or statement to get a claim paid; conspires with others to get a false or fraudulent claim paid; or knowingly uses or causes to be used a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Federal Government, or its designated entity.

   The *Michigan False Claims Act* prohibits fraud in the obtaining of benefits or payments in conjunction with the Michigan Medical assistance program; to prohibit kickbacks or bribes in connection with the program to prohibit conspiracies in obtaining benefits or payments, and to authorize the Michigan Attorney General to investigate alleged violations of this Act. Examples of criminal offenses that will result in exclusion include:
   - Medicare or Medicaid fraud
   - Abuse or neglect
   - Felony convictions for other healthcare-related fraud, theft, or other financial misconduct
   - Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances

The governmental agencies responsible for enforcing these laws are the U.S. Department of Justice, Department of Health and Human Services – Office of Inspector General (HHS-OIG), and the Centers for Medicare & Medicaid Services (CMS). In addition, the Michigan Attorney General's Office has responsibilities in Michigan for enforcement.

Fundamental Elements of OnPoint's Compliance Program

The HHS-OIG has declared that the elements described in Chapter 8 of the 2015 *United States Sentencing Commission Guidelines Manual and the US Dept of Health and Human Services Office of Inspector General, General Compliance Program Guidance, November 2023,* are the fundamental elements of an effective compliance plan. Therefore, OnPoint's Corporate Compliance Program is comprised of the recommended elements described below to ensure its program effectiveness.

Element 1 – Compliance Standards and Procedures

An effective compliance program is dependent on written policies, procedures, and code of ethical conduct. The development, distribution, and enforcement of Code(s) of Conduct and Ethics, and written policies and procedures that promote OnPoint's commitment to full compliance with applicable federal, state, and regional statutory, regulatory, and contractual obligations that are accessible and applicable to all OnPoint Personnel and Network Providers. These policies, procedures, and code(s) of conduct and ethics incorporate the culture of compliance into our day-to-day operations and address specific areas of potential fraud, waste, and abuse. OnPoint maintains its policies, procedures, and code of conduct and ethics through annual review.

See OnPoint Policies/Procedures:
For Providers at: Providers – OnPoint
For OnPoint Personnel at: Policies, Procedures and Guidelines – Home

Element 2 – Compliance Program Leadership and Oversight

OnPoint has established an extensive corporate compliance structure with defined roles that involves all levels of the organization. The structure consists of the Corporate Compliance Officer, Compliance Committee, Management Team, Chief Executive Officer (CEO), and Board of Directors.

OnPoint's Compliance Officer is responsible for the day-to-day activities of the compliance programs, monitors program implementation, and reports directly to the CEO with a direct line of reporting to the Board of Directors. The Compliance Officer:

- Is the primary "go to" person for compliance/noncompliance related issues.
- Must be familiar with the operational practices and compliance activities.
- Conducts and/or ensures compliance investigations are initiated timely and conducted within a reasonable timeframe.
- Is the chairperson and member of the Compliance Committee.
- Also acts in the capacity of OnPoint's Privacy Officer

The Compliance Committee is a multidisciplinary committee that reports to the Management Team and/or the CEO. The Compliance Officer and Compliance Committee are jointly responsible for:

- Reviewing, updating, and recommending approval of the compliance plan, policies, and procedures.
- Developing and revising, as needed, the compliance program work plan.
- Assisting in the annual risk management assessment and plan.
- Monitoring and reviewing the effectiveness of the compliance program.
- Assists and/or conducts compliance investigations.
- Is available to assist and provide guidance to the Compliance Officer.

OnPoint's Board of Directors provides oversight and monitors/ensures the effectiveness of the compliance program through the Board's Executive/Compliance committee which meets at least quarterly.

For more information on the key roles of OnPoint's Compliance Program refer to 901.3 *Compliance Structure and Oversight Policy and 900 Compliance Committee Charter*.

Element 3 – Effective Training and Education, Credentialing and Due Diligence

OnPoint requires training and education for the Compliance Officer, all personnel including senior management and board of directors, and contract providers and their employees regarding fraud, waste and abuse, the Deficit Reduction Act, other federal and State standards, and requirements applicable to program integrity and compliance. While the compliance officer may provide training to senior management, employees and board members, "effective" training for the compliance officer means it cannot be conducted by the compliance officer him/herself.

The initial training provides a comprehensive review of the OnPoint Compliance Program, the identity and role of the compliance, privacy, and security officers, the role of the compliance committee, the importance of open communication with the compliance officer, nonretaliation for disclosing or raising compliance concerns, the means through which the entity enforces its written policies and procedures equitably and impartially, and the Codes of Conduct/Ethics. Thereafter, annual training may highlight the Compliance Plan and any changes or new developments as well as re-emphasizing the OnPoint Employee Code of Conduct/Ethics. Targeted training may be required for personnel and/or contract providers involved in specific areas of risk. Successful completion of required training is considered a condition of employment/contract and failure to comply will result in disciplinary action up to and including termination.

Credentialing, criminal history checks, sanction checks and conducting due diligence on employees, potential employees and contractors are required to help ensure integrity of the workforce and contractors.

Element 4 – Effective Lines of Communication with the Compliance Officer and Disclosure Programs

Open lines of communication between the Compliance Officer and OnPoint Personnel, Contract providers, and other stakeholders is essential to the successful implementation of a compliance program and the reduction of any potential fraud, waste, and abuse. The Compliance Officer will communicate compliance messages via informal training methods, such as posters, newsletters, email, and Intranet communications. Avenues for communication must allow for anonymity and protection from retaliation for addressing concerns and/or reporting known or suspected violations.

Reporting

All OnPoint Personnel and contract providers have the responsibility of ensuring the effectiveness of the agency's compliance efforts by adhering to the Corporate Compliance Program, Employee Code of Conduct and Ethics, and reporting suspected and known violations.

Any suspected or known illegal, unethical, or improper activities need to be reported. Some examples of suspected violations include:

- Billing for services, assessments or medical tests that were never performed.
- Upcoding or inflating a bill by using diagnosis codes that increase the reimbursement amount for that service.
- Double billing or billing twice for the same service.
- Unbundling a service to submit multiple claims for a bundled service.
- Billing without reporting payments received from other sources.
- Reporting inaccurate dates and/or times of services provided.
- Billing for services that are not included in the individual's plan for services.
- Falsifying records or statements to get a claim paid or approved.
- Stealing cash or other OnPoint assets, such as property or supplies.
- Falsifying timesheets or workers comp claims.
- Falsifying expense reimbursements.
- Outside employment appears to conflict with OnPoint employment.
- Violations of the OnPoint Employee Code of Conduct/Ethics.
- Purposefully falsifying financial statements.
- HIPAA Privacy or Security violation issues.

OnPoint personnel, contract providers, persons served, or other stakeholders may choose any of the following methods for reporting suspected compliance violations and may report anonymously if desired.

- Electronic Mail (Email) – Suspected compliance violations can be sent by email to the following address: cofficer@onpointallegan.org. When emailing, staff may complete the form entitled "Compliance Complaint Reporting Form" (Refer to 903.1) or may specifically outline the details of their concerns within the content of an e-mail. For providers or individuals who do not have a @onpointallegan.org email address, PHI is **NOT** to be included in any unsecured emails.
- Mail Delivery – Suspected compliance violations can be mailed to the Compliance Officer at: OnPoint Compliance Officer, 540 Jenner Drive Allegan, MI 49010. When mailing, the form entitled 903.1 Compliance Complaint Reporting Form may be used, or the concerns may be submitted in any written format.
- In Person – Suspected compliance violations may be made in person to any member of the OnPoint Compliance Committee. Meeting via Zoom or Teams is considered to be "in person".
- By Phone – Suspected compliance violations may be made by calling the Compliance Officer directly at 269-512-4737. If there is no answer a *confidential* voice message may be left.
- In Fiscal Year 2026, OnPoint will implement a helpline for reporting. This will also allow for anonymous reporting.
- If preferred, suspected violations (related to Medicaid) may be reported directly to the Corporate Compliance Officer for the Lakeshore Regional Entity by calling 231-769-2050 and

asking for the Compliance Officer. More information may be found at: http://www.lsre.org/contact-us .

The OnPoint Compliance Officer will ensure that any problem identified through an investigative report, audit report, or data findings are analyzed and have the appropriate recommendation and/or follow-up. (Refer to policy *903 Compliance Inquiry and Investigations* for additional information.)

Where violations are substantiated, appropriate recommendation and/or corrective action will be initiated, which may include making prompt restitution of any overpayment amounts (within 60 days of identifying amount), notifying the appropriate governmental agency, staff education, and disciplinary action against responsible employees.

When it is determined that a report is deemed a credible allegation of fraud, the OnPoint Compliance Officer will immediately protect relevant information s/he has access to that may be needed to perform a thorough investigation and/or work with OnPoint's Information Management personnel to ensure protection. All document disposal practices will be stopped immediately. If reasonable suspicion exists that employees might destroy or remove documents, the employee's access to such documents may be suspended or removed pending investigative findings.

Compliance activity is reported to Lakeshore Regional Entity as required on the monthly Program Integrity Reporting template. Additionally, OnPoint's Compliance Officer will file all potential fraud allegations to the Lakeshore Regional Entity (LRE) when allegations of fraud, waste, or abuse of Medicaid dollars is estimated to be over $5,000. LRE will report to the OIG (Office of Inspector General) who will determine if further investigation will be completed by the OIG, LRE, or be assigned to OnPoint. This may also result in reporting to other governmental agencies as required.

For identified compliance related issues that do not require a formal investigation (i.e. a compliance inquiry), the Compliance Officer will document the reported incident and the outcome.

Non-Retaliation and Non-Intimidation of Persons Reporting Non-Compliance

OnPoint Personnel and Network Providers and staff, who make good faith reports of violations of federal or state law, are protected by state and federal whistleblower statutes.

Under the Federal False Claims Act and the Michigan Medicaid False Claims Act, employees who report violations in good faith are entitled to protection from disciplinary actions taken by their employer.

1. The Federal False Claims Act, 31 USC §§3729 through 3731, provides for administrative remedies, encourages enactment of parallel state laws pertaining to civil and criminal penalties for false claims and statements, and provides "whistleblower" protection for those making good faith reports of statutory violations.
2. Under the Michigan Medicaid False Claims Act, an employer shall not discharge, demote, suspend, threaten, harass, or otherwise discriminate against an employee in the terms and conditions of employment because the employee initiates, assists in, or participates in a proceeding or court action under this act or because the

employee cooperates with or assists in an investigation under this act. This prohibition does not apply to an employment action against an employee who the court finds: (i) brought a frivolous claim, as defined in section 2591 of the revised judicature act of 1961, 1961 PA236, MCL §600.2591; or (ii) planned, initiated, or participated in the conduct upon which the action is brought; or (iii) is convicted of criminal conduct arising from a violation of that act.

Element 5 – Enforcing Standards: Consequences and Incentives

For a compliance program to be effective, the organization should establish appropriate consequences for instances of noncompliance, as well as incentives for compliance. Consequences may involve remediation, sanctions, or both, depending on the facts. Incentives may be used to encourage compliance, performance, and innovation. Both incentives and consequences are important to enforcing compliance.

Consequences

OnPoint has established appropriate consequences for instances of noncompliance. Consequences are the result of noncompliant actions. Consequences may be educational or remedial and non-punitive, they may be punitive sanctions, or they may involve both.

To deter noncompliant behavior, the consequences of noncompliance will be consistently applied and enforced. All levels of employees are subject to the same consequences for the commission of similar offenses. The commitment to compliance applies to all personnel levels within the agency, including contractors and medical staff. Officers, managers, supervisors, health care professionals, and medical staff are all held accountable for failing to comply with, or for the foreseeable failure of their subordinates to adhere to, the applicable standards, laws, policies, and procedures.

OnPoint's policy 910 Enforcement and Discipline for Noncompliance Policy includes recommended disciplinary guidelines.

Corrective Action Plans

If an internal investigation substantiates a reported violation, corrective action will be initiated and may include, as appropriate, OnPoint: 1) issuing a non-compliance letter, 2) requiring a Corrective Action Plan (CAP) from the department or agency found out of compliance, 3) monitoring CAPs with appropriate follow-up, 4) requesting out of compliance agency develop a CAP inclusive of monitoring for adequate implementation and risk mitigation with approval from OnPoint, and 5) requiring changes to prevent a similar violation from recurring in the future, is possible.

As appropriate, given the nature of the noncompliance, a corrective action plan submitted to OnPoint for approval shall, at a minimum, include: 1) A detailed description of the corrective action that will be taken to minimize or eliminate the risk from repeating in the future, 2) Names or Titles of those responsible for implementing the corrective action, and 3) An implementation date.

Depending on the seriousness of the offense, the resulting action for OnPoint staff could include additional training, written reprimand, suspension, or termination of employment. The resulting action for the Network Provider would also depend on the seriousness of the offense and could include additional training, written reprimand, suspension, letter of contract non-compliance, and termination of contract.

Incentives

As a behavioral health service provider, OnPoint is unable to publicly recognize an individual who raises a substantiated concern that results in the mitigation of harm or risk. However, OnPoint will respond to suspected or known offenses reported and individually thank individuals for raising concerns when able. OnPoint also strives to recognize personnel in the performance reviews of individuals. This, of course, is not possible for people who wish to remain anonymous. Also, this does not apply to individuals who raise compliance or legal violations for which they themselves committed or were responsible.

Element 6 – Risk Assessment, Auditing, and Monitoring

Risk assessment, auditing, and monitoring each play a role in identifying and quantifying compliance risk.

Risk Assessment

Risk assessment is a process for identifying, analyzing, and responding to risk. A compliance risk assessment is a risk assessment process that looks at risk to the organization stemming from violations of law, regulations, or other legal requirements. As an entity participating in or affected by government health care programs, OnPoint's compliance risk assessment must focus on risks stemming from violations of government health care program requirements and other actions (or failures to act) that may adversely affect OnPoint's ability to comply with those requirements. Periodic compliance risk assessments is a component of OnPoint's compliance program and is reviewed/updated/conducted at least annually.

Responsibility for OnPoint's Risk Assessment and Plan have been assigned to the QI Department who will present to the Compliance Committee and Management Team for review, feedback, and final approval. The assessment and plan will incorporate all areas of risk including privacy, security, and departmental.

Auditing and Monitoring

A schedule of audits to be conducted based on risks identified by the annual risk assessment and other activities will be included in the annual Compliance work plan. This work plan will also contain routine monitoring of ongoing risks, plus the capacity to monitor the effectiveness of controls and risks remediation. Routine monitoring may include monthly screening of LEIE and State Medicaid exclusion lists, regular screening of State licensure and certification databases, routine audits of clinical documentation and billing, and annual review of OnPoint policies and procedures. Other areas appropriate for routine monitoring will be based on OnPoint's risk assessment and results of audits, monitoring, and investigations.

Element 7 – Responding to Detected Offenses and Developing Corrective Action Initiatives

Allegations of noncompliant conduct are investigated, and the outcome of the investigation should determine whether, and what kind of, reporting to the Government is necessary. There may be material violations of applicable law where no monetary loss to a federal or State health care program or Government entity has occurred; however, in these instances, corrective action and reporting (e.g., to CMS or a State Medicaid program) are still necessary to protect the integrity of the applicable program

and its enrollees.

OnPoint believes in the importance of self-reporting. OnPoint will utilize the OIG's voluntary self-reporting program to report suspected fraud, as necessary.

OnPoint will take prompt corrective action upon the collection of sufficient credible information to determine the nature of the misconduct. Corrective action may include, but is not limited to:

- refunding of overpayments;
- enforcing disciplinary policies and procedures; and
- making any policy or procedure changes necessary to prevent a recurrence of the misconduct.

If the misconduct resulted in an overpayment, OnPoint will promptly repay the overpayment to affected government agency(ies). Federal law requires repayment to Medicare or State Medicaid program within 60 days after identification.

Element 8 – Compliance Program Effectiveness Review

A compliance program effectiveness review is conducted annually and should assess how effective each element of the compliance program is. The OnPoint Board's Executive/Compliance Committee will review and confirm the effectiveness assessment and present the findings and recommendations to the full Board of Directors.

CONFIDENTIALITY AND PRIVACY

OnPoint Personnel and Network Providers and staff must conduct themselves in accord with the principle of maintaining the confidentiality of consumers' information in accordance with all applicable laws and regulations, including but not limited to the Michigan Mental Health Code and the Privacy and Security Regulations issued pursuant to HIPAA and HITECH regulations, and 42 CFR Part 2 as it relates to substance abuse records. OnPoint Personnel and Network Providers and staff will refrain from disclosing any personal or confidential information concerning consumers unless authorized by laws relating to confidentiality of records and protected health information. If specific questions arise regarding the obligation to maintain the confidentiality of information or the appropriateness of releasing information, OnPoint Personnel and Network Providers and staff should seek guidance from the OnPoint Compliance/Privacy Officer or anonymously seek guidance through the OnPoint Corporate Compliance and Privacy Helpline at 1-866-951-0063.

OnPoint Personnel and Network Providers and staff are expected to maintain confidentiality and refrain from discussing reports of non-compliance and associated, interviews, documentation, etc. pertaining to such report, inquiry, or investigation. OnPoint will strive to maintain the confidentiality of the reporting employee/provider's identity. There may be a point where the individual/provider's identity may become known or may have to be revealed. For example, in certain instances OnPoint may be required to inform governmental authorities.

ONPOINT COMPLIANCE CONTACT AND REPORTING INFORMATION

OnPoint Compliance Officer – Tel: 269-512-4737; Email: Cofficer@onpointallegan.org
OnPoint Privacy Officer – Tel: 269-512-4737; Email: Cofficer@onpointallegan.org
OnPoint Security Officer– Tel: 269-512-4737; Email: Cofficer@onpointallegan.org
OnPoint Compliance Helpline – Tel: 1-866-951-0063– anonymous reporting
Lakeshore Regional Entity (LRE) Compliance Officer– Tel: 231-769-2079; Email: Compliance@lsre.org

GOVERNMENTAL AGENCIES

To report suspected Fraud, Waste, or Abuse to the Office of Inspector General: MDHHS Medicaid Fraud Hotline: 1-855-MI-FRAUD (1-855-643-7283) voicemail available after hours or send a letter to:

Michigan Office of Inspector General
PO Box 30062
Lansing, MI 48909

Health and Human Services (HHS)/OIG Hotline: 1-800-HHS-TIPS (1-800-447-8477) or make an online report: https://oig.hhs.gov/fraud/report-fraud/

OnPoint
Caring for Allegan County

Attachment A – OnPoint Personnel Compliance Attestation

OnPoint Personnel Compliance Attestation

1. I acknowledge that I received a copy of and/or training on OnPoint's Corporate Compliance Program. This includes an overview of OnPoint's written Compliance Plan and associated compliance policies, standards, procedures, structure, and Code of Conduct and Ethics which collectively make up the OnPoint Corporate Compliance Program.
2. I understand that I am responsible for participation and successful completion of future compliance training and understand that failure to do so may result in disciplinary action, up to and including termination of my employment.
3. I have received and understand the Corporate Compliance Plan and Code of Conduct and Ethics and pledge to act in compliance with and abide by both, the Compliance Program and Code of Conduct and Ethics.
4. I understand the processes for reporting potential violations and accept my responsibility to report any suspected or known compliance violations. I understand that failure to report may result in disciplinary action, up to and including termination of my employment.
5. If I have questions concerning appropriate actions that I may need to take to comply with the requirements, I will seek advice from OnPoint's Compliance Officer and/or a member of the OnPoint Compliance Committee.

_____ _____

OnPoint Personnel (Please print) Title (Please print)

_____

Organization

_____ _____

Signature Date

OnPoint

Caring for Allegan County

Attachment B – OnPoint Contract Provider Compliance Attestation

OnPoint Contract Provider Compliance Attestation

1. I acknowledge that I have received a copy of and/or training on OnPoint's Corporate Compliance Program. This includes a copy and/or overview of OnPoint's written Compliance Plan and applicable compliance policies, standards, procedures, and Code of Conduct and Ethics which collectively make up the OnPoint Corporate Compliance Program.
2. I understand that I am responsible for participation and successful completion of future compliance training, as required, and understand that failure to do so may result in sanctions up to and including termination of our contract with OnPoint.
3. I have received and understand the OnPoint Corporate Compliance Plan and Code of Conduct and Ethics.
4. I understand the processes for reporting potential violations and accept my responsibility to report any suspected or known compliance violations to OnPoint. I understand that failure to report may result in sanctions, up to and including termination of our contract with OnPoint.
5. I pledge to educate staff and others within my organization on OnPoint and internal compliance related requirements, as applicable, including how and where to report suspected or known violations or wrongdoing.
6. If I have questions concerning appropriate actions that I may need to take to comply with OnPoint's Compliance Program requirements, I will seek advice from OnPoint's Compliance Officer and/or a member of the OnPoint Compliance Committee and ensure staff are aware of this opportunity.

_____ _____

Contract Provider Owner/CEO/Director (Please print) Title (Please print)

_____

Organization

_____ _____

Signature Date

OnPoint
Caring for Allegan County

Attachment C – 901.5 Compliance Related Definitions and Terms

Abuse - Practices that are inconsistent with sound fiscal, business, or clinical/medical practices, and result in an unnecessary cost to the Medicaid program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards of care. It also includes beneficiary practices that result in unnecessary cost to the Medicaid programs. (42CFR 455.2)

Alleged Violation/Alleged Wrongdoing - Conduct which, at face value, appears to conflict with required law, regulation, contract language, agency policy or Code of Conduct/Ethics or illegal activity. (Also see "Wrongdoing" and "Violation").

Breach - The unauthorized acquisition, access, use, or disclosure of PHI in a manner which compromises the security of privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain the information." (45 CFR 164.408)

Business Associate (BA) - A person or organization that performs a function or activity on behalf of a *covered entity* but is not part of the c*overed entity's workforce*. A *business associate* can also be a *covered entity* in its own right. Also see Part II, 45 CFR 160.103.

Complaint - A complaint is any report of suspected or known violation of applicable laws, regulations, contract language, regional and local policies, etc., any suspected wrongdoing, or known or suspected fraud, waste, or abuse of public funding.

Complainant - The individual reporting the alleged compliance violation, wrongdoing or improper conduct. A reporting person can be any agency officer, board member, full-time, part-time and temporary employee, volunteer, student, applicant for employment, provider, vendor, (sub)contractor and any other person or entity that may become part of or affiliated with the provider network in the future.

Compliance Investigations - The observation or study of suspected fraud, abuse, waste, or reported violations of laws and regulations for all OnPoint covered services aby close examination and systematic inquiry.

Confidentiality of Alcohol and Drug Abuse Participant Records - 42 CFR Part 2 - 42 CFR Part 2 applies to AOD (Alcohol and Other Drugs) programs that are federally conducted, regulated or assisted in any way, directly or indirectly. Regulations apply to recipients of AOD and their participant identifiable information and prohibit most disclosures of information without participant consent.

https://www.gpo.gov/fdsys/granule/CFR-2010-title42-vol1/CFR-2010-title42-vol1-part2/content-detail.html

Contract Provider (Also referred to as Network Provider) - Any individual, group, or organization that has a provider agreement with OnPoint to provide services and supports to individuals we serve.

Corporate Compliance - The organization's adherence to laws, regulations, contract language, and policies applicable to its operations. Consists of the mechanisms, including the written Compliance Plan and Policies, that are collectively intended to prevent and detect unethical and/or illegal business practices and violations of law.

Corporate Compliance Plan - Provides a formal statement of OnPoint's intention to conduct itself ethically in regard to business operations, government regulations, conduct, and services and care; it includes the required seven fundamental elements of an effective compliance plan, which provides the overall strategy on how the agency will address fraud, waste and abuse and overall compliance.

Corporate Compliance Program - A formal program specifying an organization's policies, procedures, and actions (plan) to help prevent and detect violations of laws, regulations, contractual obligations, standards, and ethical practices. OnPoint's "Corporate Compliance Program" is made up of the Corporate Compliance Plan and all association compliance policies, including but not limited to the Code of Conduct and Ethics.

Covered Entity - Is defined at CFR 160.103 as one of the following: (1) A health plan; (2) a health care clearinghouse; (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by part 162 of title 45 of the Code of Federal Regulations (CFR).

Disclosure - The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Also see Part II, 45 CFR 164.501.

Fraud (Federal Claims Act) - An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some authorized benefit to himself or some other person [or agency/organization]. It includes any act that constitutes fraud under applicable Federal or State law including but not limited to the Federal False Claims Act and the Michigan False Claims Act (42CRF 455.2)

Fraud (Per Michigan Statue and Case Law Interpretation) - Under Michigan law, a finding of Medicaid fraud can be based upon evidence that a person "should have been aware that the nature of his or her

conduct constituted a false claim for Medicaid benefits, akin to constructive knowledge." Errors or mistakes do not constitute "knowing" conduct necessary to establish Medicaid fraud, unless the person's "course of conduct indicates a systematic or persistent tendency to cause inaccuracies to be present."

FWA -The federal term contained in the Deficit Reduction Act (DRA) refers to any event pertaining to an alleged or actual wrongdoing of Fraud, Waste or Abuse (i.e., generically known as "FWA").

Health Information - Any information, whether oral or recorded in any form or medium that: (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and that (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

HIPAA Privacy Rule - Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without participant authorization. The Rule also gives participants' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA Security Rules - Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

HITECH (Health Information Technology for Economic and Clinical Health Act of 2009) - The Act provides for improved portability of health benefits and enables better defense against abuse and fraud, reduces administrative costs by standardizing format of specific healthcare information to facilitate electronic claims, directly addresses confidentiality and security of patient information - electronic and paper. HIPAA was amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (**HITECH** Act), as set forth in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009. The United States Department of Health and Human Services (DHHS) promulgated administrative rules to implement HIPAA and HITECH, which are found at 45 CFR Part 160 and Subpart E of Part 164 (the "Privacy Rule"), 45 CFR Part 162 (the "Transaction Rule"), 45 CFR Part 160 and Subpart C of Part 164 (the "Security Rule"), 45 CFR Part 160 and Subpart D of Part 164 (the "Breach Notification Rule") and 45 CFR Part 160, Subpart C (the "Enforcement Rule"). DHHS also issued guidance pursuant to HITECH and intends to issue additional guidance on various aspects of HIPAA and HITECH compliance. Throughout this policy, the term "HIPAA" includes HITECH and all DHHS implementing regulations and guidance. (Contract between Lakeshore LRE and ONPOINT – Medicaid Managed Specialty Supports and Services …, p. 6)

Individually Identifiable Health Information (IHHI) (Also see Protected Health Information (PHI)) - Information that is a subset of health information, including demographic information collected from an individual and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identified the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Inquiry - An informal process whereby a person makes the Compliance Office aware of a potential compliance related concern and the Compliance Officer examines the concern to determine if it merits a formal complaint and investigation. If the outcome of the *inquiry* determines that the matter is not FWA related, the Compliance Officer will document the *inquiry* and outcome and take any action necessary to rectify the concern. Conversely, if the outcome of the *inquiry* determines that a formal investigation is warranted, the Compliance Officer will convert the informal *inquiry* into a formal complaint and will conduct a formal investigation in accordance with the policy investigation guidelines.

Knowingly - Defined under the federal False Claims Act (FCA) to include the willful disregard of a regulation imposed upon an organization, the "deliberate ignorance" of the regulation's propriety, the submission of a claim in "reckless disregard" of the truth, or the falsity of claim. Managerial staff of the provider organization can be held accountable in situations where they refuse to explore a credible concern about the compliance requirements for a particular business or clinical practice, or a submitted bill or claim requiring use of federal funds for its reimbursement.

Lakeshore Regional Entity (LRE) -The LRE is the PIHP (Prepaid Inpatient Health Plan) created to manage specialty carved out Medicaid mental health, intellectual/developmental disability, and substance use disorders services for Medicaid and Health Michigan enrollees in Allegan, Lake, Mason, Oceana, Muskegon, Ottawa, Kent counties. The LRE includes any administrators retained by contract by the LRE.

Marketing - Marketing and advertising practices are defined as those activities used by OnPoint to educate the public, provide information to the community, increase awareness of services, and recruit employees or contractual providers.

Minimum Necessary – HIPAA Privacy Rule Standard (45 CFR 164.502(b), 164.514(d)) - A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose (*need to know*) of the use, disclosure, or request.

Nominal Value - $25.00 or less per gift; $300 maximum per year from any one individual/organization/company.

Personnel - For the purposes of the Compliance Program Plan and associated Policies, Personnel means OnPoint's staff members, Board of Directors, individuals under contract, students, interns, and volunteers.

Protected Health Information *(Also see Individually Identifiable Health Information (IIHI))* - Any information, whether oral or recorded in any form or medium, that is created or received by a "Covered Entity" (or a Business Association of a Covered Entity), and relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Provider - Any healthcare organization that furnishes or renders health care services or items within the agency network for which Medicaid or Medicare reimbursement will be sought. A provider includes a person who performs billing, coding, or other reporting services functions. OnPoint often makes a distinction between internal providers (employees) and external providers (contract providers).

Psychotherapy Notes - As defined by 45 CFR 164.501 - Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the record. Psychotherapy notes do not include any information about medication prescription and monitoring counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests, nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Qui Tam Provision - The federal False Claims Act (FCA) allows any person with direct knowledge of a false claim to bring a civil suit on behalf of the United States Government, known as a "*Qui Tam*" action. The individual must first formally notify the Department of Justice of the suspected fraud. The Department of Justice then has the option of either intervening in and prosecuting the action or allowing the individual to proceed on his/her own. If the suit is ultimately successful, the individual who initially brought the suit may be awarded a percentage between 15- 30% of the funds recovered.

Violation - An action that breaks or acts against something, especially a law, agreement, principle, or something that should be treated with respect. An act or omission concerning (a) a violation of any law or regulation; (b) a breach of the Code of Conduct/Ethics of OnPoint; (c) knowing non-compliance with a OnPoint policy; (d) misuse of public funds or assets; (e) mismanagement of a nature sufficiently substantive which would lead one to reasonably believe that such mismanagement would have a potentially harmful impact on OnPoint's work, reputation or operations; or (f) conduct which includes such behaviors as intimidation, harassment and other unethical behavior.

Use of Protected Health Information (PHI)/Individually Identifiable Health Information (IIHI) - The sharing of health/clinical information, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Waste - Over utilization of services or other practices that result in unnecessary costs. Generally, not

considered caused by criminally negligent actions but rather the misuse of resources.

Whistleblower - A person who tells someone in authority about alleged dishonest or illegal activities (misconduct) occurring in a government department, a public or private organization, or a company. The alleged misconduct may be classified in many ways; for example, a violation of a law, rule, regulation and/or a direct threat to public interest, such as fraud, health/safety violations, and corruption.

Wrongdoing - Illegal or dishonest behavior. Under the federal Deficit Reduction Act (DRA), "wrongdoing" may be either an intentional act or an unintentional act (i.e., omission).