OnPoint

Caring for Allegan County

CORPORATE COMPLIANCE PLAN – FY25

October 1, 2024

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

OnPoint Compliance Committee Approval – 9/23/2024
OnPoint Program Committee Recommended Approval – 10/15/2024
Approved by OnPoint Board – 10/15/2024

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 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 other potential non-compliance.

All OnPoint Personnel and Contract Providers are required to comply with applicable federal, state, and regional statutory, regulatory, and contractual requirements including but not limited to those specifically addressed in the OnPoint Corporate Compliance Plan.

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.

Key Definitions and Terms

Please see Attachment C – 901.5 Compliance Related Definitions and Terms

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

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:

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.

In addition, 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.

New or revised regulations or requirements can represent potentially high risk for non-compliance. As these changes become effective, the Corporate Compliance Committee may determine that a special focus and/or plan are needed to become and/or maintain compliance in any given area.

There are numerous laws and regulations that affect the OnPoint Compliance Program. 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*.

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 Contract 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.

Seven Fundamental Elements of an Effective Compliance Plan

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 seven fundamental elements of an effective compliance plan. Element eight is a necessary component recommended by the Officer of Inspector General and therefore has been included in this Plan. The eight fundamental elements are outlined below.

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 written Employee Code of Conduct and Ethics, as well as written policies and procedures that promote OnPoint's commitment to full compliance with applicable federal, state, and regional statutory, regulatory, and contractual obligations and to aggressively address potential fraud, waste, and abuse is critical to a successful compliance program. These policies, procedures, and code 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.

Element 2 – Compliance Program Oversight

Corporate compliance issues are complex with a multitude of regional, State, and federal laws and regulations in which the organization must comply. In response, 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, Executive Director, and Board of Directors.

OnPoint has designated two key roles, the OnPoint Compliance Officer, and the Compliance Committee, for the primary oversight and administration of the Compliance Program. The Compliance Officer:

- Is the primary "go to" person for compliance/noncompliance related issues.
- Reports directly to the Executive Director and has a direct line of report and access to the OnPoint Board of Directors.
- 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.

The Compliance Committee is a multidisciplinary committee that reports directly to the Management Team and the Executive Director. 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 plan, policies, and the risk management 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.

For more information on the roles of the Compliance Officer and Compliance Committee, 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 and Employee Code 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. Additional 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

Open lines of communication between the Compliance Officer, OnPoint Personnel, Contract providers, and other stakeholders are essential to their knowledge and awareness of compliance issues, to the successful implementation of the Compliance Program, and minimizing noncompliance. The Compliance Officer will communicate compliance messages via informal training methods, such as posters, newsletters, and Intranet communications. Avenues for communication must allow for anonymity and protection from retaliation for addressing concerns and/or reporting known or suspected violations.

Element 5 – Reporting, Response and Prevention

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 violations.

Any suspected 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.
- Performing inappropriate or unnecessary procedures to increase reimbursement.
- 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 such as Medicare.
- Inflating the actual work performed or billing for the highest level of service when a lower level of service was delivered.
- 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 will not take disciplinary or retaliatory action against a person for reporting, in good faith, what the person reasonably believed to be a potential compliance violation or wrongdoing. However, an employee will be subject to disciplinary action up to and including termination if it is concluded that the employee knowingly fabricated, exaggerated, or minimized a report of a violation or wrongdoing to either injure someone else or to protect himself/herself or others. Also, an employee whose report contains admissions of personal violation or wrongdoing will not be guaranteed protection from discipline. Retaliation for reporting an alleged compliance violation or wrongdoing is strictly prohibited and may lead to disciplinary action up to and including termination.

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

The Compliance Officer will file a potential fraud allegation report to the Lakeshore Regional Entity (LRE) Compliance Officer if/when allegations of fraud, waste, and abuse of Medicaid dollars is

estimated to be over $5,000. This may result in reporting to an appropriate governmental agency as necessary.

Where violations are substantiated, appropriate 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.

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.

Compliance activity is reported to Lakeshore Regional Entity as required on the quarterly Program Integrity Reporting template. Additionally, compliance activities with an estimated value of $5,000 or more are reported to LRE upon identification of the estimated amount. 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.

Element 6 –Monitoring, Auditing, and Risk Management

OnPoint has created systems for monitoring and auditing the effectiveness of the Corporate Compliance Program as well as identifying compliance risks. Investigative findings will also provide areas of concern and identify opportunities for improvement.

Monitoring includes reviewing compliance related policies and procedures to gauge whether they are working as intended and follow-up on recommendations and corrective action plans to ensure they have been implemented.

Auditing ensures compliance with statutory and CMS requirements and includes routine evaluations of the compliance program to determine the program's overall effectiveness.

Monitoring and auditing of the agency's operations are critical to ensure compliance with the Compliance Program including the Code of Conduct and Ethics. This is completed by external entities as well as established internal processes. Monitoring and auditing can also identify areas of potential risk and those areas where additional education may be needed.

Risk Management - The Compliance Committee, in collaboration with the Management Team, will oversee the development and processes associated with the agency's Risk Management Plan.

A. Risk management is utilized for identifying risks to the organization and making informed decisions to avoid or control these risks, thus enabling the organization to minimize or eliminate events that contribute to losses.

B. As part of the risk analysis, risk assessments will be conducted routinely and include the vulnerabilities to the confidentiality/privacy, security, integrity, and availability of protected health information.
C. The Risk Management Plan focuses on the identified risks and what must or can be done as preventive measures, measures to protect the organization and prevent loss, and corrective measures to prevent the risk of further occurrence. The Risk Management Plan lists the potential risk to the organization and outlines a coordinated set of activities designed to control the potential threats to people, property, credibility, income, and goodwill, and reduces potential barriers for the accomplishment of the goals of the organization.

Element 7 - Enforcement and Discipline

For the compliance program to be effective, OnPoint has established appropriate consequences for instances of noncompliance. Consequences may involve remediation, sanctions, or both depending on the facts. 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.

Element 8 – Compliance Program Risk Assessment (Program Effectiveness Review)

A compliance program effectiveness review is conducted annually and should assess how effective each element of the compliance program is. Findings and recommendations will be reported to the OnPoint Board of Directors.

Conclusion

Compliance is a complex topic when providing mental health and substance use disorder services as it involves numerous regulations and layers of oversight. However, at its core, compliance is intended to promote ethical conduct and business practices. By developing and adhering to an effective Compliance Program and educating staff, OnPoint practices can prevent fraudulent activity, including fraud, waste and abuse of public resources, promote ethical behavior and business practices, and support quality care and service

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 individua; or the past, present, or future payment for the provision of health care to an individua; and that identified the individua; 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).