POLICY AND PROCEDURE

REACH for Tomorrow

POLICY: RG-108

TITLE: Compliance Investigation, Reporting, Documentation, & Resolution

EFFECTIVE DATE: 2/8/24 **AUTHORIZED BY: Board of Trustees**

This procedure shall apply to REACH for Tomorrow.

1.0 Intent

It is the intent of REACH for Tomorrow to establish and maintain mechanisms for the investigation, reporting, resolution, and documentation of suspected violations or potential misconduct with assurances for confidentiality and non-retaliation. It is the intent of REACH for Tomorrow to also ensure that all Board Members, employees, and contractors fulfill the requirements of the Deficit Reduction Act.

2.0 Deficit Reduction Act & Compliance

2.1 REACH for Tomorrow shall have internal processes to monitor for actions by providers to prevent fraud, abuse, and waste, and to identify actions likely to result in unintended expenditures.

2.2 REACH for Tomorrow Board members, employees and contractual providers will receive training or education on federal and state False Claims Acts and Whistleblower Provisions.

2.3 REACH for Tomorrow Board members, employees and contractual providers are required to report any suspected occurrences of fraud, abuse and waste. The designated REACH for Tomorrow Compliance Officer will investigate the allegations and will assure that appropriate reporting occurs.

2.4 REACH for Tomorrow Compliance Officer will inform the Affiliation Compliance Administrator if incidents occur which require reporting to state or federal agencies or place REACH for Tomorrow in jeopardy.

3.0 HIPAA/HITECH Act Reporting, Investigation and Documentation

3.1 REACH for Tomorrow will comply with the Health Insurance Portability Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Subtitle D—Privacy, the Department of Health and Human Services (DHHS) security and privacy regulations, and Commission on Accreditation for Rehabilitation Facilities (CARF) accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. The following procedure will assist REACH for Tomorrow

in fulfilling its obligation under DHHS privacy regulations to mitigate damages caused by breach of individual privacy.

3.2 Reporting breaches: The purpose of reporting health information breaches, and suspected breaches, is as follows:

3.2.1. Minimize the frequency and severity of incidents.

3.2.2. Provide for early assessment and investigation before crucial evidence is gone.

3.2.3. Quickly take remedial actions to stop breaches, correct problems, and mitigate damages.

3.2.4. Implement measures to prevent recurrence of incidents.

3.2.5. Facilitate effective disciplinary actions against offenders.

3.2.6. Properly make required notifications.

3.3. Duty to Report: All employees, providers, contractors, persons served, interns, temporary staff of REACH for Tomorrow have a duty to report breaches and should feel free to report breaches without fear of retaliation.

3.4 Protection for those who Report: REACH for Tomorrow will not take any adverse personnel or other action against a person who reports actual or suspected breach of security, confidentiality or policies and procedures protecting the security and confidentiality of health information so long as the report is made in good faith.

3.4.1 Making a knowingly false report, however, may result in disciplinary action under REACH for Tomorrow policies and procedures.

3.4.2 Program directors and supervisors will ensure that the investigating officer has access to necessary persons and information to conduct a thorough investigation.

3.5 Investigation of a report

3.5.1 Upon receiving the report, the HIPAA Security or Privacy officer will take the following steps:

3.5.1.1 Take any necessary immediate corrective action.

3.5.1.2 If the breach appears to involve gross negligence, willful misconduct, or criminal activity of a person or persons holding access privileges, immediately, in conjunction with the CEO and/or HR Director, suspend that person's or those persons' access ending investigation, including taking all necessary steps to prevent access.

- In the case that the breach investigation involves the CEO the board chair will be contacted by the Compliance Officer for administration of this procedure.

3.5.1.3 Contact appropriate lawyers for consultation.

3.5.2 The CEO may appoint an investigating officer, which may be the HIPAA Security Officer, Privacy Officer, or Compliance Officer, to conduct an investigation in appropriate cases. Factors to consider in determining whether an investigation is necessary include the following:

3.5.2.1 Seriousness of the breach

3.5.2.2 Whether the breach involved unsecured (readable) or secured (not readable – that is encrypted or destroyed) data.

- Whether the breach resulted in actual harm.
- Extent of any harm.
- Whether the breach has the potential for legal liability.
- Whether the breach involved gross negligence, willful misconduct, or criminal activity.
- Whether the breach puts patients' or other individuals' welfare at risk.
- Whether a series of similar or related breaches has occurred.
- Whether the suspected offender has committed other breaches.
- Whether the breach must be reported to the individual who is the subject of the breach, to DHHS, and/or the media.
- In the case that the CEO is the subject of the investigation, the Board Chair will be contacted for appointing an investigating officer.

3.5.3. The investigating officer will conduct a thorough investigation into all the facts and circumstances of the breach or suspected breach and will provide the CEO (or board chair in the case that the CEO is the subject of the investigation) a detailed report of

the facts and circumstances of the breach, including recommendations for corrective action.

3.5.4. The investigation shall include a risk analysis of the breach, including, but not limited to, answering the following questions:

Who was involved?

How many patients'/others' information were breached?

Did the perpetrator improperly access the data or copy, change, or transfer the data?When did the breach happen?

What are the risks to the subject(s) of the breach?

What was the motive for the breach if not accidental?

Does the potential for further harm exist?

What can REACH for Tomorrow do to limit or eliminate further damage?

What steps can REACH for Tomorrow do to prevent this type of breach in the future?

3.5.5. HITECH Act

If the breach qualifies as a breach under the HITECH Act definition of breach in Subtitle D – Privacy, Part I, § 13400, the data is unsecured, and the breach poses a significant risk to the affected individuals, REACH for Tomorrow must, without unreasonable delay and in no case later than 60 days after the discovery of the breach, notify the individual(s) whose protected health information (PHI) was involved in the breach.

3.6 Documentation

3.6.1. The report and recommendations will be discussed with appropriate personnel and appropriate action to prevent recurrence of the breach, mitigate any harm caused by the breach, and necessary disciplinary action(s) will occur.

3.6.1.1. Provide copies of the report with an endorsement as to any corrective action taken, including suspensions of access, and recommendations for future action to all the following people and departments, as necessary and appropriate:

- CEO
- COO
- Directors, Managers and Supervisors

All reports will be kept for not less than 6 years from the date of the report.

No such report will be made a part of a patient's medical record. The report is a risk management tool.

3.7 Resolution

3.7.1. A breach notification must be provided without unreasonable delay, and in no case later than 60 days after the discovery of a breach.

3.7.1.1. The notice must include:

- Description of the types of unsecured PHI that were involved in the breach (i.e. Name, SSN, Patient ID, insurance number, date of birth, home address, disability code, etc.)

- Brief description of what REACH for Tomorrow is doing to investigate the breach to mitigate losses, and to protect against further breaches.

- Contact information for individuals to ask questions or learn additional information, which will include a toll-free telephone number, an email address, and/or postal address. The HIPAA Security Officer or HIPAA Privacy Officer shall respond to all such contacts.

3.7.1.2. The notification, unless the contact information is insufficient or out-of-date, shall be sent by first class, certified mail to the individual, guardian, legal representative or next-of kin of the individual or, if specified as a preference the individual, by email.

3.7.1.3. If the contact information is insufficient or out-of-date, REACH for Tomorrow will use a substitute form of notice, such as, if the breach involves 10 or more individuals for which there is insufficient or out-of-date information, a conspicuous posting on the home page website or notice in major print or broadcast media in geographic areas in which the individuals affected by the breach likely reside as determined by the HIPAA Security Officer in conjunction with legal and risk management administration. Such notice will include a toll-free number where the individual can learn whether the individual's unsecured PHI was possibly involved in the breach.

3.7.1.4. If the HIPAA Security or Privacy Officers, in consultation with the CEO or designee determines that the breach requires urgency because of the possible imminent release of unsecured PHI, immediate notification may also be made by telephone or other appropriate means.

3.7.2. If the breach involves 500 or more individuals' unsecured PHI, REACH for Tomorrow will provide notice, as required by HIPAA and the HITECH Act, to prominent media outlets in the state or jurisdiction of the individuals and immediately to DHHS.

3.7.2.1. The HIPAA Security Officer must report breaches of fewer than 500 individuals to DHHS not later than 60 days from the end of the calendar year in the form of a log.

3.7.2.2. Notifications may be delayed if law enforcement represents that the notification will impede a criminal investigation or damage national security.

4.0 Reporting Other Compliance Violations

4.1 Employees, interns, providers, contractors, persons served, and other individuals are to report suspected violations or potential misconduct to the Compliance Officer, by phone/voicemail, email, in person, in writing, through the reporting form or to one of the PIHP Affiliate Community Mental Health (CMH) Compliance Officers. A posting shall be placed at all REACH for Tomorrow offices with the applicable contact information of all PIHP Affiliate CMH Compliance Officers. A standard form shall be made available for individuals wanting to utilize a specific form to file a report in writing.

4.2 Reports made to PIHP Affiliate CMH Compliance Officers will be forwarded for investigation and follow up to the Compliance Officer, in which the potential/suspected violation was to have occurred.

4.3 Staff are expected to cooperate in the investigation of an alleged violation of the Compliance Plan or related policies.

4.4 FRAUD, WASTE AND ABUSE:

4.4.1. REACH for Tomorrow employees, interns, contractual providers and the provider network will report all suspected fraud, waste and/or abuse to the Compliance Officer. The report will include the nature of the complaint and the name of the individuals or entity involved in the suspected fraud and abuse, including address, phone number and Medicaid identification number if applicable.

5.0 Confidentiality

5.1 Individuals making a report are encouraged to disclose their identity, recognizing that anonymity may hamper complete and timely investigation. However, no anonymous report shall be refused or treated less seriously because the complainant/reporter wishes to remain anonymous.

5.2 No promises will be made to any individuals making a report or witnesses providing supporting information about the report by the Compliance Officer or anyone else in regard to his/her culpability or what steps may be taken by REACH for Tomorrow in response to the report.

5.3 Confidentiality and anonymity of the individual making the report and the content of the report will be preserved to the extent permitted by law and by the circumstances. Information about reports, investigations, or follow-up actions shall not be disclosed to anyone other than those individuals charged with responsibility in investigation and investigative findings as well as legal counsel.

6.0 Non-Retaliation

6.0 No employee, provider, contractor, person served, or other individual making such a report in good faith shall be retaliated against by REACH for Tomorrow employees or agents and will be protected by the OHIO Whistleblower's Protection Act.

6.1 Discipline for engaging in acts that violate applicable laws and regulations, making knowingly false reports, failure to report known violations, or discipline for any other performance-related reason unconnected to reporting potential violations is not retaliation.

7.0 Investigation

7.1 Within five business days of receiving a report, the Compliance Officer shall provide a written acknowledgement of receipt to the CEO and to the individual making the report (if known) and conduct an initial assessment to determine whether the report has merit and warrants further investigation.

7.2 If it is determined that the matter does not constitute a violation of any applicable laws or regulations and warrants no further action, the issue will be closed following the appropriate documentation and reporting by the Compliance Officer.

7.3 If it is determined that the matter does not constitute a violation of any applicable laws or regulations but does identify an area for improvement or raises concern for potential future violations, the matter will be

referred to the Quality Improvement Director or other appropriate parties for appropriate assignment and follow-up action.

7.4 If it is determined that the matter requires further investigation, the Compliance Officer shall take the necessary steps to assure that documents or other evidence are not altered or destroyed through the following possible means:

- Suspending normal record/documentation destruction procedures;
- Taking control of the files of individuals suspected of wrongdoing;
- Limiting access of files, computers, and other sources of documents by individuals suspected of wrongdoing; and/or
- Placing individuals under investigation on temporary suspension.

7.0 If the Compliance Officer concludes that reporting to a governmental agency (HCFA, OIG, DOJ) or a third party, may be appropriate, the CEO shall be informed immediately. Upon recommendation by legal counsel and with notice to the Board, the Compliance Officer, after review by CEO, shall make such a report to the appropriate government agency within 30 days after the determination that a violation has occurred.

7.1 Documentation retention and destruction must take place in accordance with the established REACH for Tomorrow Record Retention procedures. REACH for Tomorrow must retain all potentially responsive documents if it has been served with a government investigation. If REACH for Tomorrow is served with a subpoena or search warrant or has reason to believe a subpoena or search warrant may be served, the CEO is responsible for immediately directing staff to retain all documents that may be potentially responsive to the subpoena or search warrant.

7.2 When corporate compliance issues arise involving an investigation and potential legal consequences, the following questions should be asked:

- Should an internal investigation be conducted?
- Should legal counsel be contacted?
  - Legal counsel will be contacted after approval of the CEO is granted.
- Should disclosure be made to the appropriate government agency?
- Does the staff person need separate counsel?

7.3 If the CEO is the subject of a subpoena or search warrant the CEO and Corporate Compliance Officer shall each contact the President of the Board who will be responsible for the administration of this procedure.

7.4 A full investigation shall be completed within 90 days from the date of the initial report. An extension may be granted by the Compliance Committee.

8.0 Documentation

A record shall be maintained by the Compliance Officer or designee for all reports of potential/alleged violations utilizing the attached Compliance Investigation Report form. The record may also include copies of interview notes and documents reviewed and any other documentation as appropriate.

9.0 Resolution

Following the investigation, the Compliance Officer shall document and report the findings of the investigation to the CEO and Compliance Committee. In cases where actions of the CEO are investigated, the report of findings is made to the Board President.

If appropriate, a remedial action plan shall be developed to address any confirmed violations or address areas of concerns raised during the investigation.

If appropriate, disciplinary action shall be taken in accordance with the organization's disciplinary policies and procedures.