

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Name:** | **HIPAA Breach Reporting** | **Date Revised:** | **2/2020** |
| **Purpose:** | **Protocol Responding to a Breach of Confidentiality, Privacy and/or Security of Protected Health Information (PHI)** | **Board Approval:** |  |

**Policy:**

It is the policy of Greater New Beginnings (GNB) to assure the privacy, security and confidentiality of individually identifiable client information and other non-public information in accordance with federal, state and agency requirements. Complaints of suspected breaches of privacy, security and confidentiality by members of the workforce and Business Associates may be filed directly with GNB’s Privacy Officer or directly to the County. Instances of breach of confidentiality will be dealt with in accordance with federal, state and agency regulations.

A breach of confidentiality, privacy and/or security of individually identifiable client information is a violation of Greater New Beginnings policy. A breach occurs when unauthorized persons gain (or are given) access to protected client information whether or not the unauthorized person uses or discloses the information. This policy applies to all forms of protected records created, received, sent and/or stored by GNB.

**Procedure:**

A breach of privacy, security and/or confidentiality may result in harm whether or not it was intentional. It is a serious event that must be remedied as quickly as possible.

1. Workforce Members
   1. Workforce members who receive a complaint or encounter an actual (or potential) breach of confidentiality must take appropriate action to temporarily secure the breach and then report the circumstances to their immediate supervisor.
   2. If their supervisor is unavailable, they are required to report the situation to the next higher level of supervision.
2. Investigation, Mitigation and Risk Management by the Quality Assurance Compliance Manager
   1. The QA Compliance Manager or designee performs an investigation and evaluation of the suspected breach. The Manager or designee must assure that the following minimum activities are accomplished:
      1. Evaluate temporary measures initially used to secure the breach. When appropriate, add additional measures to mitigate harm that may have occurred as a result of the use or disclosure of PHI in violation of policy and procedure or requirements of regulations.
      2. Conduct fact-finding activities and evaluate the validity and potential impact (risk) of the suspected breach to the extent practicable.
      3. If an intentional breach is suspected, contact the Human Resource Department for guidance on how to proceed with the investigation. Subsequent management actions will take into consideration such factors as the seriousness of the breach, whether it was intentional or unintentional, and the past record of the offender(s).
      4. Take appropriate action to resolve the breach and prevent future occurrences.
      5. Make required reports and notifications.
      6. Develop an action plan for preventing future occurrences.
      7. Report the incident to the Privacy Officer within one working day, regardless of findings.
3. Investigation and Reporting by the Privacy Officer (or designee)
   1. The Privacy Officer will receive the report and take appropriate action depending upon the nature (and broader implications) of the suspected breach. If the suspected breach appears to be limited to the area of responsibility of the reporting QA Compliance Manager (and has been appropriately resolved), the Privacy Officer ends the process and documents the Manager’s report.
   2. If the complaint appears to be valid and/or appears to have implications beyond the initial program, the Privacy Officer will research the facts of the broader event. Depending upon the nature of initial findings, the Privacy Officer will consult with the Executive Director regarding the event and enlist assistance with the independent investigation.
   3. If a breach has occurred, the Privacy Officer and Executive Director will agree upon system-wide recommendations based upon the nature, severity and impact of the breach. In instances of serious breaches, the Privacy Officer will request a written plan of correction.
4. Management Responses: Sanctions and Other Consequences for a Breach of Confidentiality
   1. All members of the workforce are required to comply with federal, state, county and Greater New Beginnings’ regulations.
   2. Corrective actions for breaches of privacy, security or confidentiality by workforce members are the responsibility of program management.
   3. Sanctions for confirmed breaches may range from a warning up to job termination, depending on the circumstances of the breach.
5. Responsibility
   1. The Privacy Officer has overall responsibility for the orientation and training of the workforce in policies and procedures related to the privacy, security and confidentiality of protected health information.
   2. The Privacy Officer is available for consultation upon request.
6. Coordination
   1. The Privacy Officer investigates and coordinates situations that appear to have implications beyond the boundaries of the program where the initial complaint was made.
7. Monitoring and Reporting
   1. The Privacy Officer is required to monitor the number, type and disposition of complaints and report findings at least quarterly.
   2. The Privacy Officer will prepare an annual analysis of findings.