

ASSIGNMENT OF SECURITY RESPONSIBILITY POLICY

RESPONSIBILITY: Security Official

BACKGROUND:

The final federal regulations relating to the security of protected health information (PHI) do not require an assigned security title, but an assigned security responsibility. Assigned security responsibility refers to practices put in place to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data. This stops short of requiring a designated security official, and differs in this respect from the federal privacy rules, which require a designated Privacy Official or Designee(s). However, the appointment of a Chief Security Official is highly recommended. A critical part of the success of any plan or program is the designation of specialized personnel to oversee its development and execution.

The person assigned security responsibility should be a member of the Information Systems staff, with special knowledge and training in the administration and execution of a security management process which covers contingency (disaster) planning, access controls, audit controls, personnel security and training, incident reporting and remediation, as well as overseeing the physical and technical safeguards necessary to guard data integrity, confidentiality, and availability.

If no one is assigned security responsibility, then this policy must be modified to document how the requirement for an assigned security responsibility will be met.

POLICY:

Behavioral Health and Health Facilities (BHHF) recognizes the importance of specialized oversight for the development and implementation of the organization's security responsibilities. For this purpose, a Security Official shall be designated with the assigned responsibility to manage and supervise the execution and use of security measures to protect BHHF data and to manage and supervise personnel in relation to the protection of this data. The Security Official's duties shall include, but not be limited to, the following:

1. Oversee process for systems certification: The technical evaluation that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.
2. Coordinate development and execution of the BHHF contingency plan: A contingency plan must include
 - 2.1. Applications and data criticality analysis,
 - 2.2. A data backup plan,

- 2.3. A disaster recovery plan,
 - 2.4. An emergency mode operation plan, and
 - 2.5. Testing and revision procedures.
3. Unify and oversee information access control standards.
 - Access refers to the ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource
 - Access control refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day access, and classification or role-based access.
 4. Monitor internal audit controls of system records activity, and respond to variances. Audit controls refer to mechanisms to record and examine system activity. This includes recording pertinent data relating to the creation, modification, transmission, and deletion of records, and access to sensitive records. Sensitive records include records of employees and VIPs, or records of patients with protected diagnoses such as HIV or mental illness. Audit controls may also include procedures to monitor access to a statistical sample of all records. Audit controls allow an organization to identify suspect data activities, and respond to potential weaknesses.
 5. Maintain personnel authorization controls and clearance records. Authorization controls refers to a mechanism for obtaining consent within the system for the use and disclosure of health information. These controls may be role-based or user-based.
 6. Oversee Security Configuration Management: The integration process to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses.
 7. Oversee Security Incident procedures. Security Incident Procedures refers to the requirement to implement formal, documented instructions for reporting and responding to security breaches.
 8. Develop and oversee the Security Management Process including Risk Analysis and Risk Management provisions. Security Management Process refers to creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. The requirement for this process includes the use of risk analysis and risk management, and must include formal security and sanction policies.
 9. Coordinate termination and/or modification of access to information systems.
 10. Provide technical assistance for universal security awareness training.
 11. Develop and oversee Media Controls: The requirement for formal, documented policies and procedures that govern the receipt and removal of data storage media

