Roles and Responsibilities of an Information Security Officer

Purpose: On behalf of the _____________ County Health Department, the Security Officer (SO) will serve as the focal point for security compliance related activities and responsibilities as listed below. The SO is generally responsible for obtaining or developing the Health Departments policies and procedures for submission to the Board of Health for approval/adoption. The SO is also responsible for maintaining the health department policies and procedures, reviewing the conduct of those assigned to specific security duties, as well as administering the reviews relating to the over all security program. The SO is also responsible for ensuring that educational programs are conducted to enhance the general security awareness.

The SO serves as a resource regarding matters of information security and reports the status of ongoing information security activities to the designated person(s).

Responsibilities:

1. Lead in the development/adoption and enforcement of Information Security policies, procedures and standards. Conduct and complete an annual review of required HIPAA regulations and reports.

2. Maintain the Agency’s Security Policies. These are formal policies that detail and document actual mechanisms and controls and should include at least the following:
   - Administrative: Risk analysis and management, documentation management and controls, information access controls and sanctions for failure to comply.
   - Personnel Security: Personnel only have access to the sensitive information for which they have appropriate authority and clearance.
   - Physical Safeguards: Assign security responsibilities, control access to media and the controls in place against unauthorized access to workstations and related equipment.
   - Technical Security: Set the access and authorization controls for everyday operations as well as emergency procedures for data.
   - Transmission security: Set the standards for access controls, audit trails, event reporting, encryption and integrity controls.

3. Maintain the Agency’s Security Procedures that include:
   - Evaluation and compliance with security measures.
   - Disaster Recovery and Emergency operating procedures.
   - Security Incident Response and process protocols including Incident Reporting and Sanctions.
   - Testing of security procedures, mechanisms and measures.

4. Maintain appropriate security measures and mechanisms to guard against unauthorized access to electronically stored and /or transmitted patient data and protect against reasonably anticipated threats and hazards.
5. Oversee and/or assist in performing on-going security monitoring of organization information systems including:

- Assess information security risk periodically.
- Conduct functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements.
- Evaluate and recommend new information security technologies and counter-measures against threats to information or privacy.

6. Ensure compliance through adequate training programs and periodic security audits. These audits should be both internal and external in nature.