Georgia Department of Public Health

Form GC-09013F

GEORGIA DEPARTMENT OF PUBLIC HEALTH
SAFEGUARDS FOR THE PROTECTION OF
ELECTRONIC PERSONAL HEALTH INFORMATION

The Department must ensure the confidentiality, integrity and availability of all electronic PHI that it creates, receives, maintains or transmits, must protect against any reasonably anticipated threats or hazards to the security or integrity of such information, and must protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA regulations.

The Department may use any security measures that allow it to reasonably and appropriately implement the standards and specifications required by HIPAA. In deciding which security measures to use, the Department shall take into account its size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; the cost of security measures; and the probability and criticality of potential risks to electronic PHI.

Administrative Safeguards

1. **Security Management.** The Department shall prevent, detect, contain, and correct security violations, and shall do the following:

    a. **Risk Analysis.** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the Department;
    b. **Risk Management.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the requirements contained in the introductory paragraphs above;
    c. **Periodic Review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. **Security Officer.** The DPH Chief Information Officer shall designate a member of his or her staff to serve as Security Officer, to be responsible for the development and implementation of the information security policies and procedures required by this Form to ensure compliance with HIPAA security regulations.

3. **Workforce Security.** The Security Officer must implement policies and procedures to ensure that employees only have such access to electronic PHI as is appropriate for their duties, and to prevent other employees from obtaining access to electronic PHI, including the following:

    a. **Authorization and Supervision.** Implement procedures for the authorization and supervision of employees who work with electronic PHI, or in locations where it might be accessed;
    b. **Workforce Clearance.** Implement procedures to determine that the access of an employee to electronic PHI is appropriate;
    c. **Termination of access.** Implement procedures for terminating access to electronic PHI when the employment of an employee ends.

4. **Information Access Management**. The Security Officer must implement policies and procedures for authorizing access to electronic PHI that are consistent with HIPAA requirements, including the following:

    a. **Access Authorization.** Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, program, process or other means;
    b. **Access Establishment and Modification.** Implement policies and procedures that, based upon the Department's access authorization policies, establish, document, review and modify a user's right of access to a workstation, program or process.
    c. **Security Reminders.** Provide periodic security updates as needed;
    d. **Malicious Software.** Implement procedures for guarding against, detecting, and reporting malicious software;
    e. **Log-in Monitoring.** Implement procedures for monitoring log-in attempts and reporting discrepancies;
    f. **Password Management.** Implement procedures for creating, changing, and safeguarding passwords.

5. **Contingency Plan**. The Security Officer must establish and implement as necessary, policies and procedures for responding to an emergency or other occurrence that damages a system containing electronic PHI, including the following:

    a. **Data Backup Plan.** Establish and implement procedures for a data back-up plan, to create and maintain retrievable exact copies of electronic PHI;
    b. **Disaster Recovery Plan.** Establish and implement procedures as needed, for a disaster recovery plan to restore any loss of data;
    c. **Emergency Mode Operation Plan.** Establish and implement procedures as needed, for an emergency mode operation plan, to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
    d. **Testing and Revision.** Implement procedures for periodic testing and revision of contingency plans.
    e. **Application and Data Criticality Analysis.** Assess the relative criticality of specific applications and data in support of other contingency plan components.

6. **Evaluation**. The Security Officer must perform a periodic technical evaluation to ensure that Department security polices and procedures meet the requirements of this Policy.

Physical Safeguards

1. **Facility Access Controls.** The Security Officer must implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, but ensure that authorized access is allowed, including the following:

    a. **Contingency Operations:** Establish and implement procedures as necessary that allow facility access to support the restoration of lost data under the disaster recovery and emergency mode operations plans in the event of an emergency;

    b. **Facility Security Plan:** Implement policies and procedures to safeguard the facility and its equipment from unauthorized physical access, tampering, and theft;

c. **Access Control and Validation:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and to control access to software programs for testing and revision;
d. **Maintenance Records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility related to security (*e.g.*, walls, hardware, doors, and locks).

2. **Workstation Use**. The Security Officer must implement policies and procedures that specify the proper functions to be performed, the way in which these functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI.

3. **Workstation Security**. The Security Officer must implement physical safeguards for all workstations that access electronic PHI, to restrict access by unauthorized users.

4. **Device and Media Controls**. The Security Officer must implement policies and procedures for the receipt and removal of hardware and electronic media containing electronic PHI into and out of a facility, as well as the movement of these items within a facility, including the following:

a. **Disposal.** Implement policies and procedures to address the final disposition of electronic PHI, and the hardware or electronic media that stores it;
b. **Re-Use of Media.** Implement procedures for removal of electronic PHI from electronic media prior to the media being made available for re-use.
c. **Accountability.** Maintain a record of the movements of hardware and electronic media and anyone person responsible for such movements;
d. **Data Back-up and Storage.** Create a retrievable, exact copy of electronic PHI, when needed, before moving equipment.

Technical Safeguards

1. **Access Control**. The Security Officer must implement technical policies and procedures for information systems that maintain electronic PHI, which allow access only by those persons or software programs that have access rights, including the following:

a. **Unique User ID.** Assign a unique name or number for tracking and identifying user identity;
b. **Emergency Access Procedure.** Establish and implement procedures as needed to obtain necessary electronic PHI during an emergency.
c. **Automatic Log-off.** Implement procedures to terminate an electronic session after a certain period of inactivity;
d. **Encryption.** Implement a mechanism to encrypt and decrypt electronic PHI.

2. **Audit Controls**. The Security Officer must implement hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

3. **Integrity**. The Security Officer must implement policies and procedures to protect electronic PHI from improper alteration or destruction, and to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

4. **Person or Entity Authentication**. The Security Officer must implement procedures to verify that a person or entity seeking to access electronic PHI is the one claimed.

5. **Transmission Security**. The Security Officer must implement technical security measures to guard against unauthorized access to electronic PHI being transmitted over an electronic communications network, including the following:

    a. Integrity Controls. Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified during transmission;
    b. Encryption. Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.

Documentation

The Security Officer must maintain the policies and procedures implemented to comply with this section in written format. A copy must be provided to the Privacy Officer. The documentation must be reviewed periodically and updated as needed due to environmental or operational changes affecting the security of electronic PHI. Procedures followed in the event of a security incident and the outcome must also be documented. The documentation must be kept for six years from the date of its creation or the date when it was last in effect, whichever is later.