Georgia Department of Public Health

Form GC-09013E

GEORGIA DEPARTMENT OF PUBLIC HEALTH
PERSONAL HEALTH INFORMATION SECURITY
INCIDENT RESPONSE PROTOCOL

This protocol sets out the procedures for responding to an actual or suspected personal health information security incident, and the responsibilities of persons tasked to respond to such incidents.

A **Security Incident** is an actual, suspected, or attempted loss or disclosure of individually identifiable personal health information within the custody or control of a DPH or County Board of Health employee. A Security Incident can take place in many different ways: the loss of a disk or laptop computer containing PHI, a malfunction or unauthorized attempt to enter into an information system on which PHI is stored, disclosure of PHI by email or telephone to the wrong person, an unauthorized modification or destruction of data, leaving papers with PHI in plain sight in a common area, etc.

A Security Incident shall be declared to be a **Breach** if protected health information was acquired, accessed, used, lost, or disclosed in a manner not permitted under HIPAA or other privacy laws, unless an investigation and risk assessment show that there is a low probability that the information was actually compromised.

The **Security Incident Response Team** consists of the DPH Privacy Officer and the DPH Information Security Officer. Depending on the circumstances of the incident, they may request the support of the Director of Communications or the Inspector General. If the Security Incident involves PHI within the custody of a county or District office, then the District Privacy Officer and District MIS Director will be on the Response Team.

Step One: Investigation.

Any event that might possibly be a Security Incident shall be reported immediately to the Privacy Officer or Information Security Officer. The Security Incident Response Team shall immediately investigate the event, including personal interviews of any person who might have knowledge of the facts, and shall include the Director of Communications and Inspector General if necessary.

At the conclusion of the investigation, the Response Team shall decide whether there has been a Breach. The incident shall not be considered a Breach in the following circumstances:

- The acquisition, access, or use of the PHI was by a DPH employee or business associate in good faith and within the scope of their authority, and there was no further use or disclosure in violation of HIPAA;

- An inadvertent disclosure of PHI was made by a DPH employee or business associate authorized to access PHI to another DPH employee or business associate authorized to access PHI, and there was no further use or disclosure in violation of HIPAA;

- The PHI was disclosed to an unauthorized recipient, but there is a good faith belief that the recipient would not reasonably have been able to retain the PHI; or

- A risk assessment of the following factors by the Security Incident Response Team shows that there is a low probability that the PHI was compromised:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.

Step Two: Response.

Regardless of whether or not the Security Incident is deemed to be a Breach, the Security Incident Response Team shall develop and implement a plan to accomplish the following:

- Ensure that the conditions that made the incident possible are corrected so as to prevent future incidents. This may include recommendations for further training of employees, or changes to office technology, training, policy, or procedures.

- Identify individuals whose PHI was or may have been disclosed, and the persons or entities to whom PHI was or may have been disclosed.

- Mitigate any possible harm that may have resulted from the incident.

- Recommendations to the Office of Human Resources or District Health Director for disciplinary actions against persons responsible for the incident, if warranted.

Step Three: Notifications.

If the Security Incident Response Team determines that there has been a Breach, then the Privacy Officer will advise on how to provide notice of Breach as required by law.

1. **To Affected Individuals**: Notice of a Breach shall be given to each affected individual. The Privacy Officer will prepare the notice in accordance with 45 CFR 164.404(c), and the program will be responsible to ensure that the notices are sent. The notice shall be written in plain language and contain the following:

    - The date of breach, the date it was discovered, and a brief description of what happened;
    - A description of the types of PHI that were involved (*e.g.,* full name, Social Security number, date of birth, home address, account numbers, diagnoses, disability codes, etc.);
    - Any steps that individuals should take to protect themselves from potential harm resulting from the breach;
    - A description of what DPH is doing to investigate the breach, mitigate harm to

individuals, and protect against further breaches; and
- Contact information for individuals to ask questions or learn additional information, such as an email address, website, or mailing address.

The notice shall be sent by first-class mail to each individual's last known address; by email, if the individual has agreed to electronic notice; or to the next of kin or personal representative, if deceased. The Privacy Officer may approve another form of notice in accordance with 45 CFR 164.406 if the contact information for an individual or group of individuals is insufficient or out-of-date.

2. **To Others:** If there are more than 500 affected individuals, then the Privacy Officer shall prepare a notice of the Breach for the Director of Communications to distribute to prominent media outlets serving Georgia no later than sixty days from discovery of the Breach. In addition, the Privacy Officer will provide notice to the Secretary of the U. S. Department of Health and Human Services as required by 45 CFR 164.408 contemporaneously with the notice to individuals, but no later than sixty days after discovery of the breach.

Step Four: Documentation.

At the conclusion of every investigation, the Privacy Officer shall ensure that a file is prepared and maintained to document the facts of the incident, the basis for the determination that there was or was not a Breach, the response, and proof that all notices required by law were made.