



**SHELBY COUNTY GOVERNMENT
(HEALTH CARE COMPONENT)**

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY
Notification of Breach of “Unsecured” Protected Health Information (PHI)**

Policy #	Supersedes Policy
Approved By	Effective Date
HSC _____ Date _____	Review Date
ED _____ Date _____	Revision Date

SCOPE: This policy applies to all workforce members of (insert name) and Shelby County Government (SCG) divisions that receive, maintain or transport protected health information on behalf of the Shelby County Government designated HIPAA health care components. This policy’s scope includes all protected health information, as described in the HIPAA Privacy and Security Rules and HITECH regulation.

PURPOSE: Shelby County Government is a hybrid HIPAA covered entity that is required by law to protect the privacy of individuals’ health information. SCG must notify individuals and certain entities regarding a breach of protected health information not secured according to the National Institute Standards for Technology adopted by HITECH regulation. In accordance with regulatory requirements, if a breach of “unsecured” protected health information occurs SCG must notify the individual and certain entities. The purpose of this policy is to establish a procedure for notifying the appropriate individuals and entities if such breach should occur

DEFINITION: Breach: For the purposes of the policy, the term “breach” means the acquisition, access, use or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy and Security Rule which compromises the security or privacy of the protected health information. The term “protected health information” means any information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

POLICY: It is the responsibility of SCG to protect and preserve the confidentiality of all protected information held by the County or other entities on its behalf. In an effort to minimize breach related risks, SCG has implemented administrative, physical and technical safeguards to protect the health information entrusted to the County. Employees will be trained regarding their responsibility for reporting suspected breaches. In an effort to minimize financial, reputation or other harm to the affected individuals, employees are required to report the privacy breaches to

the Privacy Officer and to report security/system related breaches to the Security Officer. The Privacy and Security Officer will be responsible for investigating suspected breaches in their respective HIPAA task related area. Upon completion of the investigation, the Privacy or Security Officer will notify the individual (s) and appropriate entities of cases determined to be breaches.

Procedure

1. Any member of SCG's Health Care Components or divisions and departments that handles protected health information on behalf of the Health Care Component who knows, believes, or suspects that a breach of protected health information has occurred must report the breach immediately to the Privacy or Security Officer.
2. The employee discovering the breach must follow any available precautions to contain the breached information from further harm while waiting on the Privacy or Security Officer immediate response.
3. The Privacy Officer and Security Officer will investigate and resolve privacy breaches and computer security breaches, respectively.
4. After a potential breach is reported, the Privacy and/or Security Officer will work with other officials and departments, including the Compliance Officer and HIPAA Attorney if necessary, to conduct a thorough investigation, which includes an assessment to determine whether a breach of unsecured protected health information under the HITECH regulation occurred and if so, what notifications are required. The Privacy or Security Officer should promptly complete its investigation within twenty (20) calendar days to ensure sufficient time for the preparation and coordination of notifications.
5. If the Privacy or Security Officer determines that there is no impermissible acquisition, access, use or disclosure of unsecured protected health information the investigating officer must note it in the comment section of the Breach Assessment Tool and Breach Reporting Form.
6. The investigating officer must maintain a copy of the Breach Assessment Tool and Breach Reporting Form and all documents related to the breach notification for six (6) years from the date it was created or the date it was last in effect, whichever is later.
7. The Privacy and Security Officers and departments that handle protected health information on behalf of the health care component must report breaches of five hundred (500) or more immediately to the Compliance Officer for reporting to the Department of Health and Human Services.
8. Each Health Care Component and departments that handle protected health information on behalf of the health care component must maintain a Breach Notification Log during a calendar year. The Breach Notification Log must be submitted to the Compliance Officer no later than December 31st of each year.

Notification

Individual Notification

1. Upon completion of the investigation of the breach, the investigating officer shall provide written notice immediately, not more than sixty (60) days for the date of discovery to the individual or:
 - a. If the individual is deceased, to the next of kin or personal representative.
 - b. If the individual is incapacitated/incompetent, to the personal representative.
 - c. If the individual is a minor, to the parent or guardian.(See guidelines in the HIPAA Verification of Identity for Disclosure Policy prior to Releasing information someone other than the individual)
2. The written notification must be in plain language at an appropriate reading level and must meet Limited English Proficiency (LEP) requirements.
3. Written notification will be sent to the last known address of the individual or next of kin, or if specified by the individual, by electronic mail. The template letter in the Breach Notification Reporting Process must be used when sending written notification to an individual, personal representative, next of kin or parent.
4. If SCG determines the individual should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, SCG will, in addition to providing notice as outlined above, contact the individual by telephone or other means, as appropriate.

Content of the Notification

The notification will include the following information relative to the breach:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach, such as full name, social security number, date of birth, home address, account number, diagnosis code or disability code.
3. The steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

Substitute Notice

1. In the case where there is insufficient or out-of-date contact information that preclude written communication, a substitute notice will be provided accordingly:
 - a. SCG will post a conspicuous notice for ninety (90) days on the homepage of our website that includes a toll-free number; or
 - b. SCG will provide notice in major print or broadcast media that serves Shelby County where an individual can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number will be included in the notice.

Media Notification

1. In the case where a single breach event affects more than five hundred (500) residents of Shelby County or the affected service area, the Compliance Officer will work with the Public Relations Department to develop a press release to submit to prominent media outlets in this area.

Health and Human Services (HHS) Notification

1. The Compliance Officer will provide electronic notice without unreasonable delay and in no case later than sixty (60) days from the breach discovery to the Secretary of the HHS if a single breach event was with respect to five hundred (500) or more individuals. The Compliance Officer shall submit a copy to the Chief Administrative Officer prior to submission to HHS.
2. The Compliance Officer will submit electronic notification to the HHS office breaches of less than 500 annually and no later than 60 days after the end of the calendar year. The Compliance Officer shall submit a copy to the Chief Administrative Officer prior to submission to HHS.

Delay of Notification for Law Enforcement Purposes

1. If a law enforcement official informs SCG that a notice or posting would impede a criminal investigation or cause damage to national security, SCG will delay the notice as follows:
 - a. If the request is made in person, the requestor must present an agency identification badge, other official credentials, or other proof of government status;
 - b. If the request is in writing, the request must be submitted on the appropriate government agency letterhead; or
 - c. If the request is made via telephone, the SCG representative will note it in the file and request that the caller submit a written request. If a written request is not received in thirty (30) days, the SCG representative may release the breached information for notification to the individual and appropriate agencies.
 - d. Documentation of the request must be noted in the file along with proof of identify of the government agency.

RESPONSIBLE PARTIES

Shelby County Government's Compliance Officer holds the chief responsibility of monitoring HIPAA compliance of each health care component. The administrative/management team of each health care component must ensure that departments under their direction adhere to this policy. The Privacy and Security Officers are responsible for monitoring and enforcement of this policy in accordance with the areas of their respective HIPAA compliant duties.

ENFORCEMENT

Employees violating this policy will be subject to the appropriate disciplinary process up to an including termination of employment.

REFERENCE

45 C.F.R. 164.404
164.406
164.408