	Department of Human Services Online Directives Information System	**Index:** **Effective:** **Review:**	**POL1660** **01/1/2016** **11/07/2016**

DATA BREACH RESPONSE POLICY

EFFECTIVE DATE: January 1, 2016 **PUBLISHED DATE:** January 1, 2016
REVISED:

Policy

The Health Insurance Portability and Accountability Act of 1996, as modified by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HIPAA"), established Federal standards for safeguarding the privacy of individually identifiable health information. HIPAA mandates rigorous compliance with the requirements for the use and/or disclosure of protected health information.

Additionally, Georgia enacted the Georgia Personal Identity Protection Act (GPIPA) of 2005 in an effort to protect individuals from the growing threat of identity theft caused by data breaches. GPIPA was expanded in 2007 to include state agencies as a requirement to comply with GPIPA.

In strict compliance with the requirements of HIPAA, GPIPA and other mandatory data breach protocols, as set forth herein, it is the policy of the Georgia Department of Human Services ("DHS") that any data breach be reported internally within DHS and investigated, in accordance with applicable law, in order to determine and mitigate any potential harm. The purpose of the Data Breach Response Policy is to require all DHS divisions, offices, and sections thereof, including, but not limited to, HIPAA-covered functions, to complete a Data Breach Incident Reporting Form to determine whether an incident is a breach of protected health information ("PHI") or personally identifiable information ("PII").

I. Authority

Georgia Personal Identity Protection Act (GPIPA) (O.C.G.A. §10-1-910, et. seq.)

The Privacy Act of 1974 (5 U.S.C. 552a)

Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 C.F.R. Parts 160 and 164)

Health Information Technology for Economic and Clinical Health Act (HITECH) (2009) (42 U.S.C. § 300jj et seq.)

II. Applicability

A. This policy applies to all DHS employees, management, contractors, student interns, leased employees, volunteers and any other personnel that may have access to data of which DHS is the custodian.

B. This policy describes DHS' objectives, policies, and responsibilities regarding reports of suspected or known data breaches.

III. Definitions

Access: the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach: the unauthorized and/or impermissible acquisition, access, use, or disclosure of protected health information or unsecured personally identifiable information which compromises the security or privacy of such information.

Management: authoritative personnel within the department including but not limited to the commissioner, deputy commissioner(s), and divisional directors.

Personally Identifiable Information: any information about an individual maintained by DHS, including:

1. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Protected Health Information: information that is created or received by a health care provider, health plan, employer, or health care clearinghouse that identifies an individual or provides a reasonable basis to believe the information can be used to identify the individual and that relates to:

1. The past, present, or future physical or mental health or condition of an individual;
2. The provision of health care to an individual; or
3. The past, present, or future payment for the provision of health care to an individual.

IV. Implementation

A. DHS Management responsibilities

1. Establish a cross-functional incident response team to prevent, investigate and mitigate any suspected or known breaches of PHI and PII (the "Data Breach Task Force" or "DBTF").
2. Approve policy and necessary procedures to become compliant and maintain compliance with all breach notification regulations.
3. Provide privacy and security training and updates for workforce and ensure compliance with training schedules.
4. Enforce sanctions, if necessary, against any employee, staff or contractor who does not comply with this policy.
5. Designate a Privacy Officer.

B. Employee responsibilities

1. Understand and comply with organization's policies and procedures regarding confidentiality, privacy and security of all DHS data.
2. Report any suspected or known breach of personal identifying information (PII) or protected health information (PHI) of which DHS is the custodian.
3. Complete all mandatory training, as assigned.

V. Procedure

A. Reporting

All potential data breaches are to be immediately reported to the DHS Privacy Officer as soon as a breach is suspected or discovered. If the DHS Privacy Officer is not available then the breach should be reported to the General Counsel, Deputy General Counsel or the Associate General Counsel associated with the Division that is the custodian of the data suspected of being breached. A written report detailing the known or suspected facts involving the breach is the preferred method of reporting, however depending on the urgency of the circumstances, alternative means of reporting the breach are acceptable but should be followed up with a written report within two (2) business days of discovering the breach. The breach is to be reported using **the Data Breach Incident Reporting Form** (Attachment A).

B. Investigation

1. The DHS Privacy officer will perform a risk analysis assessing the following factors to determine whether the PHI or PII at issue has been compromised:

a. The nature and extent of the PHI or PII involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the PHI or PII or to whom the disclosure was made;
c. Whether PHI or PII was actually acquired or viewed; and
d. The extent to which the risk to the PHI or PII has been mitigated.

The results of the incident investigation will determine the actions to be taken.

2. Depending on the analysis by the DHS Privacy Officer or a representative substitute, the Privacy Officer will determine:

    a. If the event meets the criteria of a breach, and, if applicable,
    b. The type of breach and the subsequent regulatory reporting protocols that must be followed, i.e., HIPAA, Privacy Act, Social Security Act, FNS, etc.

Once it is determined that a breach either has occurred or if it can reasonably be expected that a breach may have occurred or is continuing to occur, the Privacy Officer will alert the Data Breach Task Force (DBTF).

C. Response

Upon review of the incident and regardless of whether or not PHI or PII is breached, the DBTF shall develop and implement a plan to accomplish the following:

1. 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.
2. Identify individuals whose PHI or PII was or may have been disclosed, and the persons or entities to whom PHI or PII was or may have been disclosed.
3. Mitigate any possible harm that may have resulted from the incident.

D. Notification

Upon determination and mitigation of the breach, the DBTF will take necessary steps to adhere to all noticing requirements for the individuals' whose information was compromised and comply with all noticing requirements, of applicable, regulatory agencies, as required by statute, rules or regulation. The DBTF will follow the appropriate DHS procedures consistent with the type of data or information that has been disclosed including but not limited to any of the following or any combination of the following:

1. HIPAA Data Breach Protocol

2. Privacy Act Data Breach Protocol
3. Social Security Act Data Breach Protocol
4. Georgia Personal Identity Protection Act (GPIPA) Protocol
5. IRS Data Breach Protocol
6. OCSE Data Breach Protocol
7. FNS Data Breach Protocol
8. Any other contractual Data Breach Requirements (e.g., Accurint, etc.)

The DBTF will also provide guidance on how to prevent additional breaches from occurring in the future and any remedial efforts that are recommended.

E. Documentation

DHS, through its Privacy Officer, will keep a record of each reported breach in compliance with applicable regulations or requirements. If no time is prescribed for records retention, then for a reasonable period not to exceed five (5) years from when the breach is discovered.

VI. Administrative Requirements

A. Training

DHS shall train all members of the DHS workforce with respect to breach reporting obligations and procedures annually, so employees are able to identify suspected breaches of protected health information and personally identifiable information and know how to immediately report all suspected breaches to the Privacy Officer. Evidence of employees receiving this annual training shall be documented and maintained.

1. New staff member training: New staff members will be trained on data security awareness and HIPAA training (Privacy and Security Training) within a reasonable time period after their hire date with the department.
2. Recurrent training: Staff members are to be trained on Privacy and Security Training as a refresher within a reasonable time and no less than annually. Please refer to the Privacy and Security Training Protocol for guidance on the most current training and frequency of training.
3. Special function training: Staff members are to be trained on Privacy and Security Training within three months after substantive changes are made to this policy or as necessary.

B. Sanctions

DHS expects that all employees will comply with all laws, regulations, standards, policies, procedures, guidelines and expectations regarding the privacy and security of DHS protected health information and personally identifiable information, including, but not limited to protected health information and personally identifiable information. Applicable consequences of non-compliance with this policy may include reprimand, suspension, removal, or other actions in accordance with applicable law and DHS policy. The minimum consequence DHS may consider is prompt removal of authority to access information or systems from individuals who demonstrates egregious disregard or a pattern of error in safeguarding personally identifiable information and/or protected health information.

C. Additional Information

For additional information or assistance, please contact the Office of General Counsel.

VII. Authentication

_____ _____

Commissioner Date