	Department of Human Services **Online Directives Information System**	**Index:** **Revised:** **Next Review:**	**POL1660** **03/22/2020** **03/22/2021**

SUBJECT: DATA BREACH RESPONSE POLICY

POLICY:

The policy of the Department of Human Services (DHS) is to follow state and federal laws regarding the privacy and security of personal information. In particular, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as modified by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") established Federal standards for safeguarding the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without authorization. HIPAA mandates rigorous compliance with the requirements for the use and/or disclosure of protected health information ("PHI").

Additionally, Georgia enacted the Georgia Personal Identity Protection Act ("GPIPA") of 2005 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 confidentiality laws and regulations, as set forth herein, it is the policy of the Georgia Department of Human Services that any known or suspected unauthorized access or disclosure of information be reported internally within DHS to the Privacy Officer and investigated, in accordance with applicable law, in order to evaluate the circumstances and risk to the disclosed information and 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, any HIPAA-covered functions, to complete a Data Breach Security Incident Reporting Form so that DHS may determine whether an incident is a breach of protected health information ("PHI") or personally identifiable information ("PII") and establish a clear responsibility regarding the reporting of suspected or known unauthorized disclosures of confidential information.

A. Authority

O.C.G.A. § 10-1-910 et seq.

5 U.S.C. § 552a
45 C.F.R. Part 160
45 C.F.R. Part 164
42 U.S.C. § 300jj et seq.

B. References

Internal Review Service (IRS) Publication 1075

C. Applicability

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

D. 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 informatio

- **Data Breach Task Force (DBTF)**: a cross-functional incident response team gathered to investigate, mitigate and prevent any suspected or known breaches of PHI and PII

- **Management**: authoritative personnel within the department including but not limited to the Commissioner, Deputy Commissioner(s), and Divisional Director

- **Personally Identifiable Information (PII)**: any information about an individual maintained by DHS, including:

    a. 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 record

    b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

- **Protected Health Information (PHI)**: information that is created or received by a health care provider, health plan, 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:

    a. The past, present or future physical or mental health or condition of an individual

b. The provision of health care to an individual

c. The past, present or future payment for the provision of health care to an individual

E. Responsibilities

1. Reporting
   a. 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.
   b. 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 Security Incident Reporting Form**. A Microsoft word version of the Data Breach Security Incident Reporting Form can be found on the Office of General Counsel's page on the DHS website.
2. Investigation
   a. The DHS Privacy Officer will perform a risk assessment by using the following factors to determine whether the PHI or PII at issue has been compromised:
      i. The nature and extent of the PHI or PII involved, including the types of identifiers and the likelihood of re-identification;
      ii. The unauthorized person who used the PHI or PII or to whom the disclosure was made;
      iii. Whether PHI or PII was actually acquired or viewed; and
      iv. The extent to which the risk to the PHI or PII has been mitigated.
   b. Depending on the analysis by the DHS Privacy Officer or a representative substitute, the Privacy Officer will determine:
      i. If the event meets the criteria of a breach; and, if applicable,
      ii. 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 and/or contact the division manager to provide the next steps.
3. 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:

a. Ensure that the conditions that made the incident possible are corrected to prevent future incidents. This may include recommendations for further training of employees, or changes to office technology, training, policy, or procedures;
b. 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; and
c. Mitigate any possible harm that may have resulted from the incident.

4. Notification

   Upon determination and mitigation of the breach, the DBTF or Privacy Officer will take the 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 or Privacy Officer 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:

   a. HIPAA Data Breach Protocol
   b. Privacy Act Data Breach Protocol
   c. Social Security Act (SSA) Data Breach Protocol
   d. Georgia Personal Identity Protection Act (GPIPA) Protocol
   e. Internal Revenue Service (IRS) Data Breach Protocol
   f. Office of Child Support Enforcement (OCSE) Data Breach Protocol
   g. Food and Nutrition Service (FNS) Data Breach Protocol
   h. Any other contractual Data Breach Requirements (e.g., Accurint, etc.)

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

5. 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 records will be retained for a minimum period of six (6) years from when the breach is discovered.

F. Implementation

1. DHS Management
   a. Designate a Privacy Officer to which employees can report suspected or known unauthorized disclosures of confidential information to.
   b. Provide knowledgeable employees capable of joining the DBTF that is designed to investigate, mitigate and prevent any future occurrences of any suspected or known breaches of PHI and PII.
   c. Approve policies and necessary procedures to become compliant

and maintain compliance with all breach notification regulations.
   d. Provide privacy and security training and updates for workforce and ensure compliance with training schedules.
   e. Enforce sanctions, if necessary, against any employee, staff or contractor who does not comply with this policy and applicable state/federal laws.
2. Employees
   a. Understand and comply with organization's policies and procedures regarding confidentiality, privacy and security of all DHS data.
   b. Report any suspected or known breach of personal identifying formation (PII) or protected health information (PHI) of which DHS is the custodian.
3. 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 PHI and PII 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.
   a. **New staff member training**: New staff members will be trained on Data Security Awareness and HIPAA Privacy and Security within a reasonable time period after their hire date with the department.
   b. **Recurrent training**: Staff members are to be trained on Data Security Awareness and HIPAA Privacy and Security as a refresher no less than annually.
   c. **Special function training**: Staff members are to be trained on HIPAA Privacy and Security within three months after substantive changes are made to this policy or as necessary.
4. Sanctions
   DHS expects all employees to comply with all laws, regulations, standards, policies, procedures, guidelines and expectations regarding confidential information, including the privacy and security of protected health information and personally identifiable information. Applicable consequences of non-compliance with this policy and state/federal laws 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 demonstrate egregious disregard or a pattern of error in safeguarding personally identifiable information and/or protected health information.

G. History

Replaces POL 1660, last reviewed 04/08/2019.

H. Evaluation

The Privacy Officer and the General Counsel evaluate the effectiveness of this policy every year.

I. Additional Information

For additional information or assistance, please contact the Privacy Officer at privacy@dhs.ga.gov.