



OIT 62.905: Data Breach Notification

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 4/19/2011
Effective Date: 7/1/2011
Revision Date: 4/11/2011

I. Policy Statement

Data Breach Notification addresses notification of information security incidents.

II. Purpose

The Data Breach Notification policy specifies the University's notification requirements by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

All of the following are industry best practices. Where electronic records or IT infrastructure are involved, the following are requirements that the University shall adhere to. Based on business requirements, the University may need to comply with regulatory and/or industry requirements that are more restrictive. Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:

The University shall:

1. Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain personal information or medical information.
 - a. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:
 - 1) Social security number;
 - 2) Drivers license number or state identification card number issued in lieu of a driver's license number; or

- 3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
 - b. Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:
 - 1) Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
 - 2) An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
2. "Redact" for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:
- a. Five digits of a social security number; or
 - b. The last four digits of a driver's license number, state identification card number, or account number.
3. "Redact" for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:
- a. An individual's medical history; or
 - b. Mental or physical condition; or
 - c. Medical treatment or diagnosis; or
 - d. No more than four digits of a health insurance policy number, subscriber number; or
 - e. Other unique identifier.

Note: The terms for personal information or medical information do not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

- 4. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
 - a. Provide immediate notification to the agency of suspected breaches; and
 - b. Allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.
- 5. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:
 - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.;
 - b. Theft or loss of physical hardcopy; and
 - c. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).

An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.

The University shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #9, below.

6. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their personal or medical information exposed due to use of that computer must be alerted in accordance with data breach rules. Agencies shall notify the CISO when notification of affected individuals has been completed.
7. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of personal or medical information that was involved;
 - c. What actions have been taken to protect the individual's information from further unauthorized access;
 - d. A telephone number that the person may call for further information and assistance, if one exists; and
 - e. What actions the agency recommends that the individual take. The actions recommended should include monitoring account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).
8. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. Written notice to the last known postal address in the records of the individual or entity;
 - b. Telephone notice;
 - c. Electronic notice; or
 - d. Substitute notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
 - 1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
 - 2) Conspicuous posting of the notice on the web site of the individual or the entity if the individual or the entity maintains a web site; and
 - 3) Notice to major statewide media.
9. Hold the release of notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that

the notification will no longer impede the investigation or jeopardize national or homeland security.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.