Texas A&M University System - Data Breach Reporting Standards

Standard Statement

The Texas A&M University System (System) is committed to compliance with all federal and state laws and regulations relating to the compromise or Protected Health Information (PHI) and Sensitive Personal Information (SPI).

Reason for Standard

This standard establishes measures that must be taken to report and respond to a possible breach or compromise of PHI of SPI (collectively Protected Data).

Definitions

Breach – Any unauthorized access or use or other exposure of an individual's Protected Data that triggers a duty under state or federal law to provide a notification to the individual or a third party.

Business Associate – Any entity that contracts with a Covered Entity to provide services that require the entity to access, use, maintain or disclose the Covered Entity's PHI.

Covered Entity – A health care provider, health plan or clearinghouse that is required to comply with HIPAA.

> **HIPAA** – Health Insurance Portability and Accountability Act (HIPAA) as specifically set forth in Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 as the Administrative Simplification provisions and the regulations adopted by the U. S. Department of Health and Human Services (HHS) to implement HIPAA, which give HHS the authority to establish standards and requirements for the electronic transfer of health care information, and for the privacy and security of PHI.

Incident – Any unauthorized use, disclosure, or event that could reasonably involve Protected Data and/or indicates that a Breach has occurred.

Protected Health Information (PHI) – Individually identifiable health information that is transmitted or maintained in any medium or form that is subject to HIPAA. PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended; in records described at 20 U.S.C. 1232g(a)(4)(iv) (student treatment records excepted from FERPA); and in employment records held by a covered entity in its role as an employer.

Protected Data – Information maintained by the System and members that is subject to the Breach notification requirements of HIPAA/HITECH and/or Texas Business & Commerce Code Chapter 523 or other state or federal breach notification.

Sensitive Personal Information – Information stored in or derived from an electronic data base that includes: (i) and individual's last and first name or initial plus a Social Security Number, Driver's License or other state issued ID number, or account information plus a PIN or password; or (i) information that identifies an individual and relates to the individual's physical or mental condition, or the provision of health care to, or payment of healthcare for, the individual.

Standards

- Each office or department within the System shall require its employees to immediately report, upon discovery, any incident of inadvertent disclosure or unauthorized access that may constitute a breach to the SCISO within 24 hours. Offices and Departments should err on the side of caution when determining whether to report incidents.
- Offices and Departments shall not conduct internal investigations prior to, or otherwise delay, timely notification of the SCISO. Once notified, the SCISO will work with the affected unit to prevent any further unauthorized exposure.
- If it is determined by the affected unit and SCISO that protected data was involved in the breach, the SCISO must notify the System Breach Response Team.
- All Contracts and Agreements of any kind, including Business Associate Agreements, that involve access or use of Protected Data, shall require the contractor to notify a designated member employee of any unauthorized use or disclosure by the Contractor or its workforce, agents, or subcontractors that constitutes a security incident involving Protected Data and the remedial action taken or proposed to be taken with respect to the use or disclosure. Any employee receiving such a report must immediately forward such report.

Breach Response Team – Duties

A Breach Response Team shall be assembled to investigate and determine the System's compliance duties as to each incident reported to the SCISO that could trigger the System's duty to provide breach notifications under applicable federal or state privacy laws.

Members - SCISO, SCIO, and representatives from Office of General Counsel (OGC), Risk Management, Audit and Communications. Additional members can be included who, based on the nature of the incident, and is deemed to have experience or skills that make them appropriate for inclusion as a member of a Breach Response Team. The team may also include individuals from the affected unit that is the owner of the affected Protected Data, provided that inclusion of such individuals does not present a conflict of interest.

Duties – The duties of the Breach Response Team shall include, at a minimum, as applicable:

(i) Investigation of the incident, which may include interviewing relevant Workforce Members to learn about circumstances surrounding the incident and/or reviewing logs, tapes and/or other resources;
(ii) Identifying and engaging outside consultants, as required, to assist the investigation and/or risk analysis;
(iii) Identifying the nature of the breach (outside attack, human error, etc.);
(iv) Developing a mitigation plan to prevent future exposure of Protected Data, which may include revision of policies and procedures and/or additional training;
(v) Determining the appropriate notification requirements required and developing an action plan for the delivery of such notices;
(vi) If the incident involves a contractor, recommending termination or amendment of the terms of the Business Associate Agreement or other contract if required;
(vii) Ensuring compliance with applicable legal and regulatory requirements;
(viii) Oversight of the content and distribution of all internal and external communications regarding the incident.

At any time during the process, upon determination by the SCISO that it is likely that the incident may be the result of criminal action, or if for any other reason, the Breach Response Team determines that law enforcement participation is required or advisable, local law enforcement agencies, and/or the FBI, as appropriate, shall be notified without delay.

Required Notifications

Individuals:

Timing - Upon determining that a breach has occurred, individual notifications will be disseminated as soon as reasonably possible, taking the necessary time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual, but in no case shall notifications take place later than 60 days following the discovery of a breach, except when an agency of law enforcement requests a delay. Any delay based on law enforcement request must be documented in writing provided by or acknowledged in writing by the requesting law enforcement authority enforcement.

Process – Unless otherwise determined by the Breach Response Team, the affected unit with responsibility for the Protected Data that was the subject of the incident will be responsible for working with the Breach Response Team to ensure of the required reporting.

Contractor – In the case of a breach involving a contractor, notifications may be handled by the Breach Response Team or the contractor, as determined by the Breach Response Team, depending on the terms of the contract or agreement in place and the circumstances surrounding the incident.

Other:

Notification to HHS and other notifications required by other laws will be made by the General Counsel, in consultation with the Breach Response Team.

Reports to the media shall be made by the Office of Marketing and Communications, in consultation with the Breach Response Team.