Data Breach Response Guide

A&M System

Fall 2014

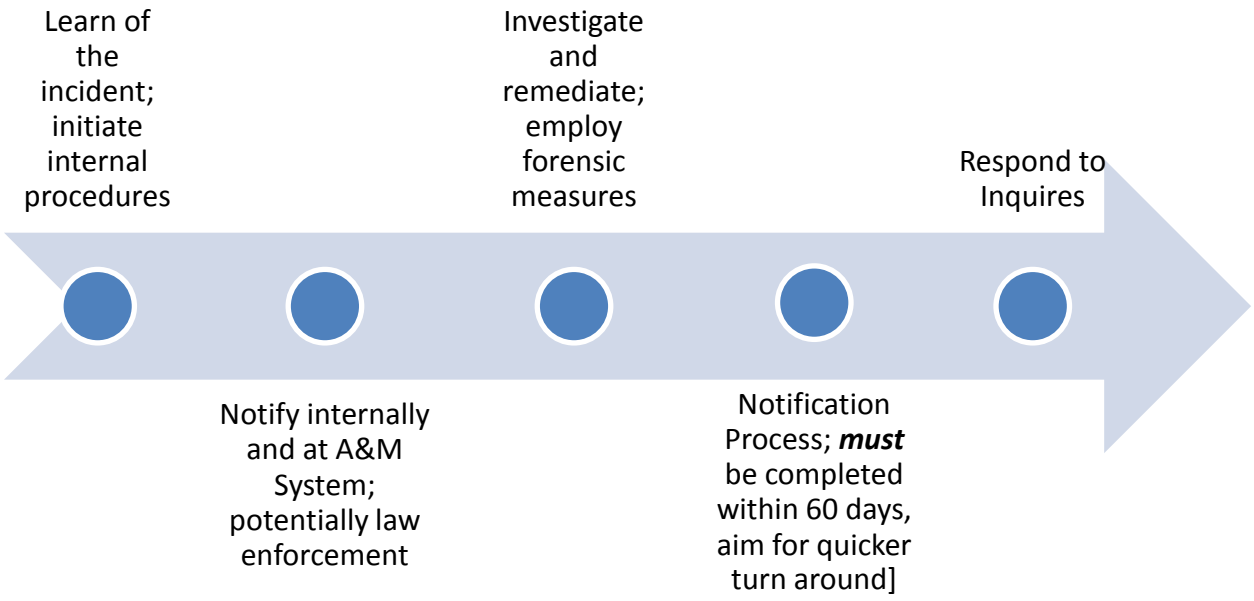
Introduction

What is a breach?

As defined by Texas law, a breach is an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information (SPI) maintained by a person."[1]

Preparation is the best defense.

Guideline of Actions for Data Breach Response



Pre-Breach Preparedness

During a data breach is not the time to decide who is to be handling necessary tasks; instead, developing a response plan and a standing response team now will help mitigate the complications of a discovered data breach.

The team's primary functions are 1) developing a data breach response plan and disseminating to the entire organization the proper protocol during a breach, and 2) carrying out the plan throughout the entirety of a data breach cycle.

[1] Tex. Bus. & Com. Code § 521.053(a)

Assembling the Response Team

While the specific make up of each team will vary, the general needs include:

- Incident Lead: manages and coordinates overall response efforts and team; acts as intermediary between member and A&M System
    - Recommend that this individual be the member CISO or individual with similar job responsibilities/skills
- IT and Security
- Public Relations/Communication

Preparedness Training

The Response Team will be in charge of disseminating information and training employees on how to handle breaches, but also member-specific best practices, including:

- Developing data security and mobile device policies that protect member data. Additionally, reviewing and updating these policies at regular intervals.
- Employee outreach ingraining the importance of data security in everyday use
- Continual review and updates to cybersecurity infrastructure
- Review and monitoring of data access for employees
- Ease of reporting noncompliance

Additionally, the Response Team will work closely with A&M System to set up breach tests.

Post-Breach Actions

Acting quickly and strategically following a breach will help regain security, preserve evidence, and protect your brand. Always collect, document, and record as much information about the data breach and response efforts as possible.

Post-Breach Checklist

- Record the data and time the breach was discovered.
- Contact A&M System (data breach contacts found at https://apps.system.A&M System.edu/datasecurity/index.html) and Response Team.
- Stop additional data loss. Take affected machines offline but do not turn them off or start probing until a forensics team arrives.
- Draft a summary report. Who discovered the breach, who reported the breach, who else knows about the breach, what type of breach occurred, what data was potentially compromised, how much data is involved, what devices/databases are involved.

Continued work to mitigate and repair the vulnerability will be coordinated by the Incident Lead through the A&M System SCISO and the forensic vendor.

Notification Process[2]

Working with the A&M SYSTEM OGC, notification must be provided to the affected individuals. In Texas, this notification must be made "as quickly as possible." A&M SYSTEM will aim for notification within 60 days of the breach discovery.

In most cases, the notification will be achieved by written notice to the last known address of the individual. However, in the case of a large breach (affected individuals exceed 500,000 or notice would exceed $250,000), exceptions may apply. Work with OGC to determine the best way to proceed with written notification.

Note if more than 10,000 notices must be sent out, each consumer reporting agency must be notified of the timing, distribution, and content of notices.

HIPAA Breach[3]

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Individual Notice. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and

[2] *See* Tex. Bus. & Com. Code §§ 521.002, 521.053
[3] *See* Breach Notification Rule, U.S. Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

Media Notice. Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice. This notice would be handled in conjunction with A&M SYSTEM Communications and OGC.

Notice to the Secretary. Covered entities will notify the Secretary by visiting the HHS web site (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.