AMERICAN COUNCIL ON EDUCATION

GENERAL COUNSEL

University Responses to Breach of Data Security

The recent effective date for enforcement of the new HIPAA/HITECH data-security breach notification law, and continued passage of and amendments to state notification laws, make compliance with data-security breach notification requirements more challenging than ever. Drawing on work for university and other clients, we provide here some observations on institutional response to data-security breaches.

Universities collect, maintain, use, and exchange vast amounts of personal data on students, faculty, staff, alumni, applicants, and third parties. Unwanted release or exposure of personal information can violate privacy, lead to identity theft, and result in adverse publicity. Lawmakers, regulators, and advocates are increasingly focused on data security and breaches of it. Data security is becoming a risk-management priority at universities. Effective handling of a data-security breach and legal compliance are best achieved with advanced planning to ensure that an institution's response is effective, efficient, and timely. Institutional responses will be facilitated if the institution already knows which laws and contracts apply to its data and what its duties will be if its information is improperly disclosed or accessed.

What law applies to a data-security breach?

Starting in California in 2003, the law began to impose an obligation on those who hold data on persons to provide notice if there is a breach of its security. Forty-five states, Washington, DC, the Virgin Islands, and Puerto Rico have such laws currently, and federal rules govern disclosure of health-related personal information.

The Federal Trade Commission, state attorneys general, and private plaintiffs have pursued universities that have experienced data-security breaches. Such investigations typically have focused not only on whether notice protocols were followed, but also on underlying data security.

What actions should the institution take promptly after a breach?

Contain the breach. As soon as the institution becomes aware of a data breach it should take all necessary steps to limit further data loss and should investigate the incident. It should also determine whether to involve law enforcement and should limit traffic into the affected area until security officials or law enforcement investigate.

This memorandum was prepared by Christopher Wolf and Tracy Gray of Hogan & Hartson, LLP (March 2010).

One Dupont Circle NW, Washington, DC 20036-1193
Telephone: (202) 939-9355 • Fax: (202) 833-4762
Web: http://www.acenet.edu

Convene a response team. A university should have a standing security breach response team that includes representatives from the office of the general counsel, information technology security, human resources, internal audit, and the news office. When a breach occurs, the response team should convene without delay. Team composition may vary, according to the type and location of the breach.

Analyze the breach. The institution should record all information relevant to the breach; learn and evaluate the cause and effect of the incident; determine whether other systems are at serious risk of future breach; and consider engaging specialized consultants to capture relevant information and perform forensic analysis.

Determine timing requirements. Time is of the essence. Law of many states prescribes time limits for notification of persons data on whom was breached. Expedition is not just sensible; often it is legally mandated.

Collect information promptly. Information that should be gathered promptly includes the date, time, duration, and location of the breach; how the breach was discovered, by whom, and any known details about it; and information on compromised data, including a list of affected individuals by category, data fields, the number of records affected, and which if any data were encrypted.

What next steps should the institution take?

Analyze legal implications of the breach. Legal analysis should include analysis of relevant business contracts for notification and other obligations; breach-notification requirements; and pertinent indemnification agreements. The states and countries potentially involved in the breach should be identified with reference to the location of persons and systems affected by the breach. Federal, state, and international statutes and regulations potentially triggered or violated by the breach, and their notification requirements, should be identified.

Contact law enforcement. Where appropriate, contact local or federal law enforcement agencies.

Contact insurance carrier. Review insurance pertinent to the breach; notify the insurance carrier in accordance with policy requirements.

What internal and external breach-related communications should the institution make?

A wave of telephone calls, e-mails, and other inquiries should be expected when a breach is reported. Before occurrence of a breach, the institution should have a plan for handling such inquiries. Actions to consider include selecting a mode of communication with the public (toll-free numbers and/or e-mail address); selecting a mode of communication with students, staff, faculty, and alumni; training and hiring staff for inquiry response, or outsourcing such activities; preparing a script; notifying credit-reporting agencies prior to providing notification to a large group of affected persons (or as required by applicable law); documenting inquiry responses; and preparing Frequently Asked Questions ("FAQs") for potential online posting.

What should be in the institution's notification plan?

The institution should develop a notification plan for affected persons, based on legal requirements and its contractual obligations. The content of notice to affected persons may be dictated by regulation or contract, and public relations considerations should be taken into account. Generally, notice should include this information:

- description of what happened
- type of protected data involved
- actions the institution has taken to protect data from further unauthorized access
- what the institution will do to assist affected persons
- what affected persons can do to assist themselves
- contact information for the institution to respond to inquiries (a toll-free number should be provided)
- contact information for local and federal government authorities

The institution may elect to offer remediation services to assist affected persons after a breach, including credit monitoring services, identify-theft insurance, identity-theft information packets, and/or compensation for identity theft. A number of universities have elected to offer remediation services, although usually such services are not legally required.

What other post-breach actions are indicated?

Prepare for litigation. If litigation is threatened, preservation of relevant documents and information is vital.

Reassess technology systems and physical security. The institution should conduct an analysis of the breach to determine causes and should review access controls and procedures to ensure that weaknesses have been addressed and resolved.

Perform an assessment. Assess the institution's operations to determine necessary revisions to data collection, retention, storage, and processing policies and procedures, so that further breaches are less likely to occur.

Evaluate the institutional response. After the institution has responded to the breach, it should evaluate its response and implement changes to improve its effectiveness in preventing and responding to breaches.

Summary

- Have a written post-breach response plan ready and tested before a breach happens.
- Ensure that institutional officials know what role they will have when a breach happens.
- Have a communications plan regarding breaches.
- Know what regulations, statutes, and contracts cover post-breach obligations.
- Act promptly to prevent further exposure of data when a breach happens.
- Promptly find out what happened and preserve the evidence.
- Involve technology and legal experts as needed.
- Have draft notices that are ready to be customized with reference to the facts.
- Contact law enforcement, credit reporting agencies, and the institution's insurance carrier as appropriate.
- Keep regulators informed, both when required by law and when merely sensible.
- Provide timely notice; legal deadlines are strict.
- Help affected individuals; their goodwill can forestall legal difficulties.
- Update the breach response plan periodically.