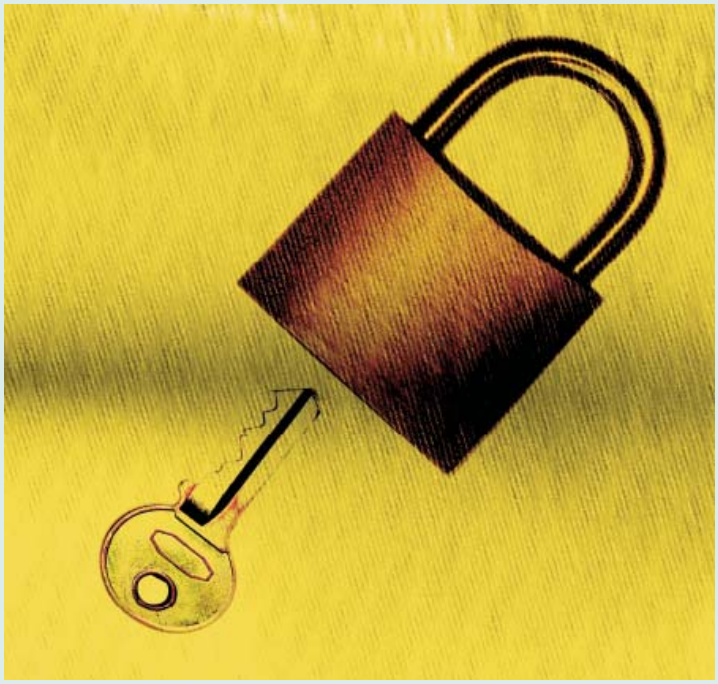
Treat Security Breaches With Caution

Kevin D. Lyles, Esquire
Jones Day
Columbus, Ohio

Ritu Kaur Singh, Esquire
Jones Day
Washington, DC



I. Introduction

Because of advances in computer technology and electronic data storage, as well as the ostensible "green light" for hospitals to assist physicians with information technology from the Internal Revenue Service (IRS),[1] the Centers for Medicare and Medicaid Services (CMS), and the Department of Health and Human Services Office of Inspector General (OIG),, the use of electronic health records (EHRs) is becoming commonplace among healthcare entities. EHRs are intended, among other things, to allow physicians remote access to electronic protected health information (ePHI), particularly from their offices or at home. The use of EHRs, however, may well increase the risk of data security breaches.[2]

Data security breaches occur in many ways at healthcare entities. A hacker could break into a system, or a thief could steal a notebook computer that is left in a car. An employee could inadvertently send ePHI over the Internet or make it accessible on a website. Or, an employee could intentionally abscond with patient information in an attempt to personally profit or harm his or her employer (or a patient). Often, the way a breach occurs dictates the way the organization responds to the breach. For example, the Information Technology (IT) department might handle the case of the computer hacker while the Human Resources (HR) department might handle the rogue employee.

Although it is appropriate to involve these departments in the response to a security breach, we believe that most breaches warrant an organizational response that involves a number of departments, including IT, HR, Legal, and Compliance, as well as Senior Management. Because of the large number of patient records that may be involved, a healthcare entity faces significant potential liability from a data security breach. This liability may include damages suffered by patients, information technology costs, damage to reputation, and, for public companies, a decline in stock price. Therefore, a healthcare entity should respond to a data security breach as it would any other serious compliance event and not treat it as just an IT or HR problem.

To properly respond to a data security breach a healthcare entity must understand its legal obligations. The two primary sources of these obligations are found in the Security Rule promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and in various state security breach notification laws.

II. Requirements Under HIPAA Security Rule

The Security Rule generally requires a covered entity to:

- Ensure the confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against reasonably anticipated uses or disclosures of such information that are not permitted or required.
- Ensure compliance by the employer's workforce.

In addition, the Security Rule requires a covered entity to execute written policies and procedures detailing how the covered entity will identify and respond to suspected or known security breaches, mitigate any harmful effects resulting from security breaches, and document security breaches and their outcomes. Further, a covered entity must assess and implement a number of security measures relating to administrative, physical, and technical safeguards with respect to any patient ePHI that is created, received, maintained, or transmitted.

Notably absent from these requirements is an obligation for the covered entity to notify patients that their ePHI has been compromised. Despite this lack of an express requirement, however, in many, if not most, cases a covered entity will conclude that patient notification is required to fulfill its obligation to mitigate the harmful effects of the security breach.

III. Requirements of State Security Breach Notification Laws

At least thirty-six states currently have laws requiring certain entities that experience data security breaches to notify affected individuals. A number of these laws, however, do not apply to a person who or entity that is regulated by HIPAA, meaning they do not apply to most healthcare providers, health plans, and healthcare clearinghouses. Nine states that expressly exempt healthcare entities subject to HIPAA include: Arizona, Hawaii, Indiana, Michigan, Minnesota, Ohio, Rhode Island, Vermont, and Wisconsin. Also, eight state security breach notification laws do not expressly exempt healthcare entities subject to HIPAA, but provide that notification pursuant to the laws, rules, and regulations established by that entity's primary or functional federal regulator suffices for compliance under the state security breach notification laws, implying that healthcare entities subject to HIPAA may be exempt. These eight states are: Colorado, Connecticut, Florida, Idaho, Maryland, New Hampshire, Pennsylvania, and Utah.

Although each state law varies, the state security breach notification laws typically apply, with the exceptions previously mentioned, to any person or entity doing business in the state where the person or entity owns, licenses, or maintains computerized data in the state that contains personal information. "Personal information" generally means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number.
- Driver's license number or state identification card number.
- Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

As a rule, either the name or the data element must be unencrypted to be considered "personal information." In general, "personal information" does not include information that is lawfully made available to the general public from federal, state, or local government records. A "security breach" generally means the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

In the event of a data security breach, the covered person or entity generally must notify the affected individuals of the breach in a timely manner and without unreasonable delay. Some states' laws provide a deadline for when the notice must be provided, e.g., within forty-five days after discovery of the breach. The state laws vary in the level of specificity they require for the content of the notice and the method of delivering the notice. For example, some states allow notice to be given electronically in certain cases. Healthcare entities should review their state's notification law closely to ensure compliance with these provisions.

The Tech Licensing and Intellectual Property Affinity Group

About the Tech Licensing and Intellectual Property Affinity Group. The Tech Licensing and Intellectual Property Affinity Group provides a forum for members to exchange and discover information about technology licensing and contracting and intellectual property issues related to health information technology. The Affinity Group covers topics such as negotiation strategies, key contractual issues in the acquisition of health information technology, and intellectual property rights in software, customizations, and intangible items such as data. The Affinity Group provides practical suggestions for documenting health information technology transactions and addressing the competing intellectual property interests among the parties to a health information technology transaction.

Members of the Tech Licensing and Intellectual Property Affinity Group. The HIT Practice Group wishes to thank the Tech Licensing and Intellectual Property Affinity Group:

Co-leaders:
Kevin D. Lyles
Heidi Echols
Mark Mildenberger

Members:
Carol S. Allis
Elisabeth Belmont
Deborah Lynn Biggs
Bernadette M. Broccolo
Ellen V. Chiniara
Mark T. Garsombke
Mark C. Gary
William Reece Hirsch
Janet Percy Knaus
Marilyn Lamar
Amy S. Leopard
Tracy J. Mabry
Peter Mancino
Patricia A. Markus
Robert G. Martin
Austin M. O'Flynn
C. Elizabeth O'Keeffe
Charles Warren Ott
Jeffrey M. Sconyers
Jeffrey W. Short
Michael G. Stein
Mark Tatelbaum
James A. Wellons
Robert Q. Wilson

IV. How to Respond to a Healthcare Data Security Breach

If a healthcare data security breach occurs, a healthcare entity should be prepared to respond to the breach in a timely and organized manner. A healthcare data security breach is a serious issue and should not be treated as a minor glitch in the system. The actions taken by the healthcare entity immediately after learning of a data security breach are critical to the impact the data security breach has on the entity. Failure to act in response to a data security breach or an insufficient response potentially could lead to litigation, government scrutiny, and damage to the entity's reputation. Some suggested steps include:

- Review Policies;
- Conduct an Internal Investigation;
- Report Findings to Senior Management;
- Make Any Necessary Notifications; and
- Execute Remedial Measures.

Review Policies. A healthcare entity should designate a person or department with the responsibility to ensure that the entity is compliant with HIPAA and the various state security breach notification laws. Often, this responsibility is placed on the Compliance Officer. In particular, the written policies and procedures should detail:

- Security measures relating to administrative, physical, and technical safeguards with respect to any patient ePHI that is created, received, maintained, or transmitted.
- How an entity will identify suspected or known security breaches. This may include setting up a hotline or other anonymous mechanism for employees to report suspected or known security breaches.
- A roadmap for responding to suspected or known security breaches.
- Potential steps for how an entity should mitigate any harmful effects resulting from security breaches.
- The steps a Compliance Officer should follow with regard to documenting the security breach and its outcomes.
- Training for employees on a yearly basis on the importance of ensuring the confidentiality, integrity, and availability of ePHI as well as the reporting of data security breaches.

A healthcare entity should review its existing privacy practices, privacy and data security policies, and information technology and security systems for protecting the privacy and security of personal information to ensure they address these basic considerations, as well as comply with HIPAA and other applicable laws.

Conduct an Internal Investigation. The healthcare entity should conduct an internal investigation as soon as is practicable following discovery of a known or suspected data security breach. Learn all the facts surrounding the breach. If the breach was reported via a hotline or other reporting mechanism, some facts already may be known.

The healthcare entity may want to create a "response team," led by the Compliance Officer, a designated person responsible for HIPAA compliance, or other appropriate person, to investigate the security breach. The team would be responsible for assessing the breach, containing it, and, if applicable, working with outside counsel.

Once the breach is contained, the team should retain a qualified network security consultant to conduct a privileged investigation that is overseen by legal counsel. The team should consult with the legal department or in-house counsel on whether it is advisable to engage and retain the advice of outside litigation counsel to preserve any available privileges.

Privilege extends to attorney-client communications and attorney work product—any material prepared by the party, the attorney, the retained experts or consultants, or other representative in anticipation of litigation. Using in-house counsel who act in dual capacities as legal counsel and as business advisors may prevent a healthcare entity from preserving what might have been a privileged internal investigation. Accordingly, the roles of in-house and outside counsel should be determined early in the investigation.

The team should determine whether personal information has been accessed or acquired, or is reasonably believed to have been accessed or acquired, by an unauthorized person. The team then should initiate any necessary steps to contain and control the systems affected by the data security breach. The team may need to involve the head of IT to aid in containing the data security breach and controlling the systems.

During the internal investigation, the qualified network security consultant should determine the source and scope of the data security breach and how the breach occurred. The internal investigation may reveal that employees failed to act in a manner consistent with internal privacy and security policies and procedures and/or HIPAA requirements. If this is the case, it may be necessary to discipline employees, including even termination. Any implemented sanctions should be applied consistently and properly documented. As part of the sanctions, the Compliance Officer should require employees to attend training sessions on the entity's privacy and security policies and procedures.

Because some state security breach notification laws require notification to affected individuals within forty-five days after learning of the breach, the healthcare entity should attempt to complete the internal investigation within thirty days of discovery of the breach. This allows time for the findings from the internal investigation to be reported to senior management and for senior management to develop an appropriate plan for responding to the data security breach.

Report Findings to Senior Management. All the reports, documents, and information related to the internal investigation should be compiled and retained. The response team should report to senior management the findings from the internal investigation

within a short period of time, and within seven days, after completing the internal investigation, including:

- The scope of the breach.
- The status of whether the information technology and security network have been restored.
- Whether there has been compliance with existing internal privacy and security policies and procedures and HIPAA.
- Whether there are any relevant state security breach notification laws with which the entity must comply.
- Any recommendation for disciplinary actions against employees who were involved with the security breach.

Senior Management should develop a plan for responding to the data security breach to be implemented by the team. If the entity is a public company, determine whether knowledge of the security breach before notification constitutes material non-public information and also whether the security breach must be disclosed in the company's Security and Exchange Commission reports.

Make Any Necessary Notifications. Depending on the applicable state law, the healthcare entity may be required to notify affected patients that their personal information has been compromised. As previously noted, HIPAA does not require notification to the government or patients of a data security breach. The healthcare entity, however, may determine that notification is best even if it is not required. The healthcare entity should review the applicable state security breach notification laws regarding who to notify and the timing and content of the notification.

Entities with notification obligations should develop and implement a notification plan. The notification itself should be worded carefully to prevent any further complications. For example, the notification may include information about the breach, a description of the people affected by the breach, measures the healthcare entity is taking or plans to take to avoid future security breaches, general guidance on what the potentially affected patients should do to protect themselves, and contact information for any follow-up questions. The healthcare entity should notify the affected patients, where appropriate, in a timely manner pursuant to the applicable state statute.

Execute Remedial Measures and Conduct Business as Usual. The healthcare entity should take the necessary steps to fix the problem that caused the data security breach as soon as possible. The entity may need to revise its privacy and security policies and procedures if they are not compliant with HIPAA, the applicable state security breach notification laws, and other applicable requirements. Additional employee training regarding protecting personal information may be needed. There may even be a need for new information technology and security systems for protecting the privacy and security of personal information.

By following the foregoing steps, healthcare entities will be treating data security breaches with the proper level of caution as opposed to a mere IT glitch. Further, they can fulfill their legal obligations under HIPAA and state security breach notification laws and can minimize the harm suffered by their patients and their organizations.

---

[1] Editor's Note: An update and discussion of recent IRS activity can be found in the last article in this issue.

[2] In June 2007, the Government Accountability Office (GAO) issued a report discussing whether a federal disclosure law would be appropriate in light of the high number of data security breaches in the last few years. *See* GAO, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown,* GAO-07-737 (June 4, 2007), *available at* www.gao.gov/cgi-bin/getrpt?GAO-07-737. Currently, there is no federal statute that requires entities to notify individuals whose personal information has been lost or stolen. Congress, however, is considering legislation that would establish a national breach notification requirement. The report mentions healthcare data security breaches a limited number of times. The report noted that the American Hospital Association (AHA) conducted a survey of forty-six hospitals at the GAO's request. Of those hospitals, thirteen had experienced data security breaches since 2003.