HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Nine
Number Eleven
November 2007
Published Monthly

Earn CEU credit

SEE INSERT

Meet

Juliann Tenney

Institutional Research Compliance and Privacy Officer and Director, Institutional Research Compliance Program for The University of North Carolina at Chapel Hill

PAGE 14

Quality of care initiatives: Malpractice and pay for performance

PAGE 4

Also:

CMS audit activity is fierce: Is your Medicare Advantage and Part D Program prepared?

PAGE 27

Feature Focus:

Risk Assessments and Compliance

PAGE 44

Responding to data security breaches

By Kevin D. Lyles, Esq. and Ritu Kaur Singh, Esq.

Editor's note: Kevin D. Lyles is a partner in the Columbus office of Jones Day. Mr. Lyles co-chairs Jones Day's health care practice. He can be reached by phone at 614/281-3821 or by e-mail at kdlyles@jonesday.com.

Ritu Kaur Singh is an associate in the Washington office of Jones Day. Ms. Singh is a member of Jones Day's health care practice. She can be reached by phone at 202/879-5575 or by e-mail at rksingh@jonesday.com.

In the last year, the Internal Revenue Service (IRS) and the Centers for Medicare and Medicaid Services (CMS) have come out with rulings and decisions that hospital assistance to physicians for electronic devices would be protected from scrutiny under the Federal Anti-kickback Statute and the Stark Law. In light of advances in computer technology and electronic data storage, as well as the "green light" from the IRS and CMS for hospitals to assist physicians with information technology, the maintenance and use of electronic health records (EHRs) is becoming commonplace among health care entities. EHRs are intended, among other things, to allow physicians remote access to electronic protected health information (ePHI), particularly from their offices or homes. ePHI is any protected health information (PHI) that is created, received, maintained, stored, or transmitted electronically on a health care entity's servers or electronic systems.

Using EHRs, however, poses risks for possible data security breaches. In June 2007, the United States 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.[1] The report mentions health care data security breaches a limited number of times, and noted that the American Hospital Association conducted a survey of 46 hospitals at the GAO's request. Of the 46 hospitals, 13 had experienced data security breaches since 2003. Currently, no federal statute 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. Health care entities must take into account compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] and applicable state security breach notification laws when responding to a health care data security breach.

HIPAA

HIPAA was enacted on August 21, 1996 to, among other things, improve the efficiency and effectiveness of the delivery of health care by establishing standards and requirements for the electronic data transmission and setting and enforcing standards for the protection of the confidentiality and security of health data. HIPAA regulates the use and disclosure of PHI by covered entities. PHI is defined as any demographic information that identifies an individual and relates to at least one of the following:

- The individual's past, present, or future physical or mental health;
- The provision of health care to the individual; or
- The past, present, or future payment for health care.

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity. "Covered entities" include health care providers, health plans, and health clearinghouses who transmit any health information in electronic form in connection with a covered transaction.[3]

HIPAA's administrative simplification provisions create both criminal and civil penalties for violations of HIPAA's statutory prohibitions and implementing regulations, including the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) and the Security Standards for the Protection of ePHI (Security Rule). The Privacy Rule sets forth the national standards for the protection of PHI. The Security Rule sets forth national standards for the secure storage and transmission of ePHI between entities.

The Privacy Rule governs the use and disclosure of PHI, as well as standards for individuals' privacy rights, to understand and control how their health information is used. The Privacy Rule defines and limits the instances when an individual's protected health information may be used or disclosed by covered entities. It generally requires that covered entities do the following:

- Develop criteria designed to limit PHI disclosure to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request;
- Include certain protections for PHI in business associate agreements; and
- Maintain and provide a notice to individuals regarding the use and disclosures of PHI that may be made and the individual's rights with respect to PHI.

The Security Rule applies only to covered entities who electronically create, receive, maintain, or transmit protected health information. The Security Rule generally requires that covered entities:

- Ensure the confidentiality, integrity, and availability of all ePHI that the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integ-

Continued on page 58

rity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
- 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, and document security breaches and their outcomes. Further, the covered entities are required to assess and implement a number of security measures relating to administrative, physical, and technical safeguards with respect to any patient ePHI which is created, received, maintained or transmitted.

State security breach notification laws

At least 36 states currently have laws requiring certain entities that experience data security breaches to notify affected individuals. Some state security breach notification laws do not apply to any person or entity that is regulated by HIPAA. For example, the following nine states expressly exempt health care entities subject to HIPAA from the notification requirements: Arizona, Hawaii, Indiana, Michigan, Minnesota, Ohio, Rhode Island, Vermont, and Wisconsin. Additionally, eight state security breach notification laws do not expressly exempt health care 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 is sufficient for compliance under the state laws, implying that health care entities subject to HIPAA may be exempt. These eight states are: Colorado, Connecticut, Florida, Idaho, Maryland, New Hampshire, Pennsylvania, and Utah.

Although each state varies, the state security breach notification laws typically apply (with the exceptions previously mentioned) to any person or entity doing business in a state where the person or entity owns, licenses, or maintains computerized data that contains personal information in that state. "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, or
- 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.[4]

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" is generally defined as the unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

A person or entity that has experienced a data security breach generally must notify the affected individuals of the breach in a timely manner and without unreasonable delay. The state laws vary in their requirements for the form of notice. For example, California requires that notice to affected individuals may be provided by one of the following methods: (i) in writing, (ii) electronically if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal Electronic Signature Act,[5] or (iii) by substituted notice if the entity demonstrates that notice will cost over $250,000 or the affected class of individuals is over 500,000, or the entity does not have sufficient contact information to effectuate notice. "Substitute notice" involves all of the following: (i) notice via e-mail when the entity has the e-mail address for an affected individual, (ii) conspicuous posting on the entity's Web site if the entity maintains one, and (iii) notification to statewide media.[6]

How to respond to a health care data security breach

If a health care data security breach occurs, a health care entity should be prepared to respond to the breach in a timely and organized manner. The actions taken by the health care entity immediately after learning of a data security breach are critical to the impact the data security breach has on the entity. Missteps can 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
- Execute remedial measures and conduct business as usual

Review Policies. A health care entity should first review the following internal documents and systems aimed at protecting the privacy and security of personal information:
- existing privacy practices,
- privacy and data security policies, and
- information technology and security systems.

These policies should already be in place as required by HIPAA and should provide a roadmap for responding to the security breach.

Conduct an internal investigation. The health care entity should conduct an internal investigation as soon as is practicable. It is important to understand the facts surrounding the security breach.

- Create a "response team" led by a point person to investigate the security breach. The response team would be responsible for assessing the breach, containing it, and, if applicable, working with outside counsel.
- Determine whether personal information has been accessed or acquired, or is reasonably believed to have been accessed or acquired by an unauthorized person.
- Initiate any necessary steps to contain and control the systems affected by the data security breach.
- Retain a qualified network security consultant to conduct a privileged investigation that is overseen by legal counsel. Consider whether it is advisable to engage and retain the advice of outside litigation counsel in order to preserve any available privileges. Privilege extends to attorney-client communications and 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 health care entity from preserving what might have been a privileged internal investigation.
- During the internal investigation, determine the source and scope of the data security breach and how the breach occurred.
- If the breach reveals that employees failed to act in a manner consistent with internal privacy and security policies and procedures and/or the HIPAA requirements, it may be necessary to discipline employees with sanctions or even termination. Any sanctions implemented should be applied consistently and properly documented. The employees may need to attend training sessions on the entity's privacy and security policies and procedures.

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

- the scope of the breach,
- the status of whether the information technology and security network have been restored,
- whether compliance with existing internal privacy and security policies and procedures and HIPAA has been maintained,
- whether the entity complied with any relevant state security breach notification laws, and
- 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 response team. If the entity is a public company, a determination must be made as to 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 SEC reports.

Make any necessary notifications. Depending on the applicable state law, the health care entity may be required to notify affected patients that their personal information has been compromised. As previously noted, HIPAA does not specifically require notification to the government or patients of a data security breach. It does, however, require the covered entity to mitigate the effects of the security breach. This may lead the entity to decide that notifying patients is required. Once a determination has been made to notify patients of a security breach, the health care entity should:

- Review the applicable state security breach notification laws regarding who to notify and the timing and content of the notification.
- Develop and implement a notification plan. The notification should be carefully worded in order 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 health care entity is taking or plans to take to avoid any future security breaches, general guidance on what the potentially affected patients should do to protect themselves, and a contact number for any follow-up questions.
- 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 remedial measures should be implemented as soon as possible:

- Fix the problem that caused the data security breach.
- Assist patients whose information was breached.
- Revisit and, if appropriate, revise the entity's privacy and security policies and procedures.
- Deliver additional employee training regarding protecting personal information.
- Evaluate whether new information technology and security systems are needed.
- Take any necessary disciplinary actions against employees involved in the security breach.

By following the foregoing steps, health care entities 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 See GAO, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extend is Unknown, GAO-07-737 (Washington, D.C.: June 4, 2007) available at http://www.gao.gov/cgi-bin/getrpt?GAO-07-737.
2 42 U.S.C. 1320d to 1329d-8; 45 C.F.R. Parts 160 and 164
3 42 C.F.R. 160.103; 42 C.F.R. 164.104
4 For data element 3, some of the states require only a password, unaccompanied by the account number, or an account number that does not require a password.
5 15 U.S.C. § 7001 et seq.
6 California Database Security Breach Notification Act (SB 1386), effective July 1, 2003.