ALERTBULLETIN®

CNA
We can show you more.®

AB 2012 ISSUE 4

Cyber Liability: Reducing the Risks of a Data Breach

Recent media accounts of unauthorized disclosures of protected health information (PHI) and other sensitive data underscore the importance of an effective information security program for all healthcare organizations. The following occurrences illustrate some of the more common causes of a data breach:

- *A California hospital found that a spreadsheet with information about 20,000 emergency department patients – including names and diagnostic codes – had been posted for almost a year on a commercial Web site.* The cause: data migration via a vendor responsible for bill collection.
- *A South Carolina healthcare system reported the possible disclosure of approximately 400,000 patient names, Social Security numbers, addresses, birth dates and medical billing codes.* The cause: theft of a computer containing the data from an employee's car.
- *A Boston medical center notified more than 2,000 patients of the unauthorized release of their names, medical record numbers, birth dates and medical procedures.* The cause: a data-transmitting virus, which infiltrated a hospital computer after a service vendor neglected to restore security settings.

More than 250 large-scale data breaches such as these occurred between September 2009 and December 2010, according to the U.S. Department of Health and Human Services (HHS). These disclosures, involving the medical and/or personal data of nearly 7.9 million persons, were reported to HHS in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act (Public Law 111-5, Section 13402), which was enacted in 2009 as part of the American Recovery and Reinvestment Act.

HITECH reinforces the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by mandating prompt reporting of large-scale data breaches and annual reporting of smaller breaches. In the case of disclosures involving more than 500 individuals, HITECH requires informing not only HHS, but also affected persons – and local media outlets – within 60 days of discovery. The law further requires notification following disclosure of "unsecured" (i.e., readable) PHI by business associates of HIPAA-covered entities. The business associate must inform the covered entity of any persons whose PHI may have been accessed within 60 days of discovering the breach, and the covered entity is then responsible for notifying affected individuals.[1]

This issue of *AlertBulletin*® examines how data breaches occur, presents strategies to address the major hazards and provides a listing of relevant resources.

SCOPE OF THE PROBLEM

According to Privacy Rights Clearinghouse, three of the six largest data breaches in 2011 occurred in the healthcare industry, a prime target of information thieves and hackers.[2] Human error and carelessness also play major roles in the loss and disclosure of patient data.

As reported by the HHS Office for Civil Rights, breaches fall into five general categories, listed in declining order of frequency:

- *theft of paper records or electronic media,* including computers and such portable devices as USB flash drives, personal digital assistants and smart phones
- *loss of paper or electronic records,* including laptops and storage media
- *unauthorized access to PHI,* including external hacking, "malware" infiltration and illicit employee-related exposures
- *human or technological miscues,* including erroneous mailings and electronic mail or network server glitches
- *improper disposal of paper records,* generally involving errors on the part of a billing service or other vendor

About 20 percent of the reported incidents, comprising more than half of the total records disclosed, were committed by outside contractors. Loss or theft of unsecured data accounted for about 55 percent of breaches, compared to only 7 percent due to attacks by hackers.

The potential consequences of a data breach range from sizeable monetary penalties, negative publicity, interruption of daily activities and loss of public trust to possible patient harm, if medical data integrity is compromised. Financial losses resulting from data breaches are not necessarily covered by professional, property or general liability insurance policies. In view of the risks, healthcare leaders should evaluate their overall cyber exposure, create a plan to secure confidential information and minimize the impact of a breach, and obtain appropriate insurance coverage.

1 For more information, see the 2011 "Annual Report to Congress on Breaches of Unsecured Protected Health Information" from the HHS Office for Civil Rights, available at **http://www.hipaasecurityandprivacy.com/2011/09/annual-report-to-congress-on-breaches.html**.

2 See "Three of top 6 data breaches were in healthcare," *Healthcare Finance News*, December 19, 2011, at **http://www.healthcarefinancenews.com/news/consumer-group-lists-top-6-data-breaches-2011**.

RISK CONTROL STRATEGIES

The following basic measures constitute a useful starting point for organizational discussion of data breach prevention and response:

- *Perform a cyber risk assessment/PHI inventory.* The critical first step in enhancing data security is to identify system vulnerabilities and account for how PHI is managed and secured. A variety of programs exist to assist in this task, including the Cyber Security Evaluation Tool (CSET™), at **http://www.us-cert.gov/control_systems/satool.html**, and the OCTAVE® Information Security Risk Evaluation, at **http://www.cert.org/octave/**.
- *Educate leadership and staff regarding the scope of federal and state privacy and notification requirements,* in order to encourage enterprise-wide compliance. Basic HIPAA requirements should be integrated into employee orientation and training, with an emphasis on the consequences of removing PHI from the facility, failing to log out when leaving a work station, sharing passwords, exposing laptops or storage devices to theft, leaving confidential information displayed on a screen or otherwise neglecting to observe data security policies.
- *Secure record storage space.* To reduce the possibility of theft or sabotage, periodically reevaluate the measures used to control access to restricted areas.
- *Implement a user monitoring system and effective access controls.* The HIPAA Security Rule requires that IT systems log user access to protected information. Logged activities should be closely monitored. In addition, accounts should have suitably complex, regularly reset passwords and should lock automatically after a set number of unsuccessful log-ins.
- *Examine agreements with business associates regarding data sharing and security.* Contracts should expressly address PHI confidentiality issues in accordance with federal regulatory guidelines, with language reviewed and approved by legal counsel and IT specialists. Data shared with vendors and other business associates should follow the "minimum necessary" standard, as required by the HIPAA privacy rule.
- *Adopt encryption technology,* which renders protected information unreadable and unusable in the event of a security breach. Undecipherable information is not subject to HITECH reporting requirements.
- *Institute a post-breach response plan.* In addition to complying with state and federal notification requirements, the plan should provide affected individuals with credit and medical identity monitoring services. (For ethical and reputational reasons, it is generally advisable to inform all affected parties of a data breach, even if such notification is not required by law.)
- *Obtain cyber liability insurance* to address data- and privacy-related coverage gaps. Such products generally cover third-party liability (e.g., fines, indemnity payments and associated legal expenses), as well as notification costs, system restoration expenses and related business interruption losses. To learn more, contact your local CNA underwriter.

In an age of electronic health records, stringent privacy regulations, and widespread concern about identity theft and Medicare fraud, information security has become an increasingly high-priority component of an enterprise risk management program. Sound, proactive policies can significantly reduce the likelihood and minimize the impact of a data breach.

RESOURCES

- American Health Information Management Association (AHIMA), at **www.ahima.org**.
- "The CPRI Toolkit: Managing Information Privacy and Security in Healthcare." A resource from the Healthcare Information and Management Systems Society (HIMSS), 2007. Available at **https://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D73_Admin_Requirements.pdf**.
- National Institute of Standards and Technology (NIST) Computer Security Resource Center, at **http://csrc.nist.gov**.
- U.S. Department of Health and Human Services, Office for Civil Rights, Breach Notification Rule, available at **http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html**. A listing of breaches affecting 500 or more individuals is available at **http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html**.
- "What Healthcare Executives Should Know and Do About Information Security." A white paper from HIMSS, 2005. Available at **http://www.himss.org/content/files/CEOWhitePaperFinal.pdf**.

CNA

For more information, please call us at 888-600-4776 or visit www.cna.com/healthpro.