HEALTHCARE PERSPECTIVE

2016 ISSUE 9

CNA We can show you more.®

NSO

HPSO

Cyber Liability: Minimizing the Risk 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 actual occurrences illustrate some of the more common causes of a data breach:

- *An Alabama counseling firm reported the potential disclosure of over 900 names of clients*, together with their healthcare records, Social Security numbers and medical insurance information. The cause: theft of a computer containing the data from an employee's car.
- *A California ambulatory community health clinic notified more than 4,800 patients and both current and former employees of the unauthorized release of their names*, as well as corresponding medical record numbers, birth dates and medical procedures. The cause: a former employee's improper access to information stored on the clinic's computer network.
- *A New York practitioner reported the disclosure of approximately 15,000 patient names*, plus related addresses, appointment dates and Social Security numbers. The cause: on a mass email, a staff member inadvertently attached patient information instead of a coupon advertising discounted medical care. The "eblast" with the spreadsheet was sent to an unknown number of recipients.

The potential consequences of a data breach range from sizeable monetary penalties (which are not necessarily covered by professional, property or general liability insurance policies) to negative publicity, disruption of routine, loss of public trust and possible patient harm, if medical data integrity is compromised. This edition of *Healthcare Perspective* examines the legal context, magnitude and causes of healthcare-related data breaches; suggests strategies for preventing and managing improper disclosures; and lists a variety of relevant resources. In addition, a self-assessment tool on pages 4-5 examines data security policies and controls.

SCOPE AND LEGAL BACKGROUND

The number of patient health records compromised in HIPAA-related data breaches increased 138 percent between 2012 and 2014. The breaches occurred in a wide range of settings, including general hospitals, outpatient facilities, private practices, pharmacies and health plans.

These inappropriate disclosures, involving the medical and/or personal data of as many as 45 million persons, are reported to the U.S. Department of Health and Human Services (HHS) in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted in 2009 as part of the American Recovery and Reinvestment Act. Under this law, the "covered entity" (i.e., a healthcare provider, plan or clearinghouse) is often required to take corrective actions following healthcare-related data breaches, which may include:

- Mitigating alleged or potential harm to patients or other parties.
- Imposing sanctions – which may include reprimands, suspensions or terminations – on staff members responsible for the breaches.
- Revising lax policies and procedures.
- Enhancing employee training.
- Correcting other problems identified during the investigation.

HITECH reinforces the HIPAA Privacy Rule 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. HITECH also empowers state attorneys general to sue for damages on behalf of state residents who have been threatened or adversely affected by violations of the law, as well as to enjoin statutory violations.

The law further requires notification following disclosure of "unsecured" PHI by business associates of HIPAA-covered entities.[1] Within 60 days of discovering a breach, business associates – such as staffing agencies and third-party vendors – must inform the covered entity of any person whose PHI may have been improperly accessed. The covered entity is then responsible for notifying affected individuals.[1]

DATA BREACH CAUSES

The HHS Office for Civil Rights categorizes breaches into five groups, 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 smartphones.
- *Loss of paper or electronic records,* including laptops and data storage devices.
- *Unauthorized access to PHI,* including external hacking, "malware" infection and illicit employee-related exposures.
- *Human or technological miscues,* including erroneous mailings and email or network server glitches.
- *Improper disposal of paper records,* generally involving errors made by a billing service or other vendor.

Approximately 20 percent of the reported incidents, comprising more than half of the total records disclosed, involve outside contractors hired by the covered entity. Loss or theft of unsecured data account for about 55 percent of breaches, compared with only 7 percent caused by hacker infiltration.[2]

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 within the organization. A variety of programs are available to assist in this task, including the Department of Homeland Security's Cyber Security Evaluation Tool (CSET®) and the OCTAVE® information security assessment approach.
- *Educate staff regarding the scope of federal and state privacy and notification requirements.* Basic HIPAA regulations should be integrated into employee orientation and training. Training sessions should explain the causes of data breaches and describe the consequences of neglecting to observe established data security policies, such as:
  - Disclosing PHI to anyone outside the organization who does not have a right to know.
  - Removing PHI from the facility without permission.
  - Failing to log out when leaving a workstation.
  - Leaving confidential information displayed on a screen.
  - Sharing or writing down passwords.
  - Keeping laptops or storage devices in an unlocked vehicle or otherwise exposing them to theft.

The critical first step in enhancing data security is to identify system vulnerabilities and account for how PHI is managed and secured within the organization. A variety of programs are available to assist in this task.

1 HITECH defines "unsecured PHI" as protected health information that has not been rendered unreadable, unusable or indecipherable through the use of a technology or methodology specified by the secretary of HHS. *42 U.S.C.A. § 1320d-5 (d.)*

2 For additional information on data breach causes, see the Ponemon Institute LLC's **"Fifth Annual Benchmark Study on Patient Privacy & Data Security,"** May 2015.

- *Safeguard record storage space.* To reduce the possibility of theft or sabotage, periodically reevaluate and, if necessary, revise security measures for 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. These user logs should be carefully monitored. In addition, accounts should have suitably complex, regularly changed 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, and language should be 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 adequate cyber liability insurance* to address data- and privacy-related coverage gaps. Such specialized products can provide coverage for third-party liability (e.g., certain fines, indemnity payments and associated legal expenses), as well as for certain reimbursement costs and first-party losses (e.g., notification costs, system restoration expenses and credit monitoring for affected parties, if warranted). See the sidebar at right for additional information about cyber liability coverage.

In an age of electronic health records, stringent privacy regulations, and widespread concern about identity theft and Medicare fraud, information security has become a major risk management priority. Leaders of every type of healthcare entity should evaluate their overall cyber exposure, create a plan to secure confidential information and minimize the impact of a potential breach, and obtain appropriate insurance coverage.

RESOURCES

- American Health Information Management Association (AHIMA).
- Breach notification rule from HHS.
- HHS's comprehensive, up-to-date listing of data breaches affecting 500 or more individuals.
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC).
- Collman, J. and Grimes, S. "What Healthcare Executives Should Know and Do About Information Security." A white paper from the Healthcare Information and Management Systems Society (HIMSS), revised October 2013.

Cyber Liability Insurance Coverage from CNA

To help insure healthcare practices against liability associated with privacy and confidentiality laws, Healthcare Providers Service Organization (HPSO), Nurses Service Organization (NSO) and American Casualty Company of Reading, Pennsylvania, a CNA underwriting company, offer $25,000 of privacy injury coverage related to data breaches and other related incidents. Several additional important coverages, known collectively as Enterprise Privacy Protection (EPP), are also available. The EPP endorsement, which has a $25,000 limit of liability, is available for purchase at an affordable annual premium of $100.

Note that some restrictions apply. This coverage is not available to all healthcare business entities.

Self-assessment Tool: Data Security and Patient Privacy

The following risk control recommendations are designed to aid healthcare business owners seeking to assess and enhance their data security risk control practices. For additional tools and information, visit the websites of CNA, NSO and HPSO.

AREAS OF CONCERN	STATUS	COMMENTS
RISK CONTROL STRATEGIES: STAFF		
Do staff members obtain thorough, up-to-date education and training about security- and privacy-related policies and procedures, and is this training: - Performed upon hire and annually thereafter? - Tailored to employees' job description? - Documented in employees' education files?		
Are employees encouraged to report procedural lapses and other events that could result in a security or confidentiality breach?		
Are employees held accountable for safeguarding patient privacy and confidentiality, and are they empowered to take appropriate action to secure sensitive information?		
Are information technology access and authorization lists periodically reviewed, and are individuals who no longer require access promptly removed?		
Is staff compliance with security policies and controls closely monitored and audited on a periodic basis?		
RISK CONTROL STRATEGIES: PHYSICAL AND ELECTRONIC		
Are basic security measures in place, including locks on doors and windows, as well as surveillance/monitoring cameras for entrances, exits and areas containing sensitive information?		
Is an inventory maintained of all systems, devices and media that could potentially contain protected health information, including desktop computers, laptops, flash drives, printers, copiers, tablets and smartphones?		
Is there a visitor log to record: - Names of all visitors to patient care and business areas, including family members and contractors? - Time of visit? - Reason for visit?		
Are physical and electronic safeguards in place to secure workstations and prevent inappropriate access to PHI, such as use of locked doors, cameras, keyed or fingerprint access systems, screen barriers, passwords, firewalls, etc.?		
Are workstations located in secured and monitored areas and positioned correctly to protect against theft, unauthorized use and improper viewing of screens?		
Are employees reminded to sign off on workstations when they step away, and do monitors automatically switch to a neutral screen following a period of inactivity?		
Are policies and procedures in place regarding office keys, as well as passwords, lock combinations and other access controls?		
Are locks re-keyed and combinations changed promptly when necessary – e.g., after a key is lost, a combination is compromised or a staff member departs?		

AREAS OF CONCERN	STATUS	COMMENTS
RISK CONTROL STRATEGIES: SECURITY POLICIES AND PROCEDURES		
Is there a written data security plan, and is it regularly reviewed and updated?		
Are there rules governing the use of outside computers, as well as security standards for these computers?		
Are policies established regarding safe and secure disposal of electronic devices, as well as media potentially containing electronic PHI?		
Is electronic PHI removed from electronic equipment and media prior to disposal or offsite maintenance?		
Is there a logging process for business-owned mobile devices and media containing PHI, in order to track both where these devices are located and who has possession of them?		
Are records maintained of employees' personal electronic devices and media, if they may be used to access or store electronic PHI?		
Are security policies in place governing use of laptops and tablets, if these devices are employed for purposes of patient documentation?		

CNA

1-888-600-4776 www.cna.com/healthcare

nso HPSO

1-888-288-3534 www.nso.com www.hpso.com

Healthcare Perspective is a limited-edition publication for healthcare business owners. This series explores a range of relevant risk management concepts and offers strategies to detect and mitigate risks.

Published by CNA. For additional information, please contact CNA at 1-888-600-4776. The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situation. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. "CNA" is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporation subsidiaries use the "CNA" service mark in connection with insurance underwriting and claims activities.

Healthcare Providers Service Organization and Nurses Service Organization are registered trade names of Affinity Insurance Services, Inc. (AR 244489); in CA & MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services Inc.; in CA, Aon Affinity Insurance Services, Inc. (0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency; and in NY, AIS Affinity Insurance Agency.

Published 4/16. *Healthcare Perspective* 2016-9.