



Compliance - TODAY

May 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Meet Scott Killingsworth

Partner in the Atlanta offices
of Bryan Cave LLP

See page 16



25

**Medicare
Coverage
Analysis:
Protecting your
institution**

Alexandra Burleigh

31

**How
does
your RAC
stack
up?**

Jason T. Lundy

36

**Complying
with the new HIPAA
Omnibus Rule:
Part 1**

Adam H. Greene, Rebecca L. Williams,
Louisa Barash, and John Hodges-Howell

43

**The Lilly FCPA
enforcement
action:
Key lessons
learned**

Thomas Fox

by Lucia Francesca Bruno, JD, LLM, MBA, CHC

The data breach dilemma: Steps providers can take to secure PHI and EHR

- » Conduct periodic audits to identify areas of risk related to information privacy and data security.
- » Institute role-based access controls that limit access permission to the need-to-know and specific job functions within the organization.
- » EHR should be encrypted to help protect patient data and periodic reviews of audit trails will help expose system abuse or misuse, before a breach occurs.
- » Once PHI has been de-identified, the restrictions and requirements of federal and state privacy laws no longer apply.
- » Reinforce a common sense approach to data security and stress personal accountability for the loss, misuse, and/or theft of computers, laptops, and other portable electronic devices.

Lucia Francesca Bruno (lbruno@physicianslegalgroup.com) is Principal with Physicians' Legal Group, LLC in Philadelphia and an Adjunct Professor of Law with Health Law Institute, Widener University School of Law in Wilmington, DE.

Each year millions of records containing protected health information (PHI) are exposed through malicious or inadvertent data breaches. Given the sheer volume of PHI that passes through the hands of providers, the question is not if—but when—a data breach will occur.



Bruno

The mere implementation of an electronic health records (EHR) system does not necessarily decrease liability exposure. On the contrary, the risk of liability may actually increase, especially where poor documentation practices and insufficient security measures jeopardize data integrity. Fortunately, there are several steps providers can take to ensure that PHI and EHR are kept safe and private.

What is a data breach?

Simply put, a data breach is the intentional or unintentional release of secure information into an untrusted environment.¹

The Health Information Technology for Economic and Clinical Health Act (HITECH) defines a “breach” as “the unauthorized acquisition, access, use or disclosure of PHI, which compromises the security or privacy of the information.” HITECH further defines “compromises” as that which “poses a significant risk of financial, reputational or other harm” to the individual who is the subject of the incident.”²

A data breach occurs when PHI is improperly disposed of or lost after a laptop, tablet, or portable memory device is mislaid by or stolen from a non-suspecting employee. A large-scale data breach not only impacts patients, but it can irreparably harm a provider’s reputation and compromise the fiscal health of the organization. Given the long-reaching effects of a breach, it is imperative that providers take the necessary measures to prevent a breach before one occurs.

Back to the basics – HIPAA and HITECH

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule established a set of standards for the protection of certain health information. A major goal of the

Privacy Rule is to ensure that a patient's health information is properly protected while balancing the need to promote the flow and exchange of health information so that quality health care services can be provided.³

Conversely, HITECH expanded HIPAA's privacy and security protections and provided administrative regulations which lead to a national EHR infrastructure. HITECH also included Medicare/Medicaid incentives for EHR adoption, commonly known as "meaningful use" incentives, as well as data breach notification requirements for unauthorized use and disclosure of unsecured PHI.

Although HITECH gave patients more control over their PHI, it simultaneously increased the risk to providers who manage and transmit PHI during the regular course of business.

What's at risk?

Despite its very nature, PHI has not been the target of most electronic privacy breaches; rather, data that can be used for financial fraud and identity theft, such as Social Security numbers, are the highest risk.

In a joint survey recently published by the Society of Corporate Compliance and Ethics, and the Health Care Compliance Association, nearly 60% of respondents' organizations admittedly suffered a data breach incident within the last year, and 20% suffered four or more. Among the most common causes were lost paper files and misplaced portable memory devices by employees, not database intrusions by skilled hackers.

Past lessons, future avoidance

Despite the growing number of incidents, few data breaches rise to the level of national headlines; those that do serve as examples to providers nationwide. In March 2012, BlueCross BlueShield of Tennessee (BCBST) was slapped with a \$1.5 million fine from the U.S. Department of Health and Human Services (DHHS) after 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the PHI of more than one million individuals, including names, Social Security numbers, diagnosis codes, dates of birth, and health plan identification numbers.

In a separate incident, Massachusetts General Hospital paid a hefty \$1 million to settle a data breach resulting in the impermissible disclosure of PHI containing patients' names, dates of birth, medical record numbers, and health insurer information. The documents were lost when a Massachusetts General employee left the documents on the subway while commuting to work. The documents were never recovered.

Furthermore, in June 2012, the Alaska Department of Health and Social Services (DHSS) agreed to pay HHS \$1.7 million to settle an alleged HIPAA violation following a breach report submitted by Alaska DHSS pursuant to HITECH. The report revealed that a portable electronic storage device (USB hard drive) containing ePHI was stolen from an employee's vehicle.

In light of the considerable risks, providers must take necessary measures to maximize

Despite its very nature,
PHI has not been the target
of most electronic privacy
breaches; rather, data that
can be used for financial
fraud and identity theft,
such as Social Security
numbers, are the
highest risk.

the security of PHI and EHR. Although there is no way to completely eliminate a breach, there are several steps providers can take to mitigate the risk of a breach.

Business ethics and compliance

To ensure the security of data within an organization, it is important to address the compliance program upon which security guidelines are based. Prior to the implementation of security measures, providers are encouraged to incorporate an EHR policy into their existing business ethics and compliance program. In addition to implementation strategies, the EHR policy should address the detection and prevention of violations of federal and state laws related to EHR data.

Although organizational structures differ among providers, where applicable, the policy should designate a chief privacy officer (CPO) or health information management (HIM) professional to ensure accurate documentation practices are followed. Both CPOs and HIM professionals should be given leadership roles within the organization, and be responsible for maintaining effective lines of communication related to information privacy and data security. Within this capacity, the CPO or HIM professional must educate employees regarding data integrity, enforce disciplinary guidelines with respect to privacy issues, monitor and audit areas of risk within the organization, and promptly respond to offenses with appropriate corrective action.

One of the most basic security measures to protect information data is known as role-based access control (RBAC), which uses permissions and rights that are assigned to specific roles within the organization as a means of controlling access to data.

Role-based access control

One of the most basic security measures to protect information data is known as role-based access control (RBAC), which uses permissions and rights that are assigned to specific roles within the organization as a means of controlling access to data. RBACs don't take into account access rights of individuals; instead, roles are assigned to users based on their need-to-know and specific job functions.

Although RBACs are an effective measure to protect patient data, given the increase number of medical institutions and the rights afforded to patients under HIPPA to regulate access to PHI, many providers have found that

RBACs are frequently difficult to detail and are, therefore, opting for an EHR digital rights management system known as an RBAC-Matrix. Such a system not only allows patients to determine access rights to their PHI, but also authorizes access control among matrix organizations of medical institutions by using an XrML file associated with each EHR.⁴ This two-stage protec-

tive system simultaneously enhances data security while promoting the declaration of rights and use of EHR in compliance with HIPAA specifications.

Data encryption

The two final rules for Stage 2 of HITECH address encryption and other privacy and security issues. This is relevant, because at least one-third of all breaches occur from

lost or stolen data locally stored on end-users devices, such as backup drives, laptops, and other mobile devices.

In the most simplistic terms, encryption is the conversion of data into a form (called cipher text) which cannot be easily understood by unauthorized persons. Conversely, decryption is the process of converting the encrypted data back into its original form so it can easily be understood. The stronger the cipher, the harder it is for unauthorized persons to break; however, as the strength of the encryption/decryption increases, so does the cost.

Under the meaningful use rule developed by the Centers for Medicare & Medicaid Services (CMS), participants are required to conduct a risk assessment analysis to address “the encryption/security of data stored in certified electronic health records technology” (CEHRT). The rule also requires providers to “implement security updates as necessary, and correct identified security deficiencies as part of the provider’s risk management process.”⁵

Farzad Mostashari, MD, National Coordinator for Health Information Technology at DHHS, recently asserted that “the meaningful use rule continues to reaffirm the importance of doing security assessments and mitigation.” He further encouraged providers to “make certain to follow all administrative and physical safeguards, as well as technical safeguards.”⁶ Together, these safeguards will significantly decrease the risk of a data breach.

One important distinction between EHR and de-identified PHI is the stripping of identifiers linked to the information. When PHI has been de-identified, restrictions and requirements of federal and state privacy laws no longer apply...

De-identification of PHI

Although slightly different in nature, the de-identification of PHI has become yet another tool in the arsenal against data breaches. One important distinction between EHR and de-identified PHI is the stripping of identifiers linked to the information. When PHI has been de-identified, restrictions and requirements of federal and state privacy laws no longer apply; however, it is important to keep in mind that if re-identification codes are added to the data, certain privacy and security rules remain in effect.

On November 26, 2012, the Office for Civil Rights (OCR) issued guidance on the de-identification of PHI. The guidance addressed both the expert determination and safe harbor methods carved out by Section 164.514(a)-(b) of the Privacy Rule. Subject to these methods, health information is not individually identifiable if it does not identify the individual, and the covered entity has no reasonable basis to believe it can be used to identify the individual.

Expert determination method

Under Section 164.514(b)(1), a covered entity may determine that PHI is de-identified only if:

a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable... determines that the risk is very small that the information could be used alone, or in combination with, other reasonably

available information, by an anticipated recipient to identify an individual.

Although the OCR does not mandate a particular method be used by the expert, ordinarily the de-identification process consists of the following:

- ▶ A statistical sampling and analysis to determine the extent to which the information can, or cannot, be linked back to the identity of the patient;
- ▶ Guidance to providers on which statistical or scientific methods can be applied to mitigate the risk of identification; and
- ▶ An evaluation of the de-identified information to confirm that the risk is no more than very small when disclosed to anticipated recipients.

Safe harbor method

The second way that PHI may be de-identified is called the safe harbor method. Under Section 164.514(b)(2), the covered entity may de-identify PHI by removing 18 specific identifiable elements relating to the individual subject of the information or relatives, employers, or household members of the individual, and the covered entity must have no actual knowledge that the de-identified information could be used alone or in combination with other information to identify an individual who is the subject of the information.

Audit trails

Audit trails track activities within EHR, allowing for the identification of the following:

- ▶ Who accessed the data
- ▶ When the data was accessed
- ▶ What operations were performed within the data

Periodically reviewing audit trails can alert administrators to potential system abuse, or misuse, within an organization.

Documented events in audit trails include staff members:

- ▶ logging in or out of the system;
- ▶ opening, modifying, creating, or deleting records;
- ▶ scheduling patients;
- ▶ signing charts;
- ▶ querying the system; or
- ▶ printing PHI.

Due to its confidential nature, only authorized administrators should have access to audit trails and no one, not even office administrators, should be able to modify or delete the audit trails.

Common sense precautionary measures

Like the age-old adage “An ounce of prevention is worth a pound of cure,” common sense precautionary measures remain the best way to avert a data breach.

Employees should be cautioned that computer screens must not be visible from waiting rooms, check-in areas, or anyplace an unauthorized person might be able to see a patient’s EHR. Additionally, passwords for system access should never be posted or written down near an employee’s desk.

Providers must remain vigilant and stress the importance of data security throughout the organization. As simple as it sounds, it is important to remind employees to maintain control of documents and portable electronic devices at all times. Periodically educate and train employees on information security policies and procedures, and stress the consequences of desktop, laptop, and portable device misuse or theft. ☑

1. http://en.wikipedia.org/wiki/Data_breach
2. 45 C.F.R. § 164.402.
3. Summary of the HIPAA Privacy Rule. Available at www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html#endnotes
4. HC Lee, SH Chang; RBAC-Matrix-based EMR Right Management System to Improve HIPAA Compliance. TamKang University, New Taipei City, Taiwan, September 2011. Available at <http://www.ncbi.nlm.nih.gov/pubmed/21882003>
5. Federal Register, Vol. 77, No. 171, September 4, 2012 /Rules and Regulations, HHS
6. Howard Anderson: HITECH Stage 2 Rules Unveiled, *Data Breach Today*, August 23, 2012. Available at <http://www.databreachtoday.com/hitech-stage-2-rules-unveiled-a-5060>