HBMA
Healthcare
BILLING & MANAGEMENT
Association

Billing

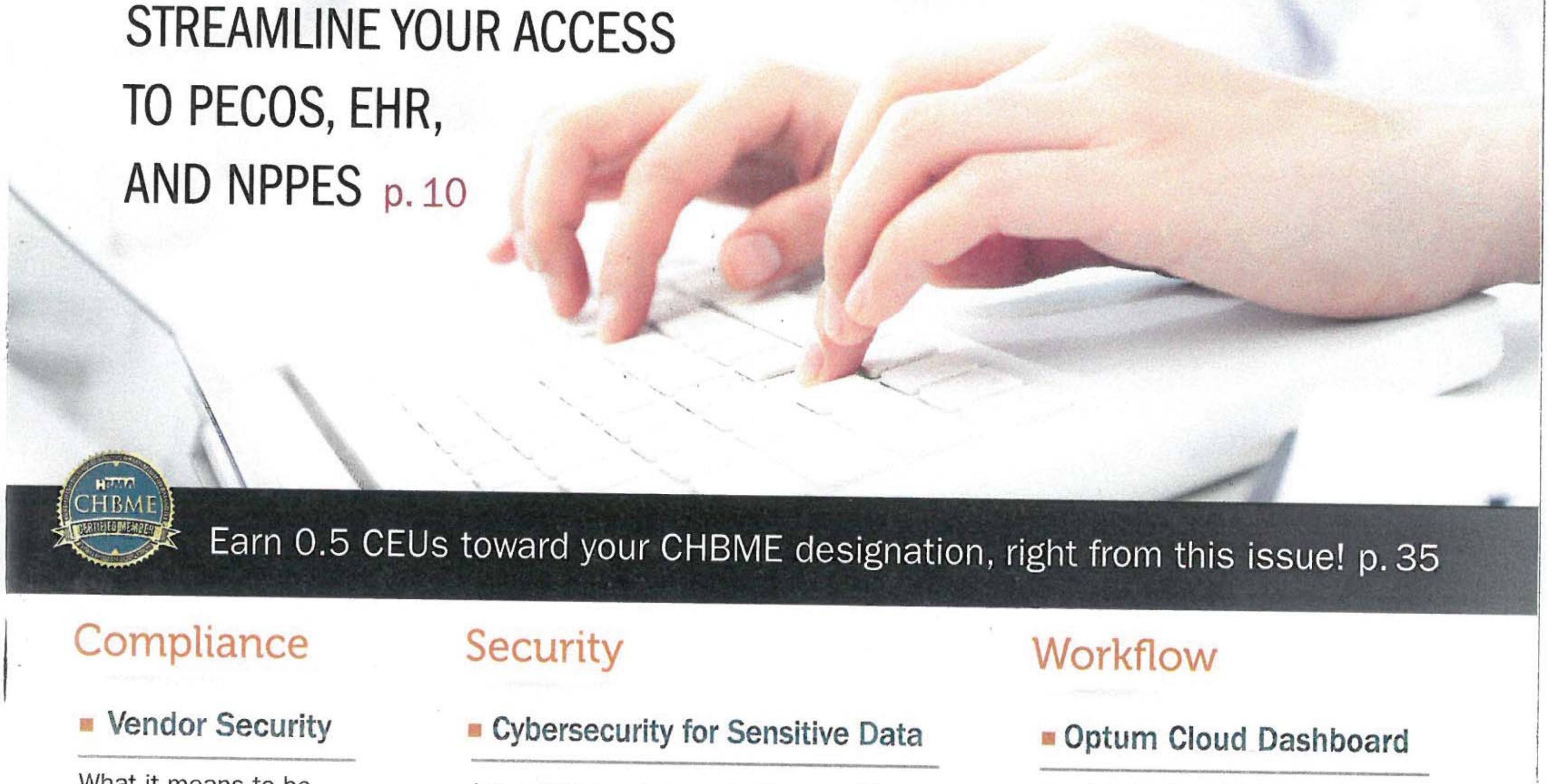
The Journal of the Healthcare Billing and Management Association

VOLUME 20 • JANUARY.FEBRUARY.2015

INDUSTRY TOOLS

Life Made Easier with CMS's Surrogacy Program

STREAMLINE YOUR ACCESS
TO PECOS, EHR,
AND NPPES p. 10



Earn 0.5 CEUs toward your CHBME designation, right from this issue! p. 35

Compliance

Vendor Security

What it means to be HIPAA compliant. p. 15

Security

Cybersecurity for Sensitive Data

A new framework for protection. p. 18

Workflow

Optum Cloud Dashboard

Administrative efficiencies for healthcare professionals. p. 21

MORE!

President's Message: Help HBMA Remain Strong in 2015 • **ICD-10:** Don't Let the Coding Get Lost in Translation
Excel Shortcuts: Business Intelligence for Medical Practices • **From the Road:** You Can't Do It All Yourself

Cybersecurity for Sensitive Data

By Harry Stephens

A NEW FRAMEWORK FOR PROTECTION

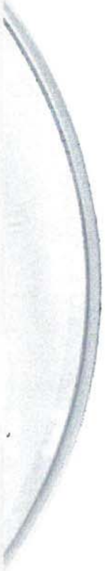
Recent large-scale data breaches at high-profile retailers have focused a lot of attention on the topic of data security. The question of how to keep sensitive data safe is one that every industry faces, but nowhere is it more important than in the healthcare industry, which by its very nature collects, stores, and shares a massive amount of confidential personal data.

Early this year, the National Institute of Standards and Technology (NIST) issued its "Framework for Improving Critical Infrastructure Cybersecurity." The Framework outlines best practices for enterprises of all types that work with and hold their clients' personal data. Because NIST's recommendations are high level and general in nature, they are applicable to every enterprise that works with very sensitive customer information.

However, it is wise to bear in mind that computer hackers probably are not your greatest risk. Vulnerabilities that exist within your own operations frequently lead to accidental privacy violations that can be equally damaging. For example, these vulnerabilities can include people taking work home with them via laptops or portable USB devices that might also house customer data or proprietary information about your systems and operations. Furthermore, mistakes such as accidentally diverting monthly statements to the wrong address can expose sensitive information. As a result of these and other possibilities, it is important to determine how well your organization identifies and tackles all the risks involved in data loss.

The Framework provides a detailed method for reviewing your organization's practices and establishing a proactive system for cybersecurity. It prioritizes the relevant issues and considerations, and classifies them into what it calls "tiers." The following are what the Framework considers the five core elements of data security:

- IDENTIFYING THE RISKS. In the broadest sense, this means understanding the context of your healthcare organization,



the resources involved in your operations, and the related risks to your IT functions. This component provides an overview of your particular situation, including asset management, business environment, governance, risk assessment, and risk management strategy.

- **PROTECTING THE DATA.** This covers the means of controlling access to systems and data, employee awareness and training, data security, information protection processes and procedures, maintenance, and protective technology. An example would be ensuring access to patient-related data is limited to only the staff members who need to see it – and/or only designated segments of it. This can be achieved at least partly through password systems that are rigorously tracked and updated as an employee's status changes.
- **DETECTING ANY BREACHES.** To avoid unhappy surprises, develop monitoring systems specific to where and how your data is stored and utilized, and explore methods to trigger alerts if the information has been accessed without authorization. NIST suggests tracking and recording any anomalies.
- **RESPONDING TO ANY BREACHES.** This refers to developing ways to contain the impacts of any security breach, including putting a plan in place ahead of time to cover communications within your organization and with clients, providing a careful and meticulous analysis of what happened and how, and using this information to improve cybersecurity in the future.
- **RECOVERY.** These are the steps taken after your immediate response, such as recovering any lost data, and also learning what you can from the incident for better planning in the future, in addition to ongoing communications with those affected by the breach and improving existing security procedures.

> It's best to have a plan in place and in operation all the time, with **procedures that you can instantly implement** if a data breach has been detected.

As NIST advises, it's best to have a plan in place and in operation all the time, with procedures that you can instantly implement if a data breach has been detected. You never know when, or in many cases how or why, a breach may occur. Because of the possible negative consequences, it's critical to take all of the above issues into account so that you can act immediately to minimize the impact.

Although the NIST Framework is a recommendation and not a regulation, all enterprises that hold or transmit sensitive customer data are held to a variety of local, federal, and international regulatory mandates relative to information security.

For improved efficiencies, many financial institutions, utilities, healthcare providers, and others that handle high volumes of private information have chosen to outsource their electronic document processing, billing, and distribution solutions to a third-party provider. But how can you be certain that third-party partners are certified in operational excellence and security?

Know Who's Handling Your Data

Any provider of print and electronic billing solutions should follow the industry standards that are essential for security compliance. Here are the top three standards relevant to processing financial data:

1. **STATEMENT ON STANDARDS FOR ATTESTATION ENGAGEMENTS NO. 16 (SSAE 16) CERTIFICATION** – SSAE 16 is an accreditation awarded by the American Institute of Certified Public Accountants (AICPA) and ensures that all outsourced documents are handled in a secure, reliable, and stable environment with tight process controls in place.

   A financial processing service provider that has attained SSAE 16 compliance offers reliable evidence of the following:

- The service provider's management has made a written assertion that gives a fairly presented description of the services provided by the service organization, along with the supporting processes, policies, procedures, personnel, and operational activities that constitute the service organization's core activities that are relevant to its customers.
- The control objectives were suitably designed (SSAE 16 Type 1) and effectively operated (SSAE 16 Type 2) during the dates/periods covered by the attestation.
- The criteria used for making the assertions were in place (Type 1) and were consistently applied (Type 2).

2. **PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) COMPLIANT** – The PCI DSS is a globally instituted security standard for all merchants and service providers who accept credit card information; it is designed to keep customer payment card data secure and prevent payment cardholder data fraud.

   Working with a financial processing service provider that is PCI DSS compliant ensures that your customer payment data is secured at the highest level, eliminating the need for your organization to undertake the costly and time consuming process of obtaining PCI DSS compliance itself.

Protecting and ensuring security compliance and due diligence is a **never-ending process**.

3. **SARBANES-OXLEY (SOX)** – Any service provider fully trained in SOX regulations will help ensure that its clients are compliant with all corporate accounting controls required by US federal law.

Check the Locks

Not all security precautions are enshrined in legislation or can be officially certified. At a minimum, high-volume billers should make sure that they and the service provider they choose have stringent internal security measures in place to protect customer data. Check on whether production areas are locked and monitored at all times. Make sure FTP servers are protected by a highly rated hardware firewall to eliminate unwanted intrusions. Additionally, all electronic payment options need to be encrypted and performed over a secure SSL internet connection.

Many of today's electronic billing solution providers offer a number of additional security features, including biller authentication and non-repudiation of bills, as well as security tokens in addition to or in place of a password that acts like an electronic key. These measures help assure customers their confidential information remains intact.

Lastly, it is imperative that the company you choose to handle your sensitive information has a comprehensive disaster recovery program in place to safeguard against fire and other natural and environmental hazards.

An Ongoing Process

Protecting and ensuring security compliance and due diligence is a never-ending process. As NIST suggests, any data breach, or even suspected breach, can help you further identify vulnerabilities and improve your procedures. But, it seems that there is no fence high enough to ensure 100 percent security. The best we can do is enforce 24/7 monitoring of all data, networks, and internal processes, while employing the best tools and practices available. To avoid potential fines, loss of customers, bad publicity, and legal action, make sure you have covered all your security bases and that your program is well executed and monitored by an independent, third-party auditor who knows what to look for and can make useful suggestions for improvement. ■

Harry Stephens is president, CEO, and founder of DATAMATX, one of the nation's largest privately held, full-service providers of printed and electronic billing solutions. As an advocate for business mailers across the country, Stephens is actively involved in several postal trade associations. He serves on the executive board of the Greater Atlanta Postal Customer Council, Major Mailers Association (MMA), PCC Advisory Committee (PCCAC), and the Board of the National Postal Policy Council (NPPC). He is a board member of The Imaging Network Group (INg), an association for Transactional and Direct Mail Marketing service bureaus. As an expert on high-volume print and mail, he has frequently been asked to speak to various USPS groups. You can contact Harry Stephens at hstephens@datamatx.com.