Publication of Medical Mutual / Professionals Advocate®

DOCTORS Rx

Volume 22 No. 2 Winter 2014

A Letter from the Chair of the Board

Dear Colleague:

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities conduct a risk assessment of their health care organization.

This issue of* Doctors RX *will provide you with information as to what is required and why.

George S. Malouf, Jr., M.D.
Chair of the Board
Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

Do You Know Your Practice's Data Security Risks?

How would your practice answer the following questions?

What would it mean to your practice if you lost access to your computer systems and the patient data on them? For a week? Permanently? Could you run the office? Could you continue to see the same number of patients? Could you capture the information you need to provide care and get paid? How long would it take to recover from such an event? Would you have to re-interview patients to get key medical data?

What if a copy of the computerized data about your patients was taken by a disgruntled former employee and posted on the Internet or used for credit card fraud? Are you prepared to respond to this event?

These situations are not hypothetical. They are based on real scenarios that some health care providers have already experienced. Hardware and software failures, hackers, and employees compromise businesses every day. Setting up a security program with procedures to manage these threats is necessary for a medical practice operating in today's computerized environment.

With the recent implementation of the Omnibus Rule and its HIPAA/HITECH pronouncements, the importance

Continued on next page

John Parmigiani
President, John C. Parmigiani and Associates, LLC

of being aware of where your practice's Protected Health Information (PHI) resides, how it is safeguarded, and how the risks are managed becomes of utmost importance.

This issue of *Doctors RX* will address the critical need for your practice to undergo a risk assessment – not only for regulatory compliance but also, and more importantly, as an essential business practice in today's health care environment.

How Did We Get Here? The HIPAA Path to eHealth

From the outset, the major intent of the Federal Government for the Administrative Simplification portion (Title II, Subtitle F) of HIPAA was to improve the management and delivery of health care through improved use of communication that leverages the most economical and secure creation, transmission, storage, and retrieval of electronic health care data. The initial requirements of HIPAA were intended to set the stage for the advent of fully electronic health care records, patient safety initiatives, enhanced clinical decision support, and improved medical research. In short, HIPAA was to provide a foundation for the construction of a robust eHealth environment. Full implementation of these standardized approaches was also to yield substantial, measurable return on investment from electronic commerce applications to health care delivery and management. In early 2013, the U.S. Department of Health and Human Services issued its final rule modifications (the Final Omnibus Rule) that implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under HIPAA.

With the recent upswing in federal and state patient data regulatory mandates and the refined and strengthened requirements in the newly implemented Omnibus Rule ("the Rule"), there is added emphasis on safeguarding patient information both "at rest" and "in transit." The major changes of the Rule fell under several broad impact categories, which include changes to the privacy rule, breach notification rule, and a new definition of business associates of covered entities. These changes are discussed in detail in the Fall 2013 issue of *Doctors RX*. Visit mmlis.com or proad.com to view a digital version of the newsletter.

Your medical practice has a regulatory as well as a practical concern. In recently released statistics by the Office for Civil Rights of the Federal Department of Health and Human Services, private practices received the highest number of corrective action notifications of all of the types of provider-covered entities. The two highest sources of privacy compliance issues involved the impermissible uses and disclosures of protected health data and the lack of safeguards for protected health information.

The Importance of Trust in Delivering Health Care

Let's imagine a near future, where the patient experience is almost entirely electronic:

A patient visits a Physician, where he or she registers with the swipe of a card. The Physician then enters information, orders tests, prescribes medication and enrolls the patient in a clinical trial – all on an electronic point of care device. Lab tests are submitted and reported electronically. Medications are manufactured in batches and sent via electronic order to maintain a ready supply. Medical claims are submitted, paid and recorded electronically. The clinical trial data is managed, signed and submitted electronically. The patient carries a personal health record on electronic media that is easily synchronized with an electronic record. The patient data is accurate, current and secure. It can be shared with authorized caregivers through national and regional networks and is available for research and data mining applications.

This scenario can lead to improved patient safety, better access to care, improved outcomes, and technological advances in care and communication. However, these benefits come with universal concerns regarding the privacy of the patient and the security of the data. While several recent surveys support these concerns, there is also evidence that the general population sees the benefit of an electronic environment in improving its health status. Recent surveys by the California Healthcare Foundation (CHF) have found that approximately two-thirds of the adult population was concerned about the privacy of their personal medical records. However, subsequent surveys by CHF found that while there was still concern over patient privacy, there was also an awareness of the benefits of electronic medical records. Furthermore, experts such as the National Committee on Vital and Health Statistics have said that ensuring the security of digital health information is necessary to persuade the public to support health IT and for its eventual widespread adoption. There is further research and expert opinion on the criticality of strong privacy and security safeguards in the eHealth environment, where the key word becomes ***trust***.

Trusted relationships and communication among all parties – but especially between a patient and the Physician – becomes especially important when it comes to guarding electronic data. There is a need for a system that provides strong authentication to verify the identity and allow access to electronic Protected Health Information (ePHI) by only authorized users, strict access controls to restrict user access to ePHI based on need-to-know, and audit controls that identify who did what and when relative to ePHI. It is this life-cycle approach to data management, enveloping the sensitive data in a system that provides accountability throughout, which has become the sentinel requirement for electronic health care.

Of particular note is the wave that is sweeping across the U.S., spurred on by the seminal legislation in California in 2003 known as the California Security Breach Information Act. This law requires any alleged breach of identifiable information stored in an unencrypted database to be reported to all potential victims, and ensures necessary follow-up actions by the company with stewardship responsibility for protecting that data. The critical safeguard to this data, preventing many costly notification and damage control activities, is encryption of the stored data. As of this writing, these provisions have been replicated in at least 47 states, including Maryland, Virginia and the District of Columbia. Some of this mirroring has included even stronger data security and protection mandates in these venues.

Very recently, the FDA has entered into the safeguarding patient data arena by issuing new cybersecurity recommendations to help health care companies protect patient information that is stored on medical devices. With the health care system moving patients' medical records online, the FDA strongly believes this confidential information could be vulnerable to cyberattacks and security breaches that could compromise patient privacy.

Data Within the Practice

Operating in this fast-paced, data-centric environment requires the use of robust, user-friendly, and multi-functional practice management systems in Physician offices, regardless of the practice's size and volume. However, the most important features and attributes of the practice management system for the eHealth era focus on the information security that the system provides both to the practice and to the patients it serves. The sources of threats to the data are both internal and external. The insider threat is amplified when sensitive data are not protected from unauthorized users, when there is error or malicious handling, and when sensitive data are put on a mobile device that becomes lost or stolen. Typically, the outsider threat materializes through a physical break-in or through the network. Practice management systems need to be cognizant of these sources of data leakages and breach possibilities when they are designed. Physicians using the systems must also exhibit awareness and a dedication to identifying and managing their risks.

What the HIPAA/HITECH Security Rule Requires

The Rule was borne out of an environment where government and industry cooperation was both emphasized and instrumental, a degree of industry self-regulation was envisioned, and a continuous development process evolving from the creation and testing of various best practices approaches was encouraged. Emphasis on a framework that provided flexibility, scalability and technology neutrality was a critical success factor. Based upon good business practices, the standards are focused on what to do, not how to do it. The Rule requires:

1. The assignment of organizational responsibility for the security of its health information, and
2. The provision of reasonable and appropriate safeguards:
    a. to ensure the integrity, confidentiality and availability of all protected health information, which is created, received, maintained or transmitted in electronic form by a covered entity,
    b. to protect against reasonable anticipated threats or hazards to the security or integrity of this information,
    c. to protect against reasonably anticipated unauthorized uses or disclosures of this information by the organization, and
    d. to ensure compliance by the organization's workforce.
3. The formal assessment of risks to the confidentiality, integrity, and availability of health information by the organization, and
4. The implementation and documentation of specific Administrative safeguards, Physical safeguards, and Technical safeguards for protecting data both at rest and in transit.

CME Test Questions

Instructions for CME Participation

CME Accreditation Statement – MEDICAL MUTUAL Liability Insurance Society of Maryland, which is affiliated with Professionals Advocate® Insurance Company, is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.

CME Designation Statement – MEDICAL MUTUAL Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit.*™ Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Instructions – to receive credit, please follow these steps:

1. Read the articles contained in the newsletter and then answer the test questions.
2. Mail or fax your completed answers for grading:

   Med•Lantic Management Services, Inc.
   225 International Circle
   P.O. Box 8016
   Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.

   Fax: 410-785-2631

3. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
4. Completion Deadline: March 31, 2015
5. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

1. The HIPAA Security Rule requires the formal assessment of risks to the confidentiality, integrity and availability of health information by an organization.

   A. True B. False

2. Physicians don't need to be aware of data risks and security measures if someone else in their office is trained to manage their data systems.

   A. True B. False

3. An insider threat to protected data could include all of the following, EXCEPT:

   A. Malicious handling of data by an employee
   B. Someone breaking into an office and stealing files
   C. Data not being password protected from unauthorized users
   D. Mobile devices with sensitive data being lost

4. Which of the following are possible consequences of noncompliance with the HIPAA Security rule?

   A. Lost or corrupted data
   B. Insurance premium increases
   C. Fees associated with defending liability suits
   D. All of the above

5. A risk assessment must be quantitative to yield measurable results.

   A. True B. False

6. Legal actions for major health data breaches cost, on average:

   A. $1,000 per patient
   B. $5,000 per patient
   C. $10,000 per patient
   D. $15,000 per patient

7. Methods to mitigate data security risks include:

   A. Disaster recovery plans
   B. Business continuity plans
   C. Access and authentication controls
   D. All of the above

8. Business associates are held accountable for a lower level of protection of health information compared to the organization that is entrusting them with that information.

   A. True B. False

9. What type of entity receives the most HIPAA corrective action notifications?

   A. Hospital systems
   B. Private practices
   C. Outpatient clinics
   D. Nursing homes

10. The two highest sources of privacy compliance issues involve the impermissible uses and disclosures of protected health data and the lack of safeguards for protected health information.

    A. True B. False

CME Evaluation Form

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the insured Physicians of MEDICAL MUTUAL/Professionals Advocate.® Its mission and educational purpose is to identify current health care related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:
1) Gain information on topics of particular importance to them as Physicians,
2) Assess the newsletter's value to them as practicing Physicians, and
3) Assess how this information may influence their own practices.

CME Objectives for "Do You Know Your Practice's Data Security Risks?"

Educational Objectives: Upon completion of this enduring material, participants will be better able to:
1) Understand the HIPAA Security Rule requirements for risk assessment
2) Describe the components of a risk assessment
3) Understand the consequences of failing to protect ePHI

	Strongly Agree				**Strongly Disagree**
Part 1. Educational Value:	5	4	3	2	1
I learned something new that was important.	❑	❑	❑	❑	❑
I verified some important information.	❑	❑	❑	❑	❑
I plan to seek more information on this topic.	❑	❑	❑	❑	❑
This information is likely to have an impact on my practice.	❑	❑	❑	❑	❑

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

_____

_____

_____

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature: _____ Date: _____

Part 4. Identifying Information: Please PRINT legibly or type the following:

Name: _____ Telephone Number: _____

Address: _____

_____

_____

_____

HIPAA Security further requires that all personnel in the organization be trained in security policies and procedures, that business associates be held accountable for the same level of protection of the health information entrusted to them, and that the organization's policies, procedures, and practices are in concert with the intent of the security standards. For successful HIPAA Security compliance, the organization must be able to pass muster against both the standards as published and the industry benchmarks that have evolved to clarify the practical implementation and measurement of those standards.

Security breaches are on the rise as we evolve into a more intensive electronic health care environment. The challenge to health care organizations is to become proactive in preventing threats from causing adverse health and financial impacts. The trick is to minimize risk by using easily available and adaptable administrative, physical, and technical safeguards and to imbed them into daily business functions. This will help ensure that your staff works in concert with your policies, processes, and native system technologies to assure protection of sensitive data.

Consequences of the Failure to Protect ePHI

The HIPAA Security Rule (the "Security Rule") regulations specify that security measures must be in place to protect the confidentiality, the integrity, and the availability of electronic patient identifiable information. Non-compliance with the Security Rule can result in the following possible consequences:

- Lost reputation, negative publicity, lost business – patients seek out a new practice;
- Lost or corrupted data, along with associated recovery or replacement costs, time and resources after an incident occurs;
- Lost intellectual property;
- Consulting and legal fees associated with investigating and determining the extent of an attack;
- Legal and public relations fees associated with defending liability suits by failing to meet contract obligations or Federal and State regulations;
- Incident reporting requirements and resulting investigative follow-up on the organization; and
- Loss of trust in management and ownership with the potential for accreditation problems.

Additionally, loss of protected health information and its subsequent unauthorized access can result in the following potential harm to the patient:

- Identity theft of credit card and financial information;
- Medical identity theft – using another person's name, Social Security number, or insurance information to obtain medical services, stealing medical records to sell to undocumented immigrants for citizenship and medical services, or using someone else's identity to falsify insurance claims;
- Employment and societal impact and embarrassment; and
- The change in either the availability and/or the integrity of the patient's health care information with resulting adverse treatment outcomes including death.

There are numerous studies chronicling the costs associated with major health data breaches. A 2014 study by the Ponemon Institute found the average cost associated with health data breaches to be $359 per record.[1] This could entail a combination of notifying potential victims and follow-up for credit protection. It does not, however, include legal actions, which typically average about

$10,000 per patient, and potential Federal and State fines that range anywhere from $1,000 to $1.5 million per incident. **Of course, as pointed out earlier, under the Omnibus Rule the use of acceptable encryption methods eliminates the notification requirements and absolves the organization, even if it has not implemented appropriate safeguards.** The strongest activity that indicates earnestness on the part of a practice is to have documented proof of having conducted a risk assessment. This includes considering the priority and the stages of taking necessary actions to manage risks and to create and maintain sufficient security for the practice's sensitive data.

The Important Components of a Risk Assessment

A risk assessment is an in-depth data-gathering and analysis process focused on identifying what information needs to be protected, what are the possible threats, and the chances of occurrences that will exploit vulnerabilities and adversely impact the organization. The risk assessment examines the safeguards, controls, and countermeasures available to protect assets and keep risk at a manageable level while being compliant with various regulatory requirements. It is essential that those conducting a risk assessment understand the core business functions of the organization, and that it encompass an understanding of the organization's risk tolerance.

When undertaking a risk assessment, the following questions should be asked and answered:

- What needs to be protected?
- What are the possible threats?
- What are the vulnerabilities that can be exploited by the threats?
- What is the probability or likelihood of a threat exploiting vulnerability?
- What is the impact to the organization?
- What controls are needed to mitigate impacts and protect against threats?

Risk Mitigation

Items that need to be protected can include assets such as hardware and software, data and information about patients, financial information, and intellectual property. Consider also that acts of nature and man can threaten protected information resulting in vulnerabilities such as inappropriate internal or external access to personal health information. There are several ways to mitigate the risk of threats that may occur and their impact. Backup or disaster recovery plans, along with business continuity plans, can play a key role in mitigating acts of nature. Similarly, having proper policies, procedures, and training can mitigate unintentional acts of employees, for example accidentally sending confidential information to the wrong recipient. To mitigate intentional threats, practices can utilize access and authentication controls, audit trails, intrusion detection, and develop sanctions for staff who do not follow established protocol.

Once the risks to the practice are identified, prioritization becomes critical. One way of determining which risks need to be addressed first is through risk scoring. Risk scoring, which can either be qualitative or quantitative, is

Some Examples of Possible Risks Include:

- Cash flow slowed or stopped;
- Fines, penalties, imprisonment, and law suits;
- Loss or corruption of patient data;
- Unauthorized access and/or disclosure;
- Temporary unavailability of patient information;
- Loss of physical assets - computers, mobile devices, and/or facilities;
- Compromised patient and employee safety;
- Loss of certification; and
- Negative publicity.

necessary to identify mitigation responses and to develop and implement an appropriate risk management plan. Qualitative scoring is more universally applied due to its relativity and better understanding in generating priorities to correct and manage through a potential breach. The qualitative approach also readily lends itself to the major compliance guidance espoused by the Security Rule to "addressable" implementation specifications – coming up with safeguards that are "reasonable" and "appropriate," and that are defensible and make good business sense in the organization's environment. A brief by The American Health Information Management Association (AHIMA) offers examples of qualitative and quantitative approaches to a risk assessment.[2]

In summary, good security is good business. It can reduce the liabilities of any health care organization. More importantly, good security can contribute to the improved delivery of health care by raising the level of trust between the patient and the provider. Better information from the patient equips the health care provider with an enhanced ability to diagnose and treat. And lastly, as health care delivery evolves and becomes more dependent on efficiently and effectively functioning in an electronic universe, the conduct of daily business in a trusted environment becomes a necessary component of business survival. Full implementation and maintenance of the HIPAA/HITECH Security Standards, the first step of which, and the cornerstone for compliance, is the performance of a risk assessment and the creation of a subsequent risk management plan equals a win-win situation both for the practice and the patients it serves.

About the Author

John Parmigiani is President of John C. Parmigiani & Associates, LLC, and will be presenting a risk management education program, *Conducting a Security Risk Assessment*, for Medical Mutual at various locations in 2015. Details will be mailed in early February.

[1] Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis Report* at 7, May 2014.

[2] Walsh, Tom, *Security Risk Analysis and Management: an Overview (Updated)*, AHIMA Practice Brief, Updated January 2011.

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
Vice President - Risk Management

Dr. George S. Malouf, Jr., M.D., *Chair of the Board*
Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Numbers you should know!

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	800-492-0193
Risk Management Education Program Info	ext. 215 or 204
Risk Management Questions	ext. 224 or 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	mmlis.com proad.com

*e-data*RESPONSE+ Privacy Breach Coverage Available for Purchase

ProAd's *e-data*RESPONSE+ is a stand-alone privacy breach coverage product that offers substantial comprehensive protection in the event of a privacy breach. Should your practice experience a privacy breach, no matter the circumstances, you will be held legally responsible for the consequences. Basic privacy breach coverage, such as ProAd MedGuard *e-data*RESPONSE, can provide limited reimbursement for certain expenses incurred as a result of a privacy breach. However, in the event of a significant breach, your responsibilities can be considerable, including researching the extent of the breach, determining what steps are needed to comply with applicable laws, notifying all relevant individuals, identifying and providing appropriate credit monitoring for the victims of the identity theft, and responding to regulatory and civil proceedings.

Purchasing the more robust *e-data*RESPONSE+ privacy breach response coverage can provide all these services and more for your practice. For more information, contact your producer, agent or broker, or our Customer Service Department at 410-785-0050 or 800-492-0193 (toll free).

Publication of Medical Mutual/Professionals Advocate®

DOCTORS Rx

Volume 22 No. 2 Winter 2014

Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company
Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193