Risk Management Program "Needs Assessment Survey" Available Online

Let us know how we're doing! On both MEDICAL MUTUAL and Professionals Advocate web sites, our Risk Management Department is offering a needs assessment survey. This brief, five question survey asks you what topics you would like us to cover in future seminars, as well as areas for comments and feedback on current seminars. Your valued insight will help us design stronger, more beneficial educational programs for our Insureds. Visit www.weinsuredocs.com for more information and links to the survey.

Publication of MEDICAL MUTUAL / Professionals Advocate®

DOCTORS Rx

Volume 16, No. 2 Winter 2008

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

Publication of MEDICAL MUTUAL / Professionals Advocate®

DOCTORS Rx

Volume 16, No. 2 Winter 2008

A Letter from the Chair of the Board

Dear Colleague:

For many Physicians, the incorporation of an electronic medical record system is an enormous undertaking. This newsletter will look at ways to protect vital patient information by establishing key security practices in your office.

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

Doing No e-Harm

The world of computers, e-mail, and electronic connectivity continues to revolutionize the efficiency of patient care. It also continues to incubate new forms of potential harm to patients: misuse and corruption of the most deeply personal information. Certainly, medicine has changed significantly since Hippocrates penned his famous pledge. Our duty to the patient has not changed.

Responsible information security practices in medicine require more than the average care commonplace in other types of business or consumer computing. Doing no harm to patient privacy and data security begins with understanding:

- What information Physicians must protect.
- How to reasonably protect this information using current strategies and technologies.
- Why maintaining information security manages risk.

In any discussion of information security issues and strategies in the practice of sound e-medicine, an important caveat is required: a Physician must ultimately judge the appropriateness of a course of action in light of all

Continued on next page

Michael D. Heckman, Esq.

circumstances presented. Similarly, each practice faces different human and technical challenges in developing an information security plan. No single software or hardware package can meet every need. This article focuses on practical security strategies and technologies in general terms rather than referring to specific products or services.

The 21st Century Medical Office

Computers have become indispensable tools in medical practices of all sizes. As hospitals adopt electronic medical records (EMR) systems, the trend toward e-medicine is likely to accelerate at the group and solo practice levels as well. The benefits of EMR systems and practice management systems are numerous. They include efficiency, long-term cost savings, and integration with the EMR systems that hospitals and other facilities continue to adopt at increasing rates. Another less publicized benefit of EMR/EHR (Electronic Health Records) systems is that they generally include extensive information security measures within their infrastructures.

Conversely, general medical office computing tasks such as billing, e-mail, and web surfing often remain areas of vulnerability. This article focuses on threats to privacy and security in general office settings rather than specific EMR or practice management applications.

Example: A group practice uses eight computers to run their office. The Physicians each have computers on their desks. So do the receptionist and the office manager/billing specialist. There is also one computer shared by the two nurses.

Everybody in the office has Internet access. They use the web for everything from researching drug interactions to ordering office supplies. In the waiting room, patients can surf the web using a wireless network protected by password access.

A popular accounting program is used for billing, bookkeeping, and payroll. Appointments are tracked and managed with a calendar/e-mail program that is nearly ubiquitous. Additionally, the Doctors enjoy using their Blackberrys and iPhones to keep up with scheduling changes when they are away from the office. They also e-mail each other and the staff regularly.

This common setup remains problematic for the practice on several levels. Without further access controls and network security measures, it leaves key data vulnerable. First and foremost, Protected Health Information (PHI) is at risk. So are other forms of protected information.

Even though the staff in this example has received HIPAA training, their Physicians/employers still risk:

- Violating various privacy laws and exposing the practice to potential patient lawsuits.
- Making electronic discovery unnecessarily expensive should they ever face a lawsuit in the future.

What Information Must You Protect?

Protected Health Information (PHI) is any information that:

1) Is individually identifiable,

2) Is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house, and

3) Relates to the past, present, or future physical or mental health or condition of an individual, or past, present, or future payment for the provision of health care to that individual.[1]

The duty to protect PHI is set forth in the medical privacy statutes of Maryland and Virginia as well as HIPAA. Maryland and Virginia also have new general privacy statutes requiring all businesses to protect "personal information" in addition to health information. An overview of these laws follows later in this article.

The bottom line, however, is that protecting nearly any and all data and e-communications has become a prudent strategy for maintaining a defensible medical office information infrastructure. This strategy contains good news and bad news. The bad news is that the legal, technical, and financial risk of breaches continues to increase. The good news is that vigilance need not be costly, cumbersome, or complicated.

PHI, Personal Information, and Nearly Everything Else Deserves Protection

Breaches and corruption of patient information result from well-intentioned acts of omission or malevolent acts of commission. Neither is unforeseeable.

Example: A patient is anxious to receive her lab results because she is afraid that she has an embarrassing STD. She instructs the Physician's nurse to call her immediately when the result is available. She also asks the nurse to "please e-mail me so that I can be notified on my Blackberry."

The nurse calls the patient and reaches only voicemail. Eager to help, the nurse then looks up the patient's work e-mail address. Instead of e-mailing instructions to call the Physician's office, the nurse decides not to prolong the patient's anxiety: She e-mails the negative results to the patient. This news reaches the patient immediately and allays her fears. Unbeknownst to her, however, the news also amuses the young men who work in her company's IT department.

The department routinely monitors employee e-mail (a practice that is both legal and well-documented in the company's employee handbook).

In addition to breaches that compromise individual privacy and dignity like the above example, the specter of data theft or corruption on a practice-wide scale requires attention. Extensive breaches and resulting lawsuits are more than remote possibilities. Verizon Business recently summarized 500 data breach investigations, reporting that:

- 87% of breaches could have been avoided with basic security measures.
- Two-thirds of the cases involved data that the organization did not know was present on the system.
- 18% of the breaches were caused by insiders/employees.
- 39% of the breaches involved business partners.
- Breaches involving partners increased five-fold from 2004 to 2007. [2]

Information Security Basics

Solid defensible information security practice has two objectives: 1) Protection of patient confidentiality and PHI from breaches, and 2) Protection of data against corruption–both intentional and unintentional. The

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 *"Doing No e-Harm"*

Educational Objectives: Participants should be able to:
1) Identify and differentiate the concepts of Protected Health Information and Personal Information.
2) Identify the areas of liability exposure commensurate with the duty to protect both types of information.
3) Describe the information security strategies to reduce the risks of compromising and corrupting patient information.

	Strongly Agree				Strongly Disagree
Part I. 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: _____

_____

_____

_____

CME Test Questions

Instructions for CME Participation

CME Accreditation Statement — MEDICAL MUTUAL Liability Insurance Society of Maryland, which is affiliated with the Professionals Advocate® Insurance Company, is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians. MEDICAL MUTUAL designates this educational activity for a maximum of 1.0 AMA PRA *Category 1 Credits*™. Physicians should only claim 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. Fax: 410-785-2631
   225 International Circle
   P.O. Box 8016
   Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.

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 27, 2009
5. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

1. If an accounting program generates a patient bill that includes the patient's name, itemized description of services rendered, diagnostic codes, and outstanding balance, the bill contains Protected Health Information (PHI).

   A. True B. False

2. There is no civil liability for data breaches resulting from a Physician's failure to exercise reasonable care in protecting PHI. HIPAA and state laws only provide for enforcement by government agencies.

   A. True B. False

3. A medical practice (in Maryland or Virginia) has a legal obligation to protect the personal information of employees AND patients.

   A. True B. False

4. Health care organizations of all sizes are exempt from state personal information protection laws entirely because HIPAA supersedes PIPA statutes.

   A. True B. False

5. Protecting patient confidentiality and protecting patient data from breaches or corruption are objectives of a defensible information security plan.

   A. True B. False

6. Medical practices generally do not have any responsibility to protect PCI data. This is the responsibility of credit card companies.

   A. True B. False

7. Risk assessment, e-mail management, access control, and intrusion defense are elements of responsible information security practice.

   A. True B. False

8. Sending lab results or other PHI to a patient via e-mail does not risk violating federal or state privacy laws as long as the patient has consented to being contacted via e-mail.

   A. True B. False

9. EMR and practice management programs are generally the only systems that can use access controls to secure protected information.

   A. True B. False

10. An electronic scan of a patient's insurance card and driver's license does not contain PHI; therefore, a medical practice has no legal duty to secure this file.

    A. True B. False

following components are essential to achieving these goals, and well worth adopting in any medical office practice.

Conduct a Risk Assessment

This process does not need to be complex or time-consuming. Risk Assessments can be maintained on documents or spreadsheets and templates for both are widely available online at little or no cost. The process entails:

1) Identifying your assets, such as computers, billing software etc.

2) Listing the risk tolerance of each asset. In this context risk tolerance is the impact on your practice if a major event happens to the asset. Example: If a practice's billing records were deleted or corrupted without backup, the impact would be major. Conversely, if a computer were accidentally knocked over and destroyed but could be replaced and loaded with backup files, the impact would be minimal.

3) Listing and evaluating current protection mechanisms.

4) Assessing unprotected assets and unaddressed threats.[3]

Adopt E-Mail Management, Internet Usage Policies, and Secure E-Mail Technology

At a minimum, sound information security practices require a clear understanding of what may and may not be sent via e-mail. Having unequivocal policies, such as prohibiting sending any form of PHI to a patient at her work e-mail address, is a start. Communicating these policies to office staff is critical. The same is true for web surfing and access/use of personal e-mail at work. Putting these policies in writing helps ensure that they are communicated clearly and that a record of that communication exists in the event of future litigation.

The other essential component to a defensible practice e-mail system is technical management. Are these features part of your practice's e-mail system?

- Automatic archiving of all e-mails sent and received. In the event of a lawsuit or audit, this feature will reduce the cost of discovery significantly.
- Spam, virus, and malware protection.
- Ability to send encrypted e-mail. Using encryption to secure PHI and other personal information generally provides a "safe harbor," or a presumption of reasonable care in the event of an unauthorized breach.
- Ability to "wipe" (erase) e-mail from mobile devices remotely if the devices are lost or stolen.

These components and other more advanced management features are widely available from specialized e-mail hosting providers. They can also be added through various hardware and software

enhancements if you are one of the few practices that operate an e-mail server internally. Many third party service providers specializing in e-mail-only hosting and archiving offer "compliance" packages.

On the other end of the spectrum, free e-mail accounts with webmail (such as Hotmail, AOL, Yahoo) and client programs (such as Outlook Express, AOL Mail) are better suited to home and personal use. Many lack the security, backup, and searchable archiving features that provide responsible protection in a professional practice setting.

Software and methods for hacking into these free accounts are widely available and publicized. Since the accounts are easily accessible online with a username and a common web site, entering them is often simply a matter of guessing (or extrapolating) a password. The cost of a secure hosted account (that preferably offers an encryption option) may seem high when compared to "free," but so is the risk of compromising PHI and commensurate liability when using the former.

Secure Your Networks, Wired and Wireless

Cable or DSL modems, wireless routers, and Ethernet connections have become ubiquitous in medical offices as well as households. For many, installing a wireless network entails using router configuration software or entrusting the job to the cable company, phone company, or local electronics superstore offering on-site service.

When performing a home installation, the easiest two choices are creating an "open" network, where no password is required for access, or simple WEP encryption. Router installation software often presents WEP encryption as the default choice, requiring whomever sets up the network to choose a 13 digit password. Users must then enter the password before initially accessing the network.

While protecting a wireless network using WEP encryption is better than no protection at all, WEP (Wired Equivalent Privacy Algorithm) has proven extremely vulnerable to deliberate intrusion. For businesses that need to secure data, choosing the WPA (Wi-Fi Protected Access) option is significantly more secure. The option is available on nearly all router software. It is no harder to set up than WEP encryption, but may require some digging through the setup menus to find.

Additionally, the following effective defense elements used to be deployed primarily in large organizations, but are now readily accessible to small medical practices:

Intrusion Defense

- Web surfing anti-virus protection
- Intrusion prevention and detection

Vulnerability Defense

- Anti-phishing and anti-pharming filtering
- Web site monitoring

System Defense

- Anti-virus and anti-spyware software
- Host intrusion prevention
- Remote backup and data recovery

Installing, configuring, and maintaining this technology may prove unduly costly as a do-it-yourself proposition. Many internet-oriented security companies, however, make this technology available as a service comparable to the offerings of your Internet service provider.

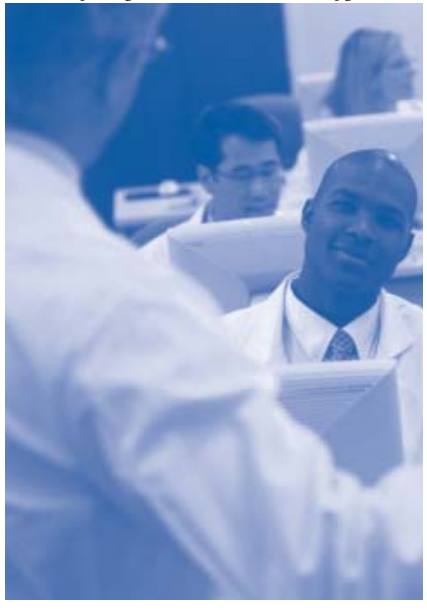
Establish Basic Access Controls

Most popular practice management and EMR programs include strong access controls. They usually

require authentication for any task that modifies or accesses patient data. Even if you do not use these types of programs, consider putting the same types of access controls on all of the patient-related software in your office. Accounting systems, patient databases, and even Excel spreadsheets can be configured so that only the "owner" of a data file may write to or read the file. Avoid using shared passwords or guest accounts.

Protect Your Storage Devices

Storage devices that include CDs, portable hard drives, flash drives, and USB memory sticks all have become popular means of backing up data. They are inexpensive and easy to configure. However, few users encrypt them or consider the ease with which they can be lost or stolen. Consequently, their use for the storage of patient data poses serious risks. If you use such devices to store patient data or other personal information, consider one of the many personal encryption programs now available. Many are inexpensive or free. Once you decide to replace a storage drive or take it out of service, destroying it completely minimizes the risk of data theft. The same is true for replacing hard drives or servers for upgrades.



The Legal Landscape

Maryland and Virginia's health privacy statutes and HIPAA contain similarly broad definitions of PHI.[4] The state statutes also segregate mental health records in general and apply more stringent disclosure restrictions on them than the general provisions of HIPAA.

Unlike HIPAA, Maryland and Virginia laws give patients a private right to sue if a breach of their PHI results in damages. While HIPAA does not give patients or any private parties this same right of action, private parties can use HIPAA violations in state law causes of action. Recent court cases in many states have involved plaintiffs citing HIPAA violations as evidence of lack of reasonable care in malpractice, invasion of privacy, and intentional infliction of emotional distress claims.

Most Physicians are familiar with their obligation to safeguard PHI, but may not be aware of additional duties to protect "Personal Information" imposed by Maryland and Virginia laws. Maryland's PIPA statute became effective in 2008 and Virginia recently amended its 2005 statute with provisions that became effective in July of 2008.

Maryland and Virginia each have a Personal Information Protection Act (PIPA) that affects medical office practice. Both state PIPA laws require businesses to protect Personal Information not covered by HIPAA. Maryland and Virginia similarly define Personal Information as an individual's first name or initial and last name combined with one or more of the following data elements: Social Security number, driver's license number, or individual taxpayer identification number. It also includes a financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account.[5]

Maryland and Virginia give your patients, employees, and former employees the right to sue for damages and attorneys' fees in the event of a breach of Personal Information that results in damages. If there is a reasonable belief that the breach will cause identity theft or other fraud, Virginia's recent amendment also creates a notice requirement: the practice must contact the Office of the Attorney General.

PCI Compliance

In addition to state and federal law, the Payment Card Industry (PCI) Data Security Standard details security requirements for businesses that store, process or transmit cardholder data. Merchant banks generally require practices that accept credit cards to use PCI-compliant terminals (which they provide) and those who do so online must use PCI-compliant gateways (which they specify).

Network Security Scans are required of all merchants with external-facing IP addresses that collect, process or transmit payment account information. Even if a practice does not do web-based transactions beyond authorizations (most don't), there may be other services that make systems vulnerable. E-mail and employee Internet access may result in the Internet-accessibility of a company's network. These paths to and from the Internet may seem inconsequential, but they can provide unprotected pathways into merchant systems and can potentially expose cardholder data if not properly secured.

Summary

The responsibility to do no harm to patients extends beyond physical protection. It includes a duty to protect the privacy and security of patients' information. The legal extent of this responsibility continues to evolve, as do the technical means of meeting it. This article summarizes some of the basic security and privacy tools, and is intended to serve as a catalyst for further exploration. Protecting health privacy begins with establishing sound information security practices in your office. While security does not necessarily ensure privacy, the latter is not possible without the former.

About the Author

Michael D. Heckman, Esq.

Michael Heckman is both an attorney and computer/internet specialist who runs an information technology security consulting practice in Rockville, Maryland. For more than ten years, he has advised health care nonprofits, pharmaceutical companies, trade associations, and law practices on information infrastructure and management.

References

1. 45 C.F.R. 164.501
2. 2008 Verizon Business Data Breach Investigations Report
3. ISO-17799, "Information Technology-Code of Practice for Information Security." ISO-17799 is a generally accepted information security program standard applied in a wide variety of industries.
4. Virginia Code Annotated § 32.1-127- § 38.2 and the Maryland Confidentiality of Medical Records Act are the general sources of respective state law governing health information/records.
5. Maryland Code Annotated § 14-3501, Virginia Code Annotated § 18.2-186.6

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
Assistant 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	ext. 163
Risk Management Seminar Info	ext. 215 or 225
Risk Management Questions	ext. 224
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	www.weinsuredocs.com