

ELECTRONIC HEALTH RECORDS: PROTECTING YOUR ASSETS WITH A SOLID SECURITY PLAN

To maximize the financial and productivity benefits of an EHR solution, you need to implement a security plan that's right for the structure and needs of your health organization.

By Carolyn P. Hartley, MLA

Securing the data for your healthcare organization or practice makes good business sense, especially if you use or are transitioning to an Electronic Health Record (EHR) solution. Aside from the investment in your clinical and administrative workforce, patient records are an asset worth protecting.

When using an EHR system, all patient records are stored in one location and readily accessible, which can enable faster access to a patient's health history, problem list, medications, lab results, diagnostic imaging and work-ups. Medical literature and medication databases that alert or support the practitioner's care plan also can be rapidly accessed.

While an EHR creates a shift in the management and access of patient records, it also requires organizations to give additional thought to having a proper data security plan and allows you to continue safeguarding protected health information (PHI).

To take advantage of the benefits you can achieve with EHR and to further protect your organization's valuable data, follow these best practices to help build a security plan and:

- Increase your EHR return on investment (ROI) with proactive secure business preparation strategies.
- Enable mobility through secure access to confidential records from inside or outside the facility.
- Protect hardware, EHR and third-party software from security breaches with firewalls and anti-virus software.
- Ensure availability of EHR information at any time.
- Provide secure electronic communications with patients, pharmacies and suppliers.

MAXIMIZE YOUR ROI

The financial incentives provided under the American Recovery and Reinvestment Act of 2009 (ARRA) for EHR have motivated many physician practices and healthcare organizations to implement one.¹

¹ Ronald Sterling, Qwest white paper, "Electronic Health Records: Helping Healthcare Practitioners Understand the Benefits of Implementing a System," 2009.

Although the cost can be significant, the investment typically pays back in dramatic ways. For example, a practice administrator in a three-physician Texas allergy clinic conducted a time and motion study in which he identified \$40,000 to \$50,000 in potential savings from administrative inefficiencies.²

By automating workflows, such as scheduling patient visits and sending patient reminders as well as using electronic faxing and computerized physician order entry (CPOE), physicians have used the recovered savings to experience many benefits that allow them to:

- Eliminate potential errors by accessing a single longitudinal record.
- Respond to emergencies or weekends on-call without going to the facility to search for a patient chart.
- Access PHI from anywhere Internet service is available.
- Securely consult other practitioners involved in the patient's care.
- Receive electronic alerts if a patient is admitted to a hospital.
- Provide educational material relevant to the patient's diagnosis without having to make copies of copies.
- Be paid for virtual office visits.³

Achieving these benefits is within reach of any practitioner no matter the size of the operation. However, it also requires business planning and preparedness to protect your network and your PHI.

PROTECT PATIENT CONFIDENTIALITY

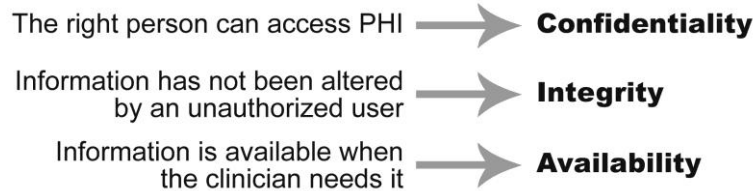
If you are considering making new hardware purchases, such as mobile devices for clinicians, and you are juggling priorities, it's a good idea to put the hardware purchase on hold until your EHR selection is finalized, and your internal security measures are in place.

You may also want to review how you safeguard PHI. Ensuring the electronic creation, use, storage and transmission of PHI has been the subject of nearly a decade of planning, legislation, stakeholder conferences and public comment. Confidentiality, integrity and availability of data are the three tenets of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.⁴

² Carolyn P. Hartley, "Identify Low-Value Work, then Automate It," *For the Record* magazine, June 12, 2006, Vol. 18 No. 12 P. 8, available online at http://www.fortherecordmag.com/archives/ptr_06122006p8.shtml.

³ Sheri Porter, "New, Revised CPT Codes Target Online, Telephone Services," *AAFP News Now*, February 29, 2008. Available online at <http://www.aafp.org/online/en/home/publications/news/news-now/practice-management/20080229cptcodes.html>. Use revised CPT codes 99441 (5-10 minutes), 99442 (11-20 minutes) and 99443 (21 to 30 minutes) when reporting medical care via telephone that is initiated by an established patient or by the patient's guardian. The reporting physician, or a physician of the same specialty in the same practice, must have seen the patient within the past three years.

⁴ The Office for Civil Rights within the U.S. Department of Health and Human Services maintains updates on privacy and security of electronic health information. View the HIPAA Security Rule and guidance about that rule at <http://www.hhs.gov/ocr>.



To safeguard PHI, the HIPAA Security Rule requires that you conduct a risk analysis⁵ to help evaluate where security vulnerabilities exist inside and outside your organization. A risk analysis is considered an industry best practice and is a required annual activity to participate in the Health Information Technology for Economic and Clinical Health (HITECH) Meaningful Use incentive funds.⁶ One forecasting tool is HITECH's Meaningful Use reporting grid, which identifies quality measures to be captured from 2011 to 2013⁷ and yet-to-be-defined measures for Stage 2 (2013-2014) and Stage 3 (2015).

For example, to meet Stage 1 Meaningful Use measures, your EHR system must enable you to provide patients with secure electronic copies of their health information, including lab results, problem list, medication list, allergies, discharge summary and/or procedures. In your business planning, you need to determine if this can be achieved via one or any combination of the following:

- The EHR vendor's secure patient online portal access options
- The patient's secure online personal health record application
- The local or regional health information exchange

The risk analysis guides you through questions that evaluate firewalls and virus protection you need from web-based threats. It also explains the security measures to support secure e-communication with other providers or your patients.

As a Covered Entity under HIPAA's Security Rule, your responsibilities include ensuring a secure electronic environment. A Covered Entity is a healthcare provider that conducts certain transactions electronically, (including doctors, clinics and pharmacies), health plan (health insurance companies, HMOs and government healthcare programs) or healthcare clearing house (companies that process health information).

⁵ Several organizations provide low-cost risk analyses for solo practitioners to multi-departmental risk analyses for hospital systems.

⁶ Ronald Sterling, Qwest white paper, "Electronic Health Records: Helping Healthcare Practitioners Understand the Benefits of Implementing a System," 2009.

⁷ The Centers for Medicare and Medicaid (CMS) EHR incentive programs will provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals that are meaningful users of certified EHR technology. The most current Meaningful Use grid can be found online at <http://healthit.hhs.gov>.

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards approach security at an organizational level so you can evaluate risks and enact policies and procedures to manage those risks. This includes policies to manage the development, implementation and maintenance of security measures to protect PHI.

You should reach out to your communications vendor or IT consultant to discuss how you will receive up-to-date information on significant potential threats and vulnerabilities that could impact your system.

You should consider having an internal security leader, or security official, to establish your security policies and procedures. This person is responsible for training the staff on procedures to manage those risks, as well as implementing sanctions for those who accidentally or intentionally put PHI at risk and breach confidentiality, negatively affect productivity and patient trust. These sanctions may include additional training or more stringent actions, including employment discipline.

TECHNICAL SAFEGUARDS

Technical safeguards establish measures to leverage network and EHR system capabilities in the most secure ways. Safeguards to evaluate include:

- Role-based access
- Access audit trails
- Remote access
- Application audit
- Vulnerability testing and reviews

Audit trails can help you learn if a current or terminated employee accessed information he or she was not authorized to see. When customizing your EHR system, you will be asked to provide user names with their role-based access — this regulates access to your computers and your network resources based on each user's job and responsibilities.

Aside from your organization's users, health IT vendors might need access to your local network to provide technical support when necessary. Your organization should also consider a virtual private network (VPN) for offsite users to be able to access your system. For example, a VPN allows practitioners using mobile handheld devices to connect to your EHR.

You can also reach out to your communications vendor and ask them to help you understand vulnerabilities you may face and test your system to help you assess your current network integrity. The results can help determine immediate short-term and strategic long-term steps for stabilizing your network.

Attack and penetration tests, for example, include having your vendor identify system vulnerabilities by attempting to gain access to your network system or your information from either the WAN or LAN.

Other tests may include assessing your web applications for various vulnerabilities and misconfigurations. Review unused or unnecessary programs installed on your network. Ask your IT vendor or IT consultant to identify unused applications that can be discarded or updated to mitigate potential transmission threats or exposure to open networks.

In addition, you can ask your vendor to perform risk assessment based on the National Security Agency's InfoSec Assessment Methodology, more commonly known as NSA IAM, which can help you craft an action plan to move from your current network's state to your desired network goals.

PHYSICAL SAFEGUARDS

Physical safeguards include an analysis of how to protect your facility, workstations and electronic information systems from natural and environmental hazards and unauthorized intrusions. Just as you lock doors to protect your physical assets, physical safeguards require you to protect your electronic systems and establish plans to handle contingencies in the event of an emergency or disaster.

Here are a few physical risks you may want to identify and manage:

- Determine whether you need a wired, wireless and/or server-based network, and review the risks and benefits of each. Nearly all organizations today select some type of secure wireless connectivity to their network.
- Assess how you will protect your hardware and software inventory and who has access to tablets, handheld devices or desktop computers.
- Control access to portable and desktop computers, network servers and information systems. You may decide to employ a security guard, use a keypad or card reader entry system, install deadbolt locks or install biometric systems, such as finger image recognition systems.
- Develop a contingency plan so your operations continue to operate after a disaster. In the event of a fire, for example, you will need secure access to insurance documents, hardware and software inventory. Also, you will want a process to re-establish secure access to health records and business data. This could include gaining secure remote access to your schedule and records of incoming patients. You'll also want to notify patients where to find you until the facility is repaired.

In addition, it's important to know how to report lost or stolen laptops or handheld devices. The Breach Notification Rule details financial penalties and public announcements you must make for a lost or stolen electronic device, but a safe harbor exists if you encrypt electronic PHI in your database (data at rest) or in your transactions (data in motion).⁸

Finally, you can establish policies on how often you should back up your system, how you will recover from a disaster and what applications are most critical to getting your system up and running again. An IT consultant can guide you through those discussions.

⁸ 45 CFR 164.308(a)(6)(i), NIST SP 800-66, p. 27-28, 68 Federal Register 8377.

ONLINE BACKUP MEASURES

As you continue securing your PHI and EHR solutions, it's also a good time to build your emergency access procedures and develop a contingency plan for downtime. Because systems and networks go down from time to time, it's a best practice to secure redundant access as a prevention strategy.

Investing in 24/7 web support that also monitors downtime is one of the best investments you can make, especially if your organization has developed the good habit of reviewing patient records the evening before a patient encounter. Organizations with server-based systems should consider server mirroring or cloning software that backs up the system in real time.

CONCLUSION

The move to EHR is a dramatic change to how you and your health organization practices medicine. Look for competent solutions advisors in the following areas:

- [Networking](#) – keeping your organization connected
- [Security/business continuity](#) – safeguarding your data against loss
- [Contact center](#) – enabling you to provide exceptional service

An advisor can help ensure that the move is done securely so you can focus on the clinical and administrative workflow changes.

ABOUT QWEST BUSINESS

Qwest Business is a choice of 95 percent of Fortune 500 companies, offering a comprehensive portfolio of data and voice networking communications solutions to enterprises, government agencies and educational institutions of all sizes. The Qwest network backbone covers the entire continental United States and has one of the largest fiber footprints in the U.S., capable of supporting 40 Gbps data transmission rates now and 100 Gbps soon.

Go to Qwest.com/business to see why enterprises coast-to-coast rely on Qwest for first-class communications solutions and to learn more about Qwest's commitment to perfecting the customer experience.

ABOUT THE AUTHOR

Carolyn P. Hartley is president and CEO of Physicians EHR LLC. She has been in healthcare since 1982 and in health information technology for more than a decade. She is lead or co-author of 13 textbooks on privacy, security and EHR implementation and also serves as EMR technical advisor to oncology, gastroenterology, community health centers and dental societies and providers. Her books include *EHR Implementation: A Step by Step Guide for the Physician's Office* (AMA Press) and *Handbook for HIPAA Security Implementation* (AMA Press).

TIPS ON CHOOSING A VOICE AND DATA PROVIDER

Voice over Internet Protocol (VoIP) uses the Internet to connect phone calls, which can bypass some of the charges associated with traditional telephone lines. VoIP also has the potential to untether your workforce from their desk, by allowing them to respond to and make patient calls using the VoIP wireless network. During a disaster recovery situation, this capability is a significant benefit that enables a physician to stay in touch with patients without being at the facility.

Evaluating the option of VoIP requires the use of strategies similar to selecting your EHR. Here are some issues to consider and questions to ask:

SERVICE PROVIDER'S REPUTATION

- How long has the company been in business?
- Ask for references from other practitioners who are in your area and use the system and who are similar to your size.

COSTS

- Are VoIP service fees the same for national and international calls?
- What are the terms for contract termination?
- Does the VoIP provider charge an installment fee?
- Ask to see a sample invoice to evaluate user fees and taxes.

TECHNICAL SUPPORT

- Who will install the system?
- What kind of technical support and training will you receive after the system is live?
- How quickly does your technical support react to incidents?

EQUIPMENT AND BANDWIDTH

- Who provides the customer with equipment, such as modems and phones?
- Who verifies that the service and equipment will connect with your network?
- What bandwidth will you need, especially as you transition to an EHR?

BUSINESS PREPAREDNESS

- Is the VoIP system dependent on electricity to power the network translator? If so, how will you communicate if a power failure occurs?
- Will the VoIP phones communicate clearly with existing phone sets?
- How often is service upgraded and what business interruption guarantees will you receive during upgrades?

If you receive satisfactory responses, document the decisions you made with the VoIP service provider and then coordinate the installation. It's best to go live on the new service before or after implementing the EHR, but not concurrently.

CHECKLIST: DATA SECURITY PLAN FOR YOUR EHR

Building or refining your healthcare organization's security plan can deliver the results you expect, especially if you follow these steps.

CONDUCT A RISK ANALYSIS

- Review current Protected Health Information (PHI) safeguards:
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf>
- Use HITECH's Meaningful Use Reporting Grid:
- Evaluate firewalls and virus protection
- Review security measures for secure e-communications
<http://healthit.hhs.gov>
- Review your responsibilities as a Covered Entity under HIPAA's Security Rule:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/>

ESTABLISH ADMINISTRATIVE SAFEGUARDS

- Assign an internal security leader
- Establish data security policies and procedures for staff
- Develop plan to ensure updates of potential web threats

BUILD TECHNICAL SAFEGUARDS

- Determine role-based access and implement audit trails
- Audit applications
- Test and review network vulnerability

CREATE PHYSICAL SAFEGUARDS

- Develop policies and procedures to inventory and control access to desktops, servers and information systems.
- Develop process for handling lost or stolen laptops and handheld devices
- Determine system backup and data recovery procedures:
 - Natural: Flood, earthquake, tornado, etc.
 - Environmental: Chemical spills, HVAC problems, power outages, etc.
 - Unauthorized intrusions: Hackers, burglary, etc.
- Establish contingency plans

DETERMINE ONLINE BACKUP MEASURES

- Create and document emergency access procedures
- Consider 24/7 web support
- Consider using server mirroring or cloning software

RESOURCES

Visit the following sites for more information:

QWEST SOLUTIONS

- [Healthcare Solutions](#)
- [Ethernet Solutions for Healthcare – Fast, Secure, Reliable](#)
- [Interactive Healthcare guide](#)

QWEST WHITE PAPERS

- [Qwest White Paper Resource Center](#)
- [Electronic Health Records: Helping Healthcare Practitioners Understand the Benefits of Implementing a System](#)
- [Healthcare IT Security Necessity](#)
- [Ethernet for Healthcare Providers](#)

AMERICAN RECOVERY AND REINVESTMENT ACT OF 2009 (ARRA)

- <http://www.recovery.gov>: Information on the federal government's economic recovery program
- <http://bit.ly/xhg5m>: IRS ARRA Information Center

MEANINGFUL USE DEFINITIONS

- <http://bit.ly/1f6RiQ>: Recommendation from the Meaningful Use Workgroup
- <http://www.meaningfuluse.org>: Discussion forum from the Association of Medical Directors of Information Systems

HIPAA SECURITY REGULATIONS

- <http://bit.ly/bqzT5k>: HHS security standards
- <http://bit.ly/ZILrF>: Detailed overview of the HIPAA security rule

SECURITY ISSUES

- <http://www.NIST.gov>: National Institute for Standards and Technology, which defines minimum encryption standards adopted into the Breach Notification Rule
- <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>: Breach Notification for Unsecured Protected Health Information; Interim Final Rule