CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Consider Security and Privacy in the Move to Electronic Health Records

Key Message: Electronic health records bring many benefits along with security and privacy challenges.

Executive Summary

Converting to the use of electronic health records can bring many advantages in the quality of health care. But it also brings particular security and privacy risks. In this podcast, Deborah Lafky, with the U.S. Department of Health and Human Services (HHS), Office of the National Coordinator for Health Information Technology (ONC), and Matt Butkovic, team lead for work CERT is doing with ONC, describe some of the opportunities and challenges that healthcare providers face as they move to electronic health records.

PART 1: BENEFITS OF ELECTRONIC HEALTH RECORDS

The HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act was passed by Congress as part of the stimulus bill at the beginning of the Obama Administration.

The HITECH Act

- includes objectives for adopting electronic health records (EHRs)
- enables physicians and patients to share information and use medical records to improve care
- is an extension of efforts that began when the federal government started studying the feasibility of electronic health records in the early 1970s
- brings the benefits of automation to the healthcare arena

Key Benefits for Providers and Patients

These include the following

- Ensure that providers (physicians, nurses, and all others involved in care) and patients have complete and accurate information about patients, including access to full medical histories.
- Avoid medical errors, such as duplicate prescriptions, duplicate tests, mistaken prescriptions, mistaken diagnoses, and getting patients confused with one another. These kinds of errors were identified by the Institute of Medicine as being a source of concern with the existing healthcare system.
- Give providers better access to care information. Doctors can share health records with one another electronically when they share the care of a patient.

  For example, providers can share test results, thus avoiding duplicative tests done for a patient. They can move lab results directly from the lab to any provider who needs to have access to them electronically.

- People can more easily manage and understand their own care and that of other family members they are responsible for. All of their medical records will be available through their own computers.

Advantages over Paper Records

For example, if a woman who is found unconscious is taken to an emergency room and her primary care physician's office is closed or unknown, no one will be able to access her paper records, which would have revealed that she is a

diabetic.

With access to EHRs, emergency room doctors could

- fully understand her condition
- avoid mistakes
- quickly diagnose that she is in a diabetic crisis
- not waste precious time on other diagnoses

PART 2: EHR SECURITY AND PRIVACY; REGIONAL EXTENSION CENTERS AND BEACON COMMUNITIES

Security and Privacy Regulations

HHS regulates the privacy and security of medical records. The U.S. Health Insurance Portability and Accountability Act (HIPAA) governs privacy and security for health records (paper and electronic).

HIPAA regulations have specific instructions for physicians, clinics, hospitals, and others who handle medical records about

- keeping medical records secure
- who can and can't see them
- for what purposes they can be used

ONC identifies and develops tools that will help providers keep EHRs secure. This includes ONC's work with CERT, to help providers reliably meet their EHR privacy and security requirements by identifying the presence or absence of key EHR management pratices.

Key Security Requirements

EHRs are critical assets in the form of patient information, at the personal level for patients, for healthcare organizations, and at the national level. The goal is to ensure justified confidence in the confidentiality, integrity, and availability of medical records.

For organizations that are moving from paper records to electronic records:

- actions to ensure the safety and soundness of paper records also apply to electronic records, with a few additions.
- they need to identify and understand the linkage between these critical assets and the healthcare services in which they are used.
- the risk management profile of the organization must address the transition to electronic records.
- their control environment and safeguards must be adequate to ensure that the new challenges introduced by EHRs are accounted for.

Identifying and Handling Security Incidents

Healthcare organizations must have a mechanism to identify and respond to security incidents involving EHRs.

Unlawful removal of paper records is limited by their bulk and visibility. Megabytes of electronic information, on the other hand, can be easily and secretly removed.

One of the key practices in securing EHRs is being able to identify if data has been alterated or exfiltrated (unauthorized removal of records), via

- a network intrusion
- an employee taking an unencrypted USB drive home. That is unfortunately a recurring example of a lapse in the control environment that results in the breach of medical records.

Guidance for identifying and handling incidents is available on CERT's incident management website and in the CERT Resilience Management Model.

Office of the National Coordinator for Health Information Technology

- Established in 2005.
- Reports directly to the Secretary of Health and Human Services.
- Uses various channels to encourage providers to adopt EHRs, to get every doctor's office to have a modern patient information system.
- With the HITECH Act, funded to push EHR adoption forward.
- Is not developing a national system of medical records.
- Current programs include Regional Extension Centers and beacon communities.

Regional Extension Centers

- Much like the U.S. Agricultural Regional Extension Centers, which are farm bureaus that provide information and assistance to farmers.
- There are 62 healthcare provider Regional Extension Centers throughout the country, where providers can get help implementing EHRs.

Most of the primary care in the U.S. is delivered by medical practices of one to five doctors. They don't have IT staffs; they don't know how to set up a computer network. ONC has used HITECH Act funding to help them.

Beacon Communities

- highly focused practice clusters of hospitals, practitioners, and clinics working together on a specific problem, such as using EHRs to help reduce the incidence of rehospitalization after discharge, or reduce the incidence of admissions for diabetes
- determine what the best practices are, and then ONC documents and disseminates those best practices to the regional centers and to the smaller providers that aren't connected to the beacon communities
- work with ONC toward its ultimate goal of improving the quality of care and reducing the cost of care throughout the U.S.

ONC Practices and Training

ONC collects input and sponsors projects to foster best practices in other areas where the beacon communities are not active. ONC creates, documents, and disseminates security and privacy best practices and gets people trained on how to use them.

One project that CERT is doing for ONC is to implement an online training program in incident response for healthcare providers.

PART 3: PATIENTS SHOULD BE AMBULATORY, NOT THEIR RECORDS

Getting Started: Manage EHR Risks

Healthcare organizations of all sizes need to understand how EHRs fit in their overall risk management process. Understanding the connection between critical healthcare service assets, risk appetite, and the safeguards around those assets is key.

CERT is working with ONC to equip providers to evaluate their current posture and make improvements based on that analysis.

Getting Started: Protect Patient Records

If a healthcare provider using EHRs allows portable storage, such as USB drives, they should:

- know how those drives are being used
- know if medical records are making their way to those drives
- at a minimum, ensure that all drives use encryption so that the information on them is protected

In essence:

- understand the disposition of your EHRs, including where they reside
- have safeguards in place to prevent the mass exodus of sensitive information

Think about your risk profile in very concrete terms, such as comparing the protection of physical medical records with their electronic equivalent. For example, a hospital had an unencrypted hard drive stolen out of an employee's car with 88,000 medical records on it. If you took all of those medical records in paper form and stacked them up, they would be taller than the tallest building in the world.

Examples such as this make is easier to understand what actions you need to take to mitigate risks to EHRs.

Resources

HealthIT.gov

- Regional Extension Centers list
- technical papers and publications
- training modules (forthcoming)

National Institute for Standards and Technology (NIST) Health Information Technology

- publications on risk management, risk assessment, and risk assessment in the context of health IT

CERT Resilience Management

Computer Security Incident Response Team (CSIRT) Development

CERT Podcast: Electronic Health Records: Challenges for Patient Privacy and Security (September 2009)