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

Electronic Health Records: Challenges for Patient Privacy & Security

Key Message: Electronic health records (EHRs) are possibly the most complicated area of IT today, more difficult than defense.

Executive Summary

While promising breakthrough improvements in patient care and cost, digitized health records that can be easily shared by patients and medical professionals present many difficult challenges: social, political, economic, and technological.

In this podcast, Bob Charette, founder of ITABHI Corporation and an internationally recognized expert in risk management, information systems and technology, and systems engineering, discusses the latest thinking and progress on electronic health records along with key privacy and security issues that need to be resolved before they can deliver on expectations.

PART 1: TECHNICAL, SOCIAL, AND POLITICAL HURDLES

Background

The push for EHRs in the U.S. is driven by federal government policy. Former president George W. Bush called for all Americans to have them by 2014.

EHRs are also called electronic medical records or personal health records. Essentially these are all terms that involve translating medical information used by all of your doctors in paper form to digital form.

The intent is that this information is made available instantly, across the National Health Information Network, to any health care provider. NHIN may use the internet or may be a specialized network.

Ideally, each patient will be able to access their own records to make sure they are accurate. Patients will also be able to define who has access. As designers attempt to define who has access and who doesn't, the technical, social, and privacy issues become quite complicated.

Benefits

The cost savings and productivity benefits of EHRs seem obvious. They include having one set of tests that all doctors can use and making all health conditions and history available to all health care providers anywhere anytime.

Technical Issues

EHRs require interoperability which means that all health information can be communicated in a form that is readable and usable by everyone.

Currently, there are no defined, agreed-to standards for how medical information is expressed. For example, there are 160-170 different ways to describe high blood pressure.

A typical hospital has 270 different IT systems including CAT scans, x-ray systems, and blood pressure systems, all of which capture information. This information needs to be recorded, stored, and transmitted as part of an EHR. There is tremendous disagreement on how much to capture, how much to transmit, when, and to whom.

Using EHRs in support of billing, administration, and insurance introduces additional challenges. Capturing the flow of patient information is difficult and complex, given all of its pieces, parts, and locations.

Social Issues

Health information is stored for a person's lifetime which raises additional concerns.

Doctors need to adapt to working with information on computers, rather than with paper records. Some patients complain that doctors are more interested in the technology than their patients.

Political Issues

The primary political driver is cost reduction; EHRs have been put forth as a means for saving Medicare by reducinge its costs.

The good news is that organizations such as the Cleveland Clinic and the Mayo Clinic have invested heavily for the last decade and are increasing the quality of patient care while reducing cost.

The current U.S. administration has set aside $19.2B to incentivize hospitals and doctors to invest in EHRs. Requirements for the use of this funding include meeting standards and using EHRs in day-to-day patient care (known as "meaningful use").

Additional incentives include non-payment or reduced payment if EHR systems and information are not used.

More Difficult than Defense

When considering the range of technological, social and political issues, EHRs are likely the most complicated area of IT today, more difficult than defense.

The U.S. health care system represents 16-20% of the U.S. economy, which is much greater than defense.

PART 2: PRIVACY: DISCONNECTS BETWEEN LAW AND REALITY

Unauthorized Disclosure

Doctors who treat patients with mental illness are concerned that if patient information leaks or could be leaked, patients will stop treatment.

There have been a number of cases where the health information of famous people has been made public (for example, the mother of the octuplets and Michael Jackson).

Some would argue that EHRs are more secure than paper records. That said, the likelihood of a large number of records being exposed by hacking is much greater. In a recent case, a hacker held millions of patient records from a prescription drug system for ransom.

Third Rail

Privacy and security are being called the "third rail" of EHRs. Neither have been adequately addressed as a fundamental part of the EHR system.

Controlling Access

Access control and identity management are substantial issues given all of the health care staff that may have access. While this is also true for paper records, access to these is physical and much more local.

With EHRs, access is much easier but the consequences of unauthorized access are much greater.

The Mayo Clinic uses cards as tokens with unique identifiers for system access; the system uses these to log every access to every record. But cards can be borrowed and used in an unauthorized manner. Solutions require strong credentialing with patient control supported by automation.

PART 3: SECURITY: PATIENT AS ADVOCATE

What's Different for Protecting EHR Information?

Standard security controls that are used today for protecting sensitive information apply to EHRs.

The primary difference is legal and regulatory: reporting breaches and complying with laws such as HIPAA in the U.S. (Health Insurance Portability and Accountability Act).

This past year, HIPAA has been upgraded to include the HITECH Act (Health Information Technology for Economic and Clinical Health) which calls for more extensive breach notification.

Having laws is well and good but it is not clear how these can be enforced legally and supported technologically.

Another possibility is to call for more robust, comprehensive security assessments of systems that hold EHR information. The reality is that there is close to 112,000 private medical practices in the U.S. This doesn't include optometrists and many other offices that use health information.

It is not practical to expect all of these providers to be sufficiently security aware to conduct or pass a risk assessment.

Patient as Security and Privacy Advocate

It seems like we all need to become our own advocates for protecting our health information as we are becoming for our own health care. We need to understand how our records are being used and protected at the local level.

Fundamental Issues Still Unresolved

In Bob's 2006 IEEE Spectrum article "Dying for Data," he raises fundamental issues that are yet to be addressed and resolved in 2009.

The current goal is to have an EHR for every American by 2020.

Resources

U.S. Health and Human Services Health Information Technology website

Government Health IT website and magazine (requires free registration)

Modern Health Care website and magazine (requires free registration)

Porter, Michael. Redefining Health Care. Harvard Business School Publishing, May 2006.

Porter, Michael. "A Strategy for Health Care Reform – Toward a Value-Based System." The New England Journal of Medicine Volume 361:109-112, Number 2, July 9, 2009.

Charette, Robert. "Electronic Health Records No Guarantee of Quality Health Care." IEEE Spectrum Risk Factor blog, June 22, 2009.

Charette, Robert. “EHRs: The Good, the Bad, and the Ugly.” IEEE Spectrum Risk Factor blog, March 2, 2009.

Charette, Robert. “Dying for Data.” IEEE Spectrum, October 2006.

Goldman, David. “Electronic Health Records: A Checkup.” CNNMoney.com, July 2, 2009.

Deloitte. “Global Life Sciences & Health Care Security Study.” Deloitte Touche Tohmatsu, July 2009.

FTC Rule Expands Health Data Breach Notification Responsibility to Web-Based Entities (August 18, 2009)

The US Federal Trade Commission has issued a final rule on health care breach notification. The rule will require web-based businesses that store or manage health care information to notify customers in the event of a data security breach. Such entities are often not bound by the requirements of the Health Insurance Portability and Accountability Act (HIPAA); this rule addresses that discrepancy.