



Pre-conference Symposium

Security and Privacy Issues in Electronic Health Records Acquisition and Implementation

Presented by Lesley Berkeyheiser, Principal The Clayton
Group, WEDI SNIP S&P Co-Chair

Susan A. Miller, JD., COO, CPO HealthTransactions.com

The Pluses and Minuses In EHR

Presented by

Lesley Berkeyheiser, Principal The Clayton Group

Susan A. Miller, JD., COO, CPO HealthTransactions.com

The Pluses and Minuses in EHR

- First: How the EHR Environment is Changing
- Lessons Learned from EHR Implementation
- Privacy/EHR Challenges
- Security/EHR
- TCS & NPI EHR Impacts

EHR Basics

- ◆ EHR systems in some form have been around for over ten years
- ◆ The dramatic increase in computer “power” and low cost have helped promote EHR’s as a practical solution
- ◆ The EHR market has evolved on two paths equally
 - ◆ stand alone products and
 - ◆ EHRs that have evolved from billing systems
- ◆ There are a wide range of solutions from simple super bill systems to electronic charts to full EHRs
- ◆ Definitions: EMR versus Electronic Health Record?
 - ◆ Versus Computerized Medical Records?



The Business Case for an EHR

Most of the reasons for implementing an EMR have remained the same for

years

1. Reduce office time spent filing and looking for charts
2. Improve continuity of care—legibility
3. Improved patient safety
4. Patient recalls ---the Vioxx challenge

Some new reasons too---

1. Diagnostic results automatically interface
2. Clinical guidelines and protocols
3. Standardization among providers
4. Improved workflow
5. Automated prescribing, referrals
6. Possible improved coding
7. Participate in clinical trials
8. Future---HIPAA claims attachment and WC first report of injury

What About the Continuity of Care Record?

- ◆ Began as a standardized paper referral form used in Massachusetts
- ◆ Has evolved into a sophisticated but simple concept---providing key medical data to health care providers who have been referred a patient or see the patient in an emergent setting
- ◆ *It is a subset of a full EHR*

Primary Components of a CCR

- ◆ Patient insurance information
- ◆ Vital signs
- ◆ Allergies and alerts
- ◆ Medications
- ◆ Lab results
- ◆ Current health status
- ◆ Diagnoses
- ◆ Recent care and procedures
- ◆ Care plans for the future

Discussion: Interoperability

- ◆ Can the EMR import data and export data technically, security and in a way that reasonably ensures privacy?
- ◆ Why is this important? Ease of importing and exporting data?
- ◆ Don't forget the conversion.....you won't keep the system forever
- ◆ Some vendors rely on locking you into their system
- ◆ How easy will the next conversion be?
 - Those of you who have lived through a billing system conversion - --multiply that many times for what an EHR conversion

More on Interoperability

- ◆ The key standard today is HL7
- ◆ What is HL7?
- ◆ There are two ways an EMR can interface with HL7—it is written into each field or it is mapped...many third party solutions exist
- ◆ But if your vendor gives you a “blank” stare you are in trouble!!!!

Now Everybody Else...

◆ Is Getting Involved:

- NHIN
- RHIO's
- ONCHIT- The President!



Community Health Information Networks

- ◆ Now known as Regional Health Information Organizations—they now have a federal mandate
- ◆ The National Health Information Network initiative has tremendous political and community support
 - Driven on a local community level
- ◆ Many are providing best of breed EHR solutions—or at least performing a community review
- ◆ These will then be interfaced to the RHIO
- ◆ The RHIO concept is anchored to the CCR
 - [previously discussed]

Current I Undertakings

- ◆ Appointed groups working as part of the ONCHIT “Privacy and Security Barriers to EHR Adoption Initiative” are currently working through multiple scenarios to spur workgroup discussion in order to carve potential solutions.
- ◆ Areas for discussion may include:
 - Sharing information electronically across state law boundaries
 - Handling information considered extremely sensitive such as mental health, drug and alcohol, HIV, family planning and genetic testing
 - Determining appropriate access based on personal representative status (custody issues, handling of deceased information).

Main Legal Barriers to EHRs *Used to Be*



- ◆ Paper-era state regulations may not permit EHRs (proposed HR 2175 would preempt such state regulations)
- ◆ The Anti-kickback Statute
- ◆ The Stark anti-referral rules
- ◆ Concerns about enhanced malpractice exposure
- ◆ HIPAA and individual state's privacy and security regulations
- ◆ In some contexts, the anti-trust laws



Partnering for Electronic Delivery
of Information in Healthcare


◆ So What Do Our New Rules Say?

- Safe Harbors and Exceptions

§ 411.351 Definitions

- ◆ ***Electronic health record*** means a repository of consumer health status information in computer processable form used for clinical diagnosis and treatment for a broad array of clinical conditions.
- ◆ ***Interoperable*** means able to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks, in various settings; and exchange data such that the clinical or operational purpose and meaning of the data are preserved and unaltered.

CMS	MMA-mandated electronic prescribing exception § 411.357(v)	Electronic health records exception § 411.357(w)
Authority for Exception Covered Technology	Section 101 of the MMA Items and services that are necessary and used solely to transmit and receive electronic prescription information. Includes hardware, software, internet connectivity, and training and support services.	Section 1877(b)(4) of the Social Security Act. Software necessary and used predominantly to create, maintain, transmit, or receive electronic health records. Software packages may include functions related to patient administration, for example, scheduling functions, billing, and clinical support. Software must include electronic prescribing capability. Information technology and training services, which would include, for example, internet connectivity and help desk support services.
Standards with Which Donated Technology Must Comply.	Applicable standards for electronic prescribing under Part D (currently, the first set of these standards is codified at § 423.160).	Electronic prescribing capability must comply with the applicable standards for electronic prescribing under Part D (currently, the first set of these standards is codified at § 423.160). Electronic health records software must be interoperable. Software may be deemed interoperable under certain circumstances.
Donors and Recipients	As required by statute, protected donors and recipients are hospitals to members of their medical staffs; group practices to physician members; PDP sponsors and MA organizations to prescribing physicians.	Entities that furnish designated health services (DHS) to any physician.
Selection of Recipients	Donors may not take into account directly or indirectly the volume or value of referrals from the recipient or other business generated between the parties.	Donors may use selection criteria that are not directly related to the volume or value of referrals from the recipient or other business generated between the parties
Value of Protected Technology	No limit on the value of donations of electronic prescribing technology.	Physician recipients must pay 15 percent of the donor's cost for the donated technology and training services. The donor may not finance the physician recipient's payment or loan funds to the physician recipient for use by the physician recipient to pay for the items and services
Expiration of the Exception	None	Exception sunsets on December 31, 2013.

	MMA-mandated electronic prescribing exception § 411.357(v)	Electronic health records exception § 411.357(w)
Authority for Final Safe Harbor	Section 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003.	Section 1128B(b)(3)(E) of the Social Security Act.
Covered Technology	Items and services that are necessary and used solely to transmit and receive electronic prescription information. Includes hardware, software, internet connectivity, and training and support services.	Software necessary and used predominantly to create, maintain, transmit, or receive electronic health records. Software <i>must</i> include an electronic prescribing component. (Software packages may also include functions related to patient administration, for example, scheduling, billing, and clinical support.) Information technology and training services, which could include, for example, internet connectivity and help desk support services. Does not include hardware.
Standards with Which Donated Technology Must Comply.	Final standards for electronic prescribing as adopted by the Secretary.	Electronic health records software that is interoperable. Certified software may be deemed interoperable under certain circumstances. Electronic prescribing capability must comply with final standards for electronic prescribing adopted by the Secretary.
Donors and Recipients	As required by statute, protected donors and recipients are hospitals to members of their medical staffs, group practices to physician members, PDP sponsors and MA organizations to network pharmacists and pharmacies, and to prescribing health care professionals.	Protected donors are (i) individuals and entities that provide covered services and submit claims or requests for payment, either directly or through reassignment, to any Federal health care program and (ii) health plans. Protected recipients are individuals and entities.
Selection of Recipients	Donors may not select recipients using any method that takes into account the volume or value of referrals from the recipient or other business generated between the parties.	Donors may not select recipients using any method that takes into account <i>directly</i> the volume or value of referrals from the recipient or other business generated between the parties.
Value of Protected Technology	No limit on the value of donations of electronic prescribing technology.	Recipients must pay 15% of the donor's cost for the donated technology. The donor (or any affiliate) must not finance the recipient's payment or loan funds to the recipient for use by the recipient to pay for the technology.
Expiration of the Safe Harbor	None	Safe harbor sunsets on December 31, 2013.

Final Rules

- ◆ Remove barriers to E-Prescribing and EHR Contracts
 - Purpose: To allow entities to donate technology for e-prescribing and HER without triggering anti-kickback statute or Stark law.
 - Allows for hospitals and doctors to invest together in expensive technology
- ◆ Final Rules Published August 8, 2006
 - OIG and CMS Parallel

Final Rules

- ◆ CMS Rule states that EHR software must be “interoperable”
- ◆ Recipients must pay 15% of cost of EHR technology and services
- ◆ OIG Rule covers a broad array of providers (suppliers, practitioners, health plans) when they provide EHR technology to physicians (and others)



Partnering for Electronic Delivery
of Information in Healthcare

Remember currently...

Less than 25% of doctors offices have
e-prescribing or EHR capabilities.

-Tom Leary, HIMSS

To Increase Participation ...

- ◆ We have to figure a way around:
 - Interoperability
 - Privacy and Security Barriers- RTI/AHRQ
 - Plain Old Privacy and Security Issues
 - The same ones we had before the EHR!

Privacy is Often THE HR Issue!

- ◆ As highlighted - the most frequent breaches of patient information confidentiality come from authorized insiders in the many organizations
 - Most with a justified need to access health information, not from outsiders
- ◆ The unauthorized sharing of sensitive health information can result in a wide range of undesirable outcomes
 - For both the patient and the facility

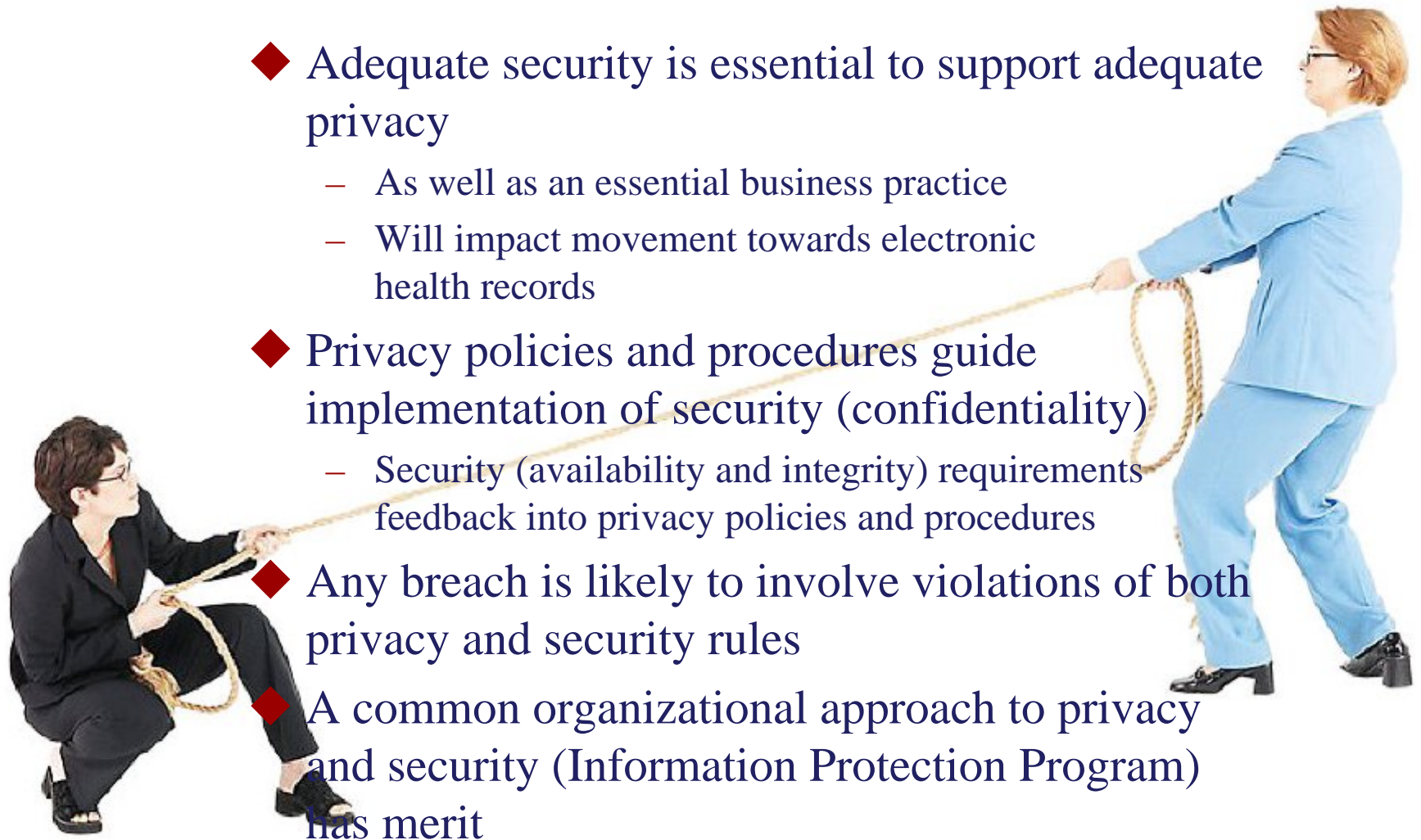


Expanding HIPAA Role?

- ◆ EHR Success will demand expansion of HIPAA standards of “PHI use and care” beyond covered entities
- ◆ Individual access and participation in the information flow
 - For many individuals the decision about whether or not to participate in the EHR will be influenced by how much control they could expect to have over the information kept on the record



Tangled Bottom Line



- ◆ Adequate security is essential to support adequate privacy
 - As well as an essential business practice
 - Will impact movement towards electronic health records
- ◆ Privacy policies and procedures guide implementation of security (confidentiality)
 - Security (availability and integrity) requirements feedback into privacy policies and procedures
- ◆ Any breach is likely to involve violations of both privacy and security rules
- ◆ A common organizational approach to privacy and security (Information Protection Program) has merit



Partnering for Electronic Delivery
of Information in Healthcare

HIPAA to the Rescue

- ◆ The HIPAA Security Rule calls for technical safeguards to protect EHR information against:
 - Unauthorized access
 - Alteration
 - Deletion
 - Transmission
- ◆ Requires unique user access and audit trail
- ◆ Suggests encryption (data at rest and in transit), role-based, context-based and user-based access controls



AHIMA 2006 Survey

- ◆ American Health Information Management Association (AHIMA) surveys healthcare privacy officers and others whose jobs relate to the HIPAA privacy function to:
 - gain an understanding of where healthcare organizations stand with regard to implementing the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA).

- ◆ AHIMA intends the results of the survey will:
 - reinforce the importance of protecting the privacy, confidentiality, and security of personal health information.
 - help the industry understand the most areas of privacy and security implementation that may need more study.
 - the findings are particularly significant in light of the research currently being conducted by the Health Information Security and Privacy Collaboration (HISPC) at the behest of the Office of the National Coordinator for Health Information Technology (ONCHIT).

Privacy Challenges

- ◆ Under HIPAA, individuals have the right to ask for an **accounting of all disclosures of protected health information** for purposes other than treatment, payment, or healthcare operations.
- ◆ As found in previous surveys, this requirement was the most significant issue for respondents, with *15 percent indicating that it was moderately to extremely difficult*.

AHIMA 2006 Survey Results



Privacy Challenges

In 2006, *10 percent* of respondents reported difficulty **obtaining protected health information from other providers**. Anecdotes indicate that the problem may be particularly acute for schools (because of conflicting state and federal Department of Education laws and regulations) and for individual practices that do not understand their options under HIPAA.

This is an area where the Office of the National Coordinator on Health Information Technology's study on privacy may be able to shed additional light.

AHIMA 2006 Survey Results

Privacy Challenges

- ◆ **Access and release of information to patients' relatives or significant others is a problem for *9 percent of the respondents***
 - The reasons why are numerous
- ◆ Respondents note that identifying a patient's personal representative can be complex, as can various laws associated with durable power of attorney. Others note that getting patients, relatives or significant others, institutions, and laws to all agree is often difficult.

Privacy Challenges

- ◆ **Signed acknowledgements of the Notice of Privacy Practices**
Can the EMR alert users when a signed acknowledgement is not on file?
- ◆ **Special privacy protections** have been requested
Can the EMR alert users when a patient or their personal representative has requested special privacy protections?
- ◆ **Alternative confidential communications channels**
Can the EMR alert users when a patient or their personal representative has requested (and the practice has agreed) an alternative form of communication?
- ◆ **Amendment of protected health information**
Can the EMR alert users when a patient has requested an amendment to their protected health information and the practice has agreed to this?
Can the EMR alert users when this has not been agreed to and a statement of disagreement from the patient is recorded?

Privacy Challenges

◆ Requests for protected health information

Can the EMR easily create a printed copy of the records when a valid request for a copy is received and approved?

Can the EMR provide the practice with an easy way to provide inspection of the records (viewing) rather than creating a printed copy?

Does this inspection method provide security against the patient or their personal representative altering the records?

Can the EMR provide the practice with an easy way to limit or select the record for copying or viewing (for example if the practice determines that the patient should not have access to protected health information (for example information that might endanger the life or physical safety of the patient or another person)?



Privacy Challenges

Some consumers are becoming more aware of the importance of the **privacy of health information**, as evidenced by the increased number of questions providers report being asked by patients.

More disturbingly, nearly a quarter reported encountering consumers who refused to sign release of information forms.

More research is needed to understand how deep those fears are or what consumers are most worried about. Clearly the industry now has an opportunity to educate consumers on how their personal health information will (or should) be protected. This is an important step. Without consumer confidence the national health information network will never succeed.



Partnering for Electronic Delivery
of Information in Healthcare

Implementation Challenges

Case Study Experience

◆ Finding:

“One of the biggest barriers to overcome has been the tension between getting a system that would be ideal (ideal means it would include notes from all providers on what was happening with patient medically and behaviorally) and getting a system implemented in a short tie that will function.” -Arizona Health Care Cost Containment System Health Information Exchange

◆ Solution: “Use more limited projects to demonstrate early success.”

Case Study Experience

- ◆ Findings:
“Providers are hesitant to share clinical data on a real-time basis because of concerns around competition and quality. IN particular, these concerns center around comparisons of patient outcomes without adequate risk adjustment or measuring quality based on non-representative patient outcomes.”
- ◆ **Solution:** “Acknowledge the importance of engaging physicians early and often in discussions”.

-Evolution of State Health Information Exchange, A Study of Vision, Strategy and Progress.
Jan 2006

EHR Implementation Case Study: Security Challenges

- ◆ Small OBGYN (multiple offices). Decided to purchase an HER for new expansion office. Process of selection went well. However, the selection team did not include a network systems person. Long story short- the provider wanted to expand the HER to an additional office and while they were considering this business change were subject to an electricity loss for 24 hours.
- ◆ Desire: Want to reroute the HER and service patients at another site if server is down. Surprise- Vendor will not support use of redundant servers- software would run very slowly.
- ◆ Lessons Learned:
 - **Physicians are loving remote access.**
 - **Initial implementation was in a new office location- volume was slow- a smart move.**
 - **Now trying to implement in larger practice.. Real problem- “Older women”!**
 - **To do again: Keep better track of comparison and rating against systems. Make sure a stronger DR plan is in place. Not just EHR- don’t forget the telephones too.**
 - **Vendor support issues are tricky- monitor them closely!**

Other Security Challenges

- ◆ Facility and physical site-Analyze current facility for efficient workflow; identify areas of improvement and areas needing upgrade to support additional hardware (power, HVAC, security and so forth).
- ◆ Existing IT infrastructure- Analyze existing information system networks for upgrade readiness. Identify problems and capabilities.
- ◆ Telephony and broadband- Analyze current telephone system and identify problems; analyze availability of broadband access.
- ◆ Review existing issues with software field support, hardware field support.

Disaster Planning

- ◆ Katrina
- ◆ 9/11
- ◆ Once ALL data is electronic- the requirement is even MORE important!

Things To Remember

- ◆ Organized documentation
- ◆ Focus Resource on Selection
- ◆ Establishment of champions (clinical, clerical)
- ◆ Certification- Ascertain that the vendor will seriously seek certification by CCHIT.
- ◆ Evaluation-Vendor presentation ranked against features toolset and baseline features.
- ◆ HIPAA evaluation-Vendor evaluated against HIPAA criteria
- ◆ Company profile-Company stability, experience, and related attributes reviewed.

◆ The Transaction and Code Set (and NPI) intersection with an EHR:

- Everything must transition to the standard
 - TCS, 4010A1, 5010, NPI etc...
- NPI number sharing may concern providers
- NPI and TCS information should always be protected and safeguarded... the increased automation may increase the risk of inappropriate access.

Q & A

- Individual Questions?





Contact Information

Lesley Berkeyheiser-

“lberkeyheiser@theclaytongroup.org”

Susan Miller –

susan.miller@healthtransactions.com