Security Issues and Possible Solutions: EHRs and HIEs

J. David Kirby
Kirby Information Management Consulting LLC
Dave@KirbyIMC.com, 919-272-1157

EHRs and Health Information Exchange:

- Individual information related to health and health care is marooned – largely in health care facilities.
- These information islands have led lives that did not require that they share much of this information or share it often.
- There are forces at work that will likely change this in the next few years.
- Routine, wide spread data sharing with a variety of other parties in support of mission-critical applications shifts and grows information security risks and therefore demands new and improved security measures.

Consider this a map.

- No one fully knows what it will be like when there is widespread routine use of health information sharing.
- But, there are some issues that will clearly arise.
- This presentation seeks to:
  - offer some insights into what this new life will be like ,
  - provide questions that EHR managers should ask when developing data sharing processes and
  - provide guidance on how to manage the security issues involved.

Elements driving this chang

- Concerns about:
  - The cost of health care:
    - US health care is much more expensive per capita than our industrial peers. The amount is beginning to sap resources from other societal needs.
  - The quality of health care
    - Health care practice is frequently not based on best practices. What best practices should be is not always well understood.
  - The safety of health care
    - Many practices (or lack of practices) injure and kill people.
  - The need to go beyond traditional health care in order to better assure the nations' health.
    - Our health only partially depends on what care we get when we get sick. How we stay well matters much more.
- The Meaningful Use (MU) criteria derived from the HITECH HITECH Act focus on all of these and provide incentives/penalties designed to supercharge the adoption rate for EHRs and HIE. The MU criteria explicitly require a review of or new risk analysis and any needed changes in security risk management.

- A core need in dealing with all of these problems is to share health data more widely, more often, and to use the shared data to improve health and care.

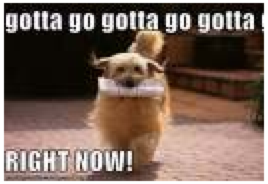
HIE’s, RHIO’s, PHRs, HRBs

- The chief health data sharing concepts today are:
  - HIE – Health Information Exchange –
    - A vehicle for moving individual health information among appropriate parties.
  - RHIO – Regional Health Information Organization –
    - An HIE supporting organization in a given region.
  - EHR – Electronic Health Record – software used to support clinic operations in the typical provider setting.
  - PHR – (Networked) Personal Health Record –
    - Vehicle for storing and using individual health information primarily managed by the person who is the subject of the data (or his designee). A networked PHR gets data from various sources and makes it available to other health team members.
  - HRB – Health Record Bank –
    - A facility for storing and sharing individual health information that is comprehensive and longitudinal for a given person. Access is controlled by the person who is the subject of the data (or his designee).
  - **Let’s call all of these concepts– Health Information Networks (HINs)**

Hopes and concerns

- Each of these concepts hopes to :
  - Improve care, lower costs, improve safety
  - The PHR and HRB ideas also focus on empowering patients/consumers/clients/recipients in order to have a greater impact on health than can be obtained with a focus on acute care only.
- They all give rise to three (traditional) security concerns (for all parties):
  - **Confidentiality**:
    - What if the PHI is not handled confidentially?
    - Do I have to be more protective than I am now?
  - **Integrity**:
    - Will the data provided have the level of integrity that I need (i.e. will it be sufficiently complete, correct, and current)?
    - Will I need to do something to improve integrity?
  - **Availability**:
    - What if the data is not available when I need it?
    - Do I have to take more measures to make PHI available?

Applying security concepts to EHRs sharing data via HINs



- But, these general concepts have to be applied in some new ways.
- Several factors make HIN security feel like a new area when compared with traditional (i.e. low-sharing) environments.
- The speed of demand for HINs (especially based on the HITECH incentives) will likely imply that typical ISO's deal with this topic before there are well worn answers. **You can't likely wait.**
- Let's look at the factors that make HIN security different from the perspective of a typical EHR manager in the typical hospital.

Key factors driving security risk in the EHR/HINs

- Distribution of Security Risk among various semi-autonomous parties.
- Size and dynamism of the data sharing community.
- Use of comprehensive (or at least aggregated) longitudinal record
- Changes in amount and effects of erroneous data being shared.
- Changing environment of laws, standards, regulations.

Factor 1: Risk Distribution

- The typical hospital focuses primarily on security for its internal operations and considers risks to itself when selecting security measures. (e.g. risk of inappropriate use/disclosure of PHI)
- When an EHR shares data via a HIN, security risks are distributed across the HIN users.
- The risk sharing model must satisfy each party (e.g. hospital, physicians, payers, patients, public health, researchers) or they won’t participate fully (or at least resist, minimize participating).
- Making security cost-benefit tradeoffs that satisfy everyone in the sharing system is harder than making tradeoffs that only have to satisfy a single EHR manager.

Risk Distribution Example–

- How will a HIN manage the risk of inappropriate disclosure of PHI?
- The risk model for sharing on paper today involves a lot of humans as part of the protections – and as part of the risk.
- A HIN model won't likely have as many people involved in manual steps and will likely share data much more frequently than our paper sharing system. So, it will have to depend more on software to enforce rules– software operated by a variety of providers, patients, payers, medical researchers etc.
- Increasingly, policy favors letting patients control PHI flow across institutions. How will this affect the risk management of inappropriate disclosure?
- Will the protections needed outweigh the impetus to be part of the HIN (say, for physicians)?

Factor 2: Large and Dynamic Health Info Sharing Community

- Typical HIN will have a large and dynamic community of information providers and recipients. – (e.g. hospitals, physicians, patients, payers, researchers, public health).
- Consider the challenge of managing registration, authentication, access audits, and authorizations among the members of this large and dynamic group.
- How will access changes be made when practitioners are no longer eligible for access (retired, quit, fired). How will changes in the legal competence of individuals affect access?
- Just to make things interesting – you can’t depend on having a compulsory universal health identifier.

Factor 3: Comprehensive Longitudinal Record (CLR)

- Having all (or at least much more) of the relevant historical data about a person “together” for access for care, research, and personal use is a core motive for EHR-using providers to participate in HINS.
- But, having this CLR also raises the risk of inappropriate disclosure.
- Data shared in this community may be used over longer times and for purposes not expected by the data originator. These limits on time and usage today help manage the risk of data being used for purposes for which it is not suitable/permitted.
- Having the data in one “place” means that availability depends on that place being up and on being connected to the inquiring party.
- What happens when a HIN goes out of business? Are there data escrow measures that will assure that the data is made available for use elsewhere? by whom? to whom?

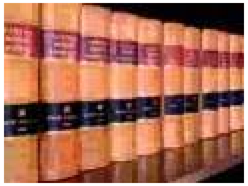
Factor 4: Erroneous PHI

- Well functioning HINs spread data quickly – whether it is true or not. So, errors will spread quickly.
- Errors come from two main sources:
  - Accident –
    - usually human error;
    - right data – wrong patient mismatch is a typical error (Factoid: About .1% to 1% of patient record selection operations that precede data entry select the wrong patient)
    - Small environments (typical medical practice) with a lot of context and personal knowledge of patients help to keep this problem down.
  - Fraud, Medical ID Theft
    - To obtain services without paying
    - To hide conditions
    - To obtain money for services not rendered
  - EHR data sharing with HINs will likely exacerbate the level of erroneous data – due to the relative “distance” (in time, space, context) of the provider of the data from the user of the data.

Erroneous PHI

- HINs must have a new set of measures to reduce both risks and consequences or:
  - A) suffer the consequences of using bad data or
  - B) suffer the consequences of not having the data be used.
- How will errors be corrected (amended!). How may patients be involved in detecting and amending information?
- How will recipients of data in error be notified to examine whether the error led to inappropriate action?
- OCR’s Privacy and Security Framework has a treatment of HIPAA Privacy Rule obligations related to correcting records used in an HIE.

Factor 5: Law, regulation and standards



- There is a large and growing set of public policies (i.e. laws and regulations) related to health information security and privacy.
  - Generally they are meant:
    - to protect the person who is the subject of the information from misuse of their information by others (third party disclosure laws),
    - to help make amends if the information is misused, and
    - to assure that the person has reasonable access to the data.

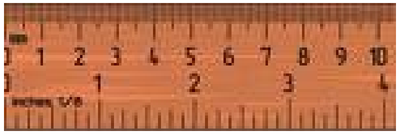
Key Law, regulation and standards

- HIPAA’s Privacy and Security Rules
- Special regulations covering drug and alcohol treatment records, and mental health records (42 CFR Part 2),
- Regulations related to information management in medical research (21 CFR part 11),
- State-specific medical practice laws,
- State identity theft protection statutes, and
- Accreditation standards related to information security and privacy
- New P&S provisions in HITECH- both direct requirements (e.g. Accounting of TPO e-disclosures) and indirect (e.g. data sharing with patients creates new security challenges)
- MU requirements in the HITECH (that incentivize PHI sharing)
- Both the specifics of these laws are becoming more burdensome and the enforcement/penalty levels are growing.

New Key HITECH Provisions

- **Breach Notice**: Obligations to notify patients and government (and media in some cases) of a breach of confidentiality of "unsecured" PHI.
- **BAs** – Directly covered by the main portions of the HIPAA Security and Privacy Rules.
- **Felony for knowing and illicit PHI use/disclosure-** now clearly applies to individuals (e.g. staff members).
- **Enforcement**: Greater fines, not-for-cause audits to be routine, no informal settlements, willful neglect penalized, state AGs can pursue, patients who have PHI breached may get a "cut" of the fine.
- **Restrictions**: Full pay patients may require restriction of disclosure of PHI to payers.
- **Accounting of disclosures** – for TPO now
- **No selling record** – without authorization from patient.
- **Right of access-** patient can require that e-PHI be transmitted in e-form to him/her.
- **Less internal use of PHI** – various requirements that will limit the use of PHI under the color of "health care operations" and require (effectively) use of limited datasets/deidentified data.
- **HHS program to inform** the public, providers, etc.
- Details for most items due from HHS by 180 days from enactment.
- Definition of "secured" data out now.
- **MU requirements** that compel/incentivize sharing of data electronically with patients

Standards, Guidance



- HHS Office of Civil Rights recently published a large collection of guidance as to how the HIPAA Privacy Rule apply to HINs
- NCVHS has recommendation on PHR security
- CCHIT has technical security standards for EMRs and HIEs. (PHRs likely coming next year)
- Healthcare Information Technology Standards Panel (HITSP)
- Health Information Security and Privacy Collaborative (HISPC).
- Integrating the Healthcare Enterprise (IHE)
- All of these can help the islanders. Using them will require thought and work. They are not canned answers to P&S issues in HINs.

A tale of two HINs

- **Let analyze the risk profiles for two types of HINs in which EHR-using providers participate--**

- **Entity-oriented HINs (EOHINs)**- focus on movement of data among third parties (e.g. providers)
- **Person-oriented HINs (POHINs)**- focus on movement of data to the person (or person's agent) for storage and/or provision to others (e.g. providers).

- **There will likely be hybrids of these two types of HIN - with an associated mixture of security risks.**

Sharing data in an EOHIN

- **Entity-oriented HINs** – focus on movement of data among third parties (e.g. providers)
  - Controlled by third party disclosure laws.
  - Limited by the interests of the parties in engaging in exchange
  - EOHIN is typically BA (under HIPAA) of the covered entities participating
  - Only move PHI of patients in common (or rarely via HIPAA Authorization)
  - May or may not have a full central store.
  - Almost always has at least an “index” of data locations.

Key risk management issues if integrating with an EOHIN.

- Confidentiality:
  - Right patient: How will patients be reliably identified?
  - Right recipient : How will you (the EHR-using provider) assure that the PHI is being delivered to an authorized party?
  - Permissibility: How will you assure that the disclosure is permissible – by law and institutional policy?
  - Handoff of legal risk: When in the HIN process does your legal/regulatory/accreditation responsibility to protect PHI begin and end?
  - Handoff of PR risk: When in the HIN process does your need to protect your reputation with the public as related to your protection of patient data begin and end?
  - Costs: What will it cost to reduce confidentiality risk to a level that is acceptable?
  - Internal benefit: What are the benefits to HIN for your organization?
  - Balance: Is the cost/benefit ratio favorable?

Key risk management issues if integrating with an EOHIN.

- Integrity:
  - Right data out: When you deliver PHI that is acted on by others, what is the extent of your obligation (legal, public) to assure that the data is correct, current, and delivered in a timely way?
  - Right data in: When you accept PHI for others, how would integrity risk limit your use of the data?
  - Correcting errors: When you or another party discovers that delivered PHI is incorrect, how will correction to the data and potential remedial care be managed?
  - Balance: Is the cost/benefit for these operations favorable?

- Availability
  - You up: How does the EO-HIN model affect your obligation to have information systems and clinical/business services up and operating to obtain and release PHI?
  - Them up: Are the other EO-HIN participants able to meet your availability needs in delivering PHI?
  - Middle up: What uptime requirements are there for the EO-HIN itself?

Ongoing Risk Management

- New laws, regulations, and underlying changes in the risk set will likely occur over time. (There is already talk at the federal level of more health privacy legislation.)
- So, revisit your risk analysis and adjust your risk management plan (HIPAA/HITECH requirements) on a regular basis.

Integrating with a POHIN

- **Person-oriented HINs (POHINs)**- focus on movement of data to the person (or person's agent) for storage and/or provision to others (e.g. providers).
  - Controlled by the patient (or designee) through a software agent.
  - Limited by interest of patient in sharing/using the data. (or adding to it)
  - Typically not a BA of the providers
  - Typically has a full store of the data (e.g. a Health Record Bank).
  - Not tethered to any one provider/payer institution.

POHIN flow foundations

- Patients have a right to copies of their PHI held by HIPAA covered entities in the form that they request (and to an e-copy of e-PHI in an EHR at labor costs only under HITECH).
- Patients can share their PHI with whomever they wish – state/national/organizational boundaries do not matter. (i.e. EHR-using provider doesn’t have disclosure risk once ePHI is in patient’s control)
- Accounting for disclosures to the patient is not required- though you may need to keep up with what data was given to whom in the case that you mis-release information to the wrong person.
- Minimum necessary considerations do not apply.

Some Patient motives to use a POHIN:

- Better health: Patients can use the PHI (together with some other resources) to better manage their health, be involved with their care, and coordinate their care. This will support improved health.
- More competition: Patients can more readily seek the best price for health services and products.
- Better data: Patients can spot errors in health records and can act to prevent the errors and limit damage (e.g. denial of insurance, fraud including medical identity theft).
- Better analysis: Patients can spot facts in lab/procedure reports that affect diagnosis and care that busy clinicians may overlook.
- Better monitoring: Patients can help detect (and prevent) inappropriate PHI access when the records include logs of access by others.
- More care providers helped: Patients can share records with their lay caregivers to help them in providing care.
  - There are 47 million lay caregivers for adults in the US today – a very large group. These lay caregivers can aid in achieving all of the advantages of the other points listed above as well as reduce their own burden in caring for the individual.
- Will they come? : Recent results from Kaiser-Permanente’s patient portal indicates that at least 50% of the general population (across all ages except teenagers) will become regular users.

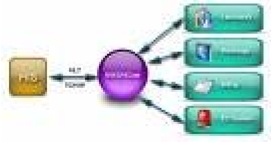
Concerns

- There are also non-security *concerns* about patients using their own PHI including:
- Lay interpretation limits: Limited patient ability to usefully interpret the records. This may result in confusion, distress, inappropriate action by patients, Workloads for healthcare providers may also increase.
- Driving care documentation underground: Less willingness on the part of providers' to accurately chart concerns knowing that the patient may be offended or distressed when reading such notes. This may endanger proper care.
- More competition: Loss of provider business to competitors as patients is more easily able to seek care given that they have their PHI.

Who is building/supporting facilities with PO-HIN principles?

- LouHIE – Louisville Health Information Exchange.
- Washington State (its state-wide RHIO principle base);
- Health Record Bank of Oregon
- New York Presbyterian Hospital – (MyNYPHR)
- CareEntrust – of Kansas City MO
- Healthy Ocala – of Ocala Florida
- State of Kentucky – statewide health information exchange
- Duke Heart Center’s Health Record Network
- Northrop Grumman's NHIN prototype
- Dossia (a joint project with Intel, Wal-Mart. AT&T, Cardinal Health, New Orleans Health Dept, and others),
- NC Southern Piedmont Health Information Exchange (SoPHIE). http://tinyurl.com/NC-SoPHIE
- SharedCarePlan.org – an RWJ project in Whatcom County Washington
- The last round of implementation grants for the National Health Information Infrastructure (for projects like this) require significant consumer information flow controls.
- HRN (the Health Record Network). http://www.healthrecord.org/
- Vendor Examples: YouTakeControl, Patient Command, eHealthTrust, Microsoft HealthVault, SharedCarePlan, Google Health, Dossia, iHealthRecord, WorldDoc, Cerner Healthe Intelligence, Network of Care.

Security Dimension of Integration Engines



- A new type of facility:
  - Focuses on connecting personal health software for consumers with health software for providers.
- E.g. Microsoft HealthVault, Google Health
- Security overall depends somewhat on the engine (and terms of its use) along with the person-end software and the provider-end software (and policy).

POHIN cf. EOHIN Security/Privacy Keys

- Confidentiality:
  - Patient controls sharing. So, provider liability sharing burden is lower.
  - Privacy policy is per person (rather than one size fits all)
  - Audit facilities allow for consumer attention to misuse.
- Integrity:
  - Patients can see many types of incorrect data (especially patient mismatches). Fraud and Medical ID Theft potential is lower.
  - Digital signature may be needed to prevent patients changing data that purports to be from a provider without detection. (and also provides irrefutable records from clinicians)
  - Reliable id of patients is easier (i.e. providers use the POHIN id that the patient provides)
- Availability:
  - Both patient and provider may have copies of data for their own use.
  - EOHIN broadband net availability based on hardened dedicated links may be better.
- Transparency and choice:
  - EOHINs operate security based on HITECHngements among the providers.
  - POHINs using integration engines depend on market forces to shape Terms of Use from which consumers can choose.
  - POHINs formed using a public trust model are organized to support patient interests.
  - Both models will require notice of breach (which should help keep out the worst HINs)
- The risk questions for POHIN participation by a provider are the same as for an EOHIN. The answers are different.

Hybrids

- We are likely to see POHIN and EOHIN hybrids emerge.
- POHIN-like facilities will likely be needed to support patient e-PHI delivery compliance and some facilities (e.g. Kaiser-Permanente) will decide that they should maximize usage of this.
- EOHIN-like facilities may be used where providers prefer to work among themselves by flowing data (and are allowed to by law).

Q&A

- Thanks for your attention!
- Dave Kirby, Dave@KirbyIMC.com
- 919-272-1157

Supplementary slides:

Groups contributing to POHIN concept development

- American Health Information Management Association (AHIMA),
- HIMSS (joint project with AHIMA, HIMSS P&S Committee)
- the Markle Foundation,
- the Robert Wood Johnson Foundation (especially through its Project HealthDesign),
- the eHealthTrust,
- the IHE
- ONCHIT/AHIC (through consumer empowerment use case development)

Support for the risk distribution issue.

- There are similar risk distribution issues in the areas of data integrity and availability.
  - Who is responsible when shared data is wrong –and harm is done?
  - Who is responsible when data is supposed to be available but is not – and harm is done?
- Many groups have contributed to a first generation of ideas about how to manage HIN risk distribution:
  - The Markle Foundation
  - IHE – Integrating the Health Care Enterprise
  - The HIMSS P&S Toolkit
  - eHealthInitiative
  - HL7 – Health Level 7
  - HITSP – Health Information Technology Security and Privacy
  - HISPC – Health Information Security and Privacy Collaborative.
- No one has the complete answer in a form that will directly usable by the typical hospital ISO.

EOHIN Development Contributors

- Office of the National Coordinator for Health Information Technology (ONCHIT),
- the American Health Information Community (AHIC),
- the Markle Foundation,
- the e-Health Initiative,
- PrivacyRights.org ,
- Health Information Management Systems Society (HIMSS),
- the State Alliance for E-Health,
- the Certification Commission for Health Information Technology (CCHIT),
- OCR, IHE, AHIMA, and HITSP.
- NHIN Project

- (Note some of these are also POHIN development contributors)