anakam®
ENABLING TRUSTED ACCESS

Role of Privacy, Security, and HIE in Health Reform

William R. “Bill” Braithwaite, MD, PhD, FACMI
Chief Medical Officer
Anakam Inc.

September 16, 2009

Why is Health Information Technology Critical?

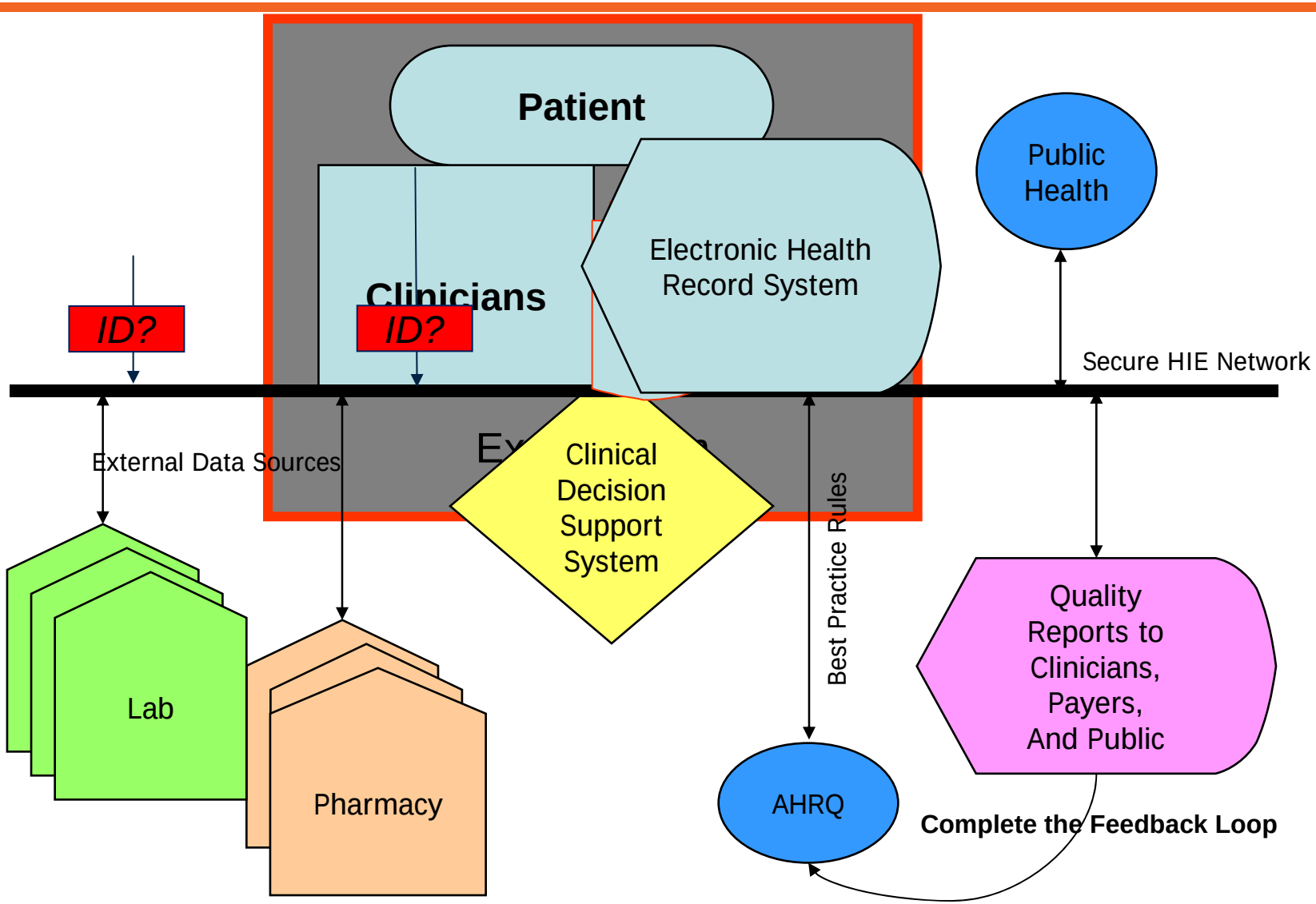
- **Avoidance of medical errors.**
  - Up to 98,000 avoidable annual hospital deaths due to medical errors.
- **Avoidance of healthcare waste.**
  - Up to $300B spent annually on treatments with no health yield.
  - We spend 2X per capita as any other industrialized nation.
  - We rank last in population health status.
- **Acceleration of health knowledge diffusion.**
  - Average of 17 years for medical evidence to be integrated into practice.
- **Reduction of variability in healthcare delivery and access.**
  - Access to specialty care is highly dependent on geography.

Why is Health Information Technology Critical?

- **Promotion of public health and preparedness.**
  - Surveillance is fragmented, and untimely.
- **Empowerment of consumer involvement in health management.**
  - Patients currently minimally involved in own health decisions.
- **Strengthening of health data privacy and protection.**
  - Public fear of identity theft and loss of privacy.

- **Healthcare Reform cannot do these things without HIT**
  - Paper records cannot solve these problems!

Evolution of New Healthcare Paradigm



Value of Interoperable HIE

- **Standardized, encoded, interoperable, electronic, clinical HIE saves money*:**
  - Net Benefits to Stakeholders of $78B/yr.
    - Providers - $34B
    - Payers - $22B
    - Labs - $13B
    - Radiology Centers - $8B
    - Pharmacies = $1B
  - Reduces administrative burden of manual exchange.
  - Decreases unnecessary duplicative tests.

  *From Center for Information Technology Leadership, 2004
- **HIE + EHR + CDSS => SAVES LIVES and $!**
  - e.g., Kaiser, Geisinger, VA, …
- **HIE is the KEY to health reform!**

The Challenge: A Complete Interoperability Profile

- **Standard Messaging**
  - Format
  - Structure
  - Terminology
  - Coding
- **Secure Conveyance**
  - Encryption
  - Transport
  - Authentication
- **Network Services**
  - Patient locator service
  - Terminology service
  - CDS rule source
- **Business issues**
  - Workflow integration
  - Professional resistance
- **"Organizational interoperability"**
  - Contracts and agreements
- **Privacy Issues**
  - Accurately linking patient records
  - Patient control over access
- **Other mutual security issues (trust)**
  - User identification, authentication, authorization, access, and audit.

Future for Healthcare

- **Goal: High quality, cost-effective healthcare.**
- **Means: Clinician/Patient interaction with Clinical Decision Support System (CDSS).**
- **Requires: EHR (with CDSS and HIE) and:**
  - **Interoperability** with sources of clinical data and sources of computable rules for best clinical practices.
  - **Incentives** to incorporate into healthcare practice.
  - **Investigations** of systemic failures to allow building systems that detect and prevent errors through feedback at the point of decision making.
  - **Trust** through agreement on standards for interoperable security and privacy (including patient consent).

Trust is the KEY to HIE

- **HIE takes control of PHI out of the hands of the trusted party (direct care provider).**
- **HIE accumulates access to large amounts of PHI, increasing the risks of unauthorized disclosures.**
- **Providers must trust the HIE system or they will not provide patient data.**
- **Patients must trust the HIE system or they will not give permission for their data to participate.**
- **HIE will fail without access to most PHI.**
- **Trust depends on believable privacy and security mechanisms and a clean track record …**

Principles of Fair Information Practice

- **Notice**
  - Existence and purpose of record-keeping systems must be known.
- **Choice – information is:**
  - Collected only with knowledge and permission of subject.
  - Used only in ways relevant to the purpose for which the data was collected.
  - Disclosed only with permission or overriding legal authority.
- **Access**
  - Individual right to see records and assure quality of information.
    - accurate, complete, and timely.
- **Security**
  - Reasonable safeguards for confidentiality, integrity, and availability of information.
- **Enforcement**
  - Violations result in reasonable penalties and mitigation.

Reasons for Privacy/Security

- **Discrimination**
  - Job
  - Health Insurance
- **Embarrassment**
  - Family
  - Friends
  - Anyone else
- **BUT, keeping secrets can kill you!**
  - High quality healthcare is dependent on the availability of high quality, timely information.
  - Missing information can lead to mistakes.
  - In healthcare, mistakes can kill you …

Definitions for Privacy & Security

- **Privacy is the right of an individual to**
  - control personal information and
  - not have it disclosed or used by others without permission.
- **Confidentiality is the obligation of another party to respect privacy by**
  - protecting personal information they receive and
  - preventing it from being used or disclosed without the subject's knowledge and permission.
- **Security is the means used protect the integrity, availability and confidentiality of information.**
  - physical, technical and administrative safeguards
- **The HIPAA Privacy Rule is about Confidentiality!**

HIPAA Privacy Rule of Thumb

- **Don't surprise the patient with a use or disclosure they don't expect!**
  1. Tell the patient about uses and disclosures necessarily part of normal operations of the healthcare enterprise (TPO).
     - e.g., listed in notice of privacy practices.
  2. Give the patient the opportunity to object to limited disclosures in common practice.
     - e.g., name in hospital directory.
  3. Follow required procedures for public policy exceptions.
     - e.g., required reporting of contagious disease.
  4. Get explicit permission for anything else.

New Privacy Issues

- **HSA**
  - Banks handling PHI to pay medical expenses
- **PHR**
  - Non Covered Entities handling PHI
- **HIE**
  - Consent granularity more than opt-in/opt-out
- **On-line services**
  - BA chain to off-shore services
  - Marketing banners and pop-ups
- **New Law**
  - Federal v. State law
  - Regulations

HIPAA Security Requirements

1. **Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.**
2. **Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.**
3. **Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule.**
4. **Ensure compliance by its workforce.**

Key Security Rule Philosophy

- **Identify & assess risks/threats to electronic information:**
  - **Availability**
  - **Integrity**
  - **Confidentiality**
- **Take reasonable steps to reduce risk.**
- **Involves policies/procedures & contracts with business associates as well as technology.**
  - **For security technology to work, behavioral safeguards must also be established and enforced.**
    - **requires administration commitment and responsibility.**

Flexibility of approach

- **Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications of the Security Rule.**
- **In deciding which security measures to use, a covered entity must take into account the following factors:**
  - The size, complexity, and capabilities of the covered entity.
  - The covered entity's technical infrastructure, hardware, and software security capabilities.
  - The costs of security measures.
  - The probability and criticality of potential risks to electronic protected health information.

Security Principles

- **Assess risk**
- **Manage risk**
  - Implement appropriate and reasonable administrative, physical, and technical security safeguards.
  - Consider size, complexity, technical infrastructure, hardware, and software security capabilities, costs, and the probability and criticality of potential risks.
- **Educate/Train**
- **Document and Monitor**
- **Repeat cycle periodically …**

Most Common Security Complaints

- **Unauthorized access to EPHI (90%).**
  - Employees or relatives accessing EPHI .
- **Loss or theft of devices containing EPHI (10%).**
  - Small volume of complaints; large volume of records.
- **Insufficient access controls for systems containing EPHI.**
  - Shared passwords.
  - Lack of encryption.

New Security Risks

- **Portable devices are being stolen.**
  - Portable media must be encrypted.
  - Consider “lo-jack” features.
- **Single factor authentication is inadequate for remote access to sensitive information**
  - Second factor authentication is now a requirement under CMS guidance and OMB Memoranda.
  - Some HIEs are also adopting strong authentication.
- **Health information is now a target for identity theft.**
  - Security must be a dynamic program responding constantly to new risks.

Security Conclusions

- **Security risks are constantly changing**
  - New and serious risks are being introduced at a very rapid rate; the unprepared are suffering.
- **Security services, tools, and methods are constantly changing.**
  - What was impossible or too costly to implement last year is now possible and cost-effective.
- **HIPAA Security Rule is clear.**
  - Security must include processes of risk assessment and management, repeated regularly, forever.
  - With appropriate risk assessment, the security rule can cover the new risks without needing to be changed.

HIPAA is the Floor

- **HIPAA Privacy Rule considers all personal health information equally sensitive.**
  - HIPAA permits patient health information to be used and disclosed for treatment, payment, and health care operations without patient consent.
  - Some state laws require patient consent even for treatment purposes.
  - A variety of federal and state statutes and regulations (laws) afford heightened privacy protections for certain classes of information generally perceived as sensitive and requiring special protections.

Inconsistency stalls HIE

- **Variations in privacy and security practices will impede HIE and HIT Initiatives unless resolved.**
- **States are starting to understand the issues.**
- **States are formulating solutions:**
  - Practice and Policy Solutions.
  - Legal and Regulatory Solutions.
  - Technology and Data Standards.
  - Education and Outreach.
- **Multi-state and National Level Recommendations are forthcoming.**

Engendering Trust

- **Trust is a critical issue that affects the viability of electronic HIE.**
- **Trust (or lack of it) leads organizations to draft extremely conservative policies that contribute to the variation in business practice and policy which in turn forms a barrier to HIE.**
- **Trust can be built over time by meeting and learning about the issues and views of other stakeholders.**
  - It takes leadership, time, and personal contact.

‘Consent’ is a Major Issue in Trust

- **Wide variation among organizations in practices and policies that determine when patient permission is required, how the permission is obtained and documented, and how patient permission is communicated to health care organizations, payers, and other outside entities.**
- **Variation caused by a number of factors, including:**
  - a basic misunderstanding of whether and when the HIPAA Privacy Rule required patient permission to disclose health information, particularly with respect to treatment;
  - confusion over the terms used for the process for obtaining patient permission;
  - federal and state laws with patient permission standards that differed from the HIPAA Privacy Rule, particularly those that applied to *specially protected health information*; and
  - organizational decisions to require patient permission as an added protection to reduce risk of liability for wrongful disclosure.

‘Consent’ is a Major Issue in Trust

- Consumers are concerned about how their health information is being managed, used, and disclosed electronically by providers, payers, researchers, and emerging HIEs and regional health information organizations (RHIOs).
- Providers are concerned about the appropriate interpretation of state laws related to consent for release of health information issues and the potential risks or liabilities associated with their failure to comply with such laws.

WHY THE CONFUSION?

- **Lack of Knowledge**
  - Small providers still do not have sufficient knowledge of HIPAA privacy at operational level, never mind any other HIPAA rule.
- **Misunderstanding**
  - Covered entities of all sizes misunderstand some provisions of HIPAA.
  - Some misinterpretation is intentional!
- **Differing Interpretations**
  - Covered entities interpret HIPAA differently for many reasons, governance, internal rules, impact of state law.
  - Each covered entity has it's own interpretation based on it's own needs.
- **Old habits are hard to break!**

It's Only Logical ...

1. **Health Reform Expectations for High Quality, Low Cost Healthcare Depend on Meaningful Use of HIT**
2. **Meaningful Use of HIT Depends on HIE**
3. **Functional HIE Trust in the System**
4. **Trust Depends on Consistent and Well Understood Privacy (Confidentiality) Practices**
5. **Trustworthy Privacy Depends on Consistent and Well Implemented Security Practices**
6. **Trustworthy Privacy and Security Practices Depend on Clear Guidance and Consistent Enforcement**

Everything in the Chain of Dependencies Must Work!

Questions?

William R. “Bill” Braithwaite, MD, PhD, FACMI
Chief Medical Officer
Anakam Inc.

BBraithwaite@anakam.com