HIPAA's Role in Health Reform: Enabling Electronic Exchange of Standardized Health Information

William R. "Bill" Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Anakam, an Equifax Company

March 10, 2011

Why Healthcare IT?

- **Avoid medical errors.**
  - Up to 98,000 annual hospital deaths due to avoidable medical errors.
- **Avoid healthcare waste.**
  - Up to $300B spent annually on treatments with no health yield.
  - We spend 2X per capita as any other industrialized nation to attain bottom rank on population health.
- **Accelerate health knowledge diffusion.**
  - Average of 17 years for medical evidence to be integrated into practice.

Why Healthcare IT?

- **Promote public health and preparedness.**
  - Surveillance is fragmented, and untimely.
- **Empower patients in health management.**
  - Patients minimally involved in own health.
- **Strengthen health data protection.**
  - Public fears identity theft and loss of privacy.
- **Streamline access to healthcare delivery.**
  - Manual processes waste time and add frustration.

- **Paper records cannot solve these problems!**

HIPAA started the process

- **HIPAA (Administrative Simplification) focussed on Health Information Exchange (HIE) for administrative purposes.**
  - Standards for secure exchange of computable information.
- **HIPAA set base standards for extension of HIE into exchange of clinical information.**
  - Privacy and Security Rules.
  - Classification and Coding of clinical problems and procedures.
  - Identifiers for patients and providers.

HITECH Updated HIPAA

- **Secretary shall annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the HIPAA security standards.**
- **New federal security breach notification requirements for covered entities, business associates and personal health record providers.**
- **New restrictions on sale of electronic health information and use of health information for marketing and fundraising.**
- **New individual rights to restrict disclosure of health information to health plans and to obtain an accounting of disclosures of health information in electronic health records.**

Extending Trust under HITECH

- **New entities are ‘Business Associates’ and thus are now directly subject to HIPAA Privacy and Security Rules:**
  - Health Information Exchange.
  - Regional Health Information Organization.
  - ePrescribing Gateway.
  - Vendor of personal health record that contracts with a covered entity to allow that covered entity to offer a PHR to patients as part of its EHR.

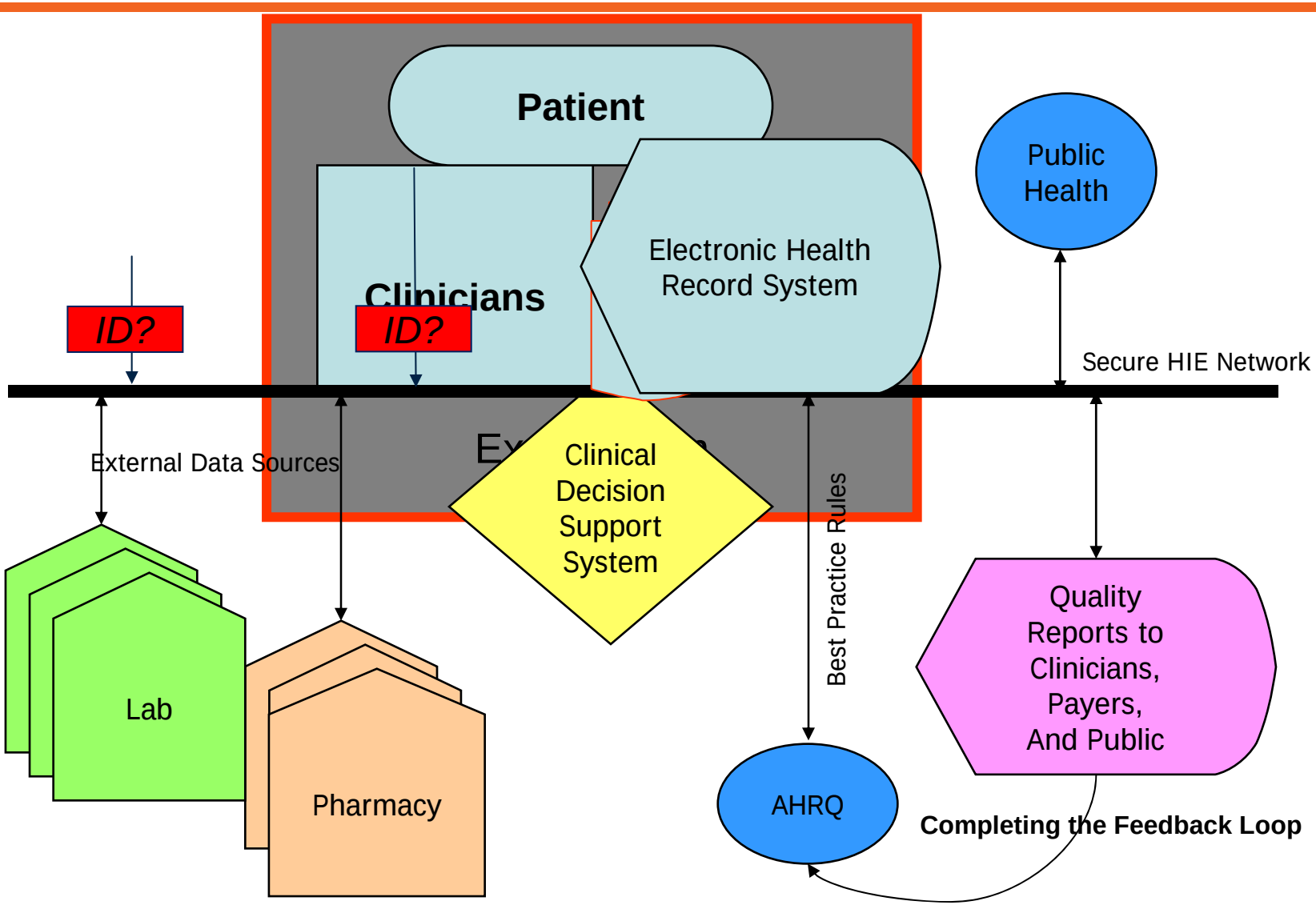
HITECH Improves Enforcement

- **HIPAA Civil and Criminal Penalties shall apply to a business associate in the same manner as they apply to a covered entity.**
- **Secretary shall formally investigate violations that may be due to willful neglect.**
- **Tiered penalties increase up to $50,000 (maximum $1,500,000).**
- **An individual who is harmed by an offense may receive a percentage of any monetary settlement.**
- **The Secretary shall provide for periodic audits.**
- **A State attorney general may bring a civil action in a district court to obtain damages.**

Health Reform – Meaningful Use

- **Goal: High quality, cost-effective healthcare.**
- **Means: Direct interaction with Clinical Decision Support System (CDSS) to enable faster, more informed decisions by providers and patients.**
- **Requires:**
  - Electronic Health Records (EHRs) & secure, interoperable, electronic Exchange of standardized, computable Health Information (HIE).
  - Trust from healthcare patients and providers.

Reform of Healthcare Paradigm toward Meaningful Use



HIE is the Backbone of Reform

- **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, …
- **Interoperable HIE is KEY to Meaningful Use of HIT which, in turn, is KEY to Health Reform!**

The Challenge: A Complete Interoperability Profile

- **Standard Messaging**
  - Format, Structure
  - Terminology, Coding
- **Secure Conveyance**
  - Encryption, Transport
  - Entity Authentication
  - Data Loss Prevention
- **Network Services**
  - Patient locator service
  - Terminology service
  - CDS rule source
  - Cloud Services
- **Privacy Issues**
  - Accurately linking patient records
  - Patient control over access
- **Business issues**
  - Workflow integration
  - Professional resistance
  - Staff Education
  - Risk Assessment
- **"Organizational interoperability"**
  - Policies, contracts and agreements
- **Other mutual security issues (trust)**
  - Strong, secure, User Identification, Authentication, Authorization, Access, and Audit.

Trusted Identity Management

- **Risk Analysis Determines Required Assurance Level of Identity Authentication (as required by HIPAA).**
  - Most clinical environments require frequent, repetitive logons by staff from relatively secure locations where other factors limit access by unknown persons.
    - Username and password are often considered adequate here.
    - If not, the controlled environment is equipped for other factors.
      - ID cards, RFID chips, tokens, fingerprints.
  - Unsecured environments require stronger authentication.
    - Home, hotel, Starbucks, …
    - Cannot use additional hardware or software.
    - Cannot scale expensive portable devices (hard tokens) to consumers.

New Risks for Identity

- **Health information is now a target for identity theft.**
  - HIPAA requires security to be a dynamic program responding constantly to new risks. (It's a process, not a floor, under HIPAA.)
  - Risk of breach increases as amount of information increases.
    - HIE aggregates data and risk from many sources.
    - Financial and reputational risk increased by HITECH.
- **Single factor authentication is inadequate for remote access to information under federal regulations:**
  - CMS guidance and OMB Memoranda.
  - FISMA requirement for all federal information systems.
  - DEA regulation for electronic prescribing of controlled substances.
  - CMS requiring TFA for submission of quality data.
  - HIEs are also adopting strong authentication.
    - CA and NY policy documents a TFA requirement for remote access.

Reliable Identity of Patient

- **No national standard for how to uniquely identify patients.**
  - Despite HIPAA mandate
- **Required for merging records from multiple locations.**
  - Matching probability is not 100%.
- **In-person identity proofing is impractical.**
  - VA currently requires it for MyHealthyVet.gov.
  - Providers don't want the job.
- **Electronic access to medical records.**
  - Internet access to patient portals required to cost-effectively fulfill consumer engagement goal of 'meaningful use' .
- **Electronic recording of consent directives.**
- **Fraud prevention in public programs.**
  - e.g., Medicare and Medicaid.

Reliable Identity of Provider

- **Remote access to patient information (HIPAA).**
  - Access from home.
  - Access from wireless devices.
  - Access from patient home.
- **Access to government held PII.**
  - OMB,FISMA, NIST.
- **Submission of quality information.**
  - Pay for performance programs.
  - Meaningful Use incentive programs (CMS).
- **Electronic prescribing.**
  - DEA IFR

Trust Holds It All Together

- **Loss of perceived control of PHI**
  - Provider not in charge.
- **Access to large amounts of PHI accumulated by HIE.**
  - Increased risk (real and perceived).
- **Providers must trust the HIE system**
  - Lack of trust => no information exchange.
- **Patients must trust the HIE system**
  - Lack of trust => no permission to disclose health records.
- **HIE will fail without trusted access to PHI, Meaningful Use will falter without HIE, Health Reform will stall without MU.**
- **<u>Trust</u> depends on believable privacy and security mechanisms and a clean track record …**

Believable Security Requires High Levels of Identity Assurance

- **High level of assurance that the person who is sending information is who say they are.**
  - Non-repudiation.
- **High level of assurance that the person who is receiving information is who we think they are.**
  - Mechanisms to prevent information from being changed or viewed by anyone else.
- **High level of assurance that the patient identified in the information is who we think they are.**
  - Patient identification accuracy.
- **These mechanisms are dependent on strong, reliable identity proofing and authentication.**
  - NIST defines requirements for high assurance at Level 3 or 4.

Types of Authentication

- **There are three major types of authentication used to identify a person attempting to login:**
  - "Something the user knows" (e.g., username and password) is the most common and weakest authentication factor;
  - "Something the user has" (e.g., ID card, security token or phone) is the most used second factor; and
  - "Something the user is or does" (e.g., fingerprint or retinal pattern, voice recognition, or other biometric) is a very strong third factor.
- **A static password alone is not adequate to prevent fraudulent or unauthorized access to sensitive information unless other protections are in place.**
- **Two-factor authentication (using two different types of authentication), provides a higher level of security and assurance than a single factor.**

It's Only Logical ...

1. **Health Reform Expectations Depend on Meaningful Use of HIT.**
2. **Meaningful Use Depends on Functional HIE.**
3. **Functional HIE Depends on Trust in the System.**
4. **Trust Depends on Believable, Consistent and Well Implemented Security Practices.**
5. **Believable Security Depends on High Assurance of Electronic Identities for Patients and Providers.**
6. **Flexible, cost-effective means for High Assurance of Electronic Identities are now commercially available.**

Everything in the Chain of Dependencies Must Work!

Identity Management is Key

NIST and OCR hosted conference on this topic:

Safeguarding Health Information: Building Assurance through HIPAA Security

May 10 & 11, 2011

Ronald Regan Center, Washington, D.C.

Bill Braithwaite
Chief Medical Officer
Anakam, an Equifax Company

BBraithwaite@anakam.com