HIPAA Summit XX

Afternoon Plenary – Welcome!
HIPAA, HITECH and Reform

William R. “Bill” Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Equifax – Anakam Identity Services

March 27, 2012

Agenda 1

- 1:15 p.m. Welcome & Introductions: Overview
  - Bill Braithwaite, MD, PhD (Co-Chair)
- 1:45 p.m. ONC Privacy and Security Policy Update
  - Joy Pritts, Esq.
- 2:15 p.m. Privacy and Security Tiger Team
  - Deven McGraw, Esq.
- 2:45 p.m. Networking Break
  - Exhibit Hall

Agenda 2

- 3:15 p.m. HIPAA and Health Information Exchanges
  - Helen Oscislawski, Esq.
- 3:45 p.m. HIPAA and Payment and Delivery System Reform
  - Mark S. Hedberg, Esq.
- 4:15 p.m. HIPAA and Cloud Computing
  - Howard Burde, Esq.
- 4:45 p.m. Mobile Messaging HIPAA –Compliant Texting Streamlining and Accelerating Communication
  - Panel of Harshul Patel, MD; Belinda Setters; and Greg Young
  - Brad Brooks (moderator)
- 5:15 p.m. Adjournment and Networking Reception
  - Exhibit Hall

The Big Picture on Privacy & Security in Healthcare: Key Role of Identity Management

William R. "Bill" Braithwaite, MD, PhD, FACMI, FHL7
Chief Medical Officer
Equifax – Anakam Identity Services

March 29, 2012

Healthcare Reform: HIT at Nexus of Transformation

- Healthcare Information Technology (HIT) brings more healthcare processes online, enabling:
  - Provider Empowerment: Higher quality, more cost-effective healthcare through support of clinical decisions with more information at the point of care coupled with empowering healthcare processes (e.g. ePrescribing)
  - Patient Empowerment: Broad-based individual access to online health information systems (e.g. enabling consent online).
  - System Empowerment: Improved overall service delivery due to consistency and transparency of healthcare information
- BUT reducing costs and bringing higher efficiencies through HIT requires secure access to information to allay privacy concerns.
  - Risk of fraud and medical identity theft increases as more sensitive health information is available online
  - Unauthorized access to healthcare information creates an environment of “fear, uncertainty, and doubt” - healthcare data is not fungible
  - Without proper protection users have no trust; without trust there is no adoption; without adoption the benefits of HIT are negligible

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 confidentiality, integrity, and availability of information through
  - physical, technical, and administrative safeguards

Why Privacy is Important…

- Privacy is important to consumers.
  - As a fundamental component of high-quality, patient-centered healthcare.
- When individuals worry about misuse of their personal health information, they take steps to circumvent the system to protect their privacy.
  - e.g., they refuse to share their information.

Source: California HealthCare Foundation and Consumers Union. *Promoting Health, Protecting Privacy: A Primer.* Oakland, Calif: California HealthCare Foundation and Consumers Union; January 1999.

HIPAA Privacy Rule of Thumb

- Don’t surprise the patient with a use or disclosure they don’t expect!
  - Tell the patient about uses and disclosures necessarily part of normal operations of the healthcare enterprise (TPO).
  - Give the patient the opportunity to object to limited disclosures in common practice.
    - e.g., name in hospital directory.
  - Follow required procedures for public policy exceptions.
    - e.g., required reporting of contagious disease.
  - 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

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.

Different Approaches to Privacy & Security

- Privacy Rule based on application of simple, stable principles to a complex environment.
  - Regulations more detailed because change is slow.
  - Compliance comfort demands specificity.
  - Intensely personal topic; demand for changes is strong.
- Security Rule based on application of general principles to rapidly changing environment.
  - Highly technical threats and potential protections change very rapidly.
  - Regulations could never be modified quickly enough to respond to needs.
  - Guidance can be used to address specifics without rule changes.
    - E.g., methods and circumstances requiring encryption

Key Security Rule Philosophy

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

Security Process 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 …

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.
- Health information is now a target for identity theft.
  - Security must be a dynamic program responding constantly to new risks.

- Challenges:
  - Risk of breach increases as amount of information increases.
    - HIE aggregates data and risk from many sources.
  - Managing new risks, controlling costs, minimizing disruption to habitual workflows, minimizing user time and hassle, meaningful training, …

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.
- Security is dynamic.
  - Security must include processes of risk assessment and management, repeated regularly, forever.
  - With appropriate risk assessment and management, security mechanisms can cover new risks without needing to change the rules.

Backbone of Trust Elements

- Identity Management
  - You can’t trust information exchange unless you truly know who is sending the information, who is receiving the information, and to whom the information refers.
- Risk Analysis determines the level of identity authentication required
  - 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 allows other factors to be used.
      - 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 (tokens) to consumers.

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.

Linking Patient Records

- Variability in methods across organizations to link patients to records, and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational electronic HIE is conducted.
- Concern about liability for incidental or inappropriate disclosures causes many to take a conservative approach.
- Clinicians believe it is ‘safer’ to make do with less information on a patient where there is any question about identity, rather than to potentially base clinical decisions on information from the wrong patient.
- The challenge is to reach agreement on how to preserve confidentiality while accurately linking patient records from different sources without a national patient identifier.

Reliable Identity of Provider

- Remote access to patient information (HIPAA).
  - Access from doctor’s home.
  - Access from patient’s home.
  - Access from wireless devices anywhere.
- Access to government held PII.
  - OMB,FISMA, NIST.
- Submission of quality information.
  - Pay for performance programs.
  - Meaningful Use incentive programs (CMS).
- Electronic prescribing.
  - DEA Interim Final Rule for controlled substances.
- Fraud prevention in public programs.
  - e.g., Medicare and Medicaid.

New Risks for Identity

- Health information is now a target for identity theft.
  - Risk of breach increases as amount of information increases.
    - Health Information sharing aggregates data and risk from many sources.
    - Institutional financial and reputational risk increased along with patient risk.
- Single factor authentication is inadequate for remote access to information under federal regulations:
  - US federal law and regulation and guidance in specific areas.
  - State health information exchange organizations are also adopting strong authentication requirements.
    - E.g., CA and NY policy documents a two factor authentication requirement for remote access.

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 technologies.
  - Identity proofing.
  - Authentication.

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.

Privacy and Security Reflections from Dr. HIPAA

- Design Privacy and Security into the Health IT System.
  - Build it right into the infrastructure, don’t try to tack it on afterwards.
- Find and Manage Risk in Reasonable and Appropriate ways.
  - Earthquake Preparations in San Francisco vs DC?
- People are Fallible – so is any System built by People.
  - Design for Failure.
- People are Creative – and can always find a way around any control.
  - Trust, but Verify – Analyze those Audit Trails!
- Educate; Don’t just Train.
  - People follow intent of instruction better when they understand why!
- Use Common Sense – Think First, Learn from Others.
  - Encrypt all portable media, but don’t set the password complexity and refresh requirements so high that people must write their passwords down and carry them in the same bag as the device.

Conclusion

- Transformation to higher quality, cost-effective healthcare is dependent on wide deployment of interconnected health IT.
- High assurance identity management services are critical to the success of health IT deployment and acceptance.

William R. “Bill” Braithwaite, MD, PhD, FACMI
Chief Medical Officer
Anakam Identity Services
Bill.Braithwaite at Equifax.com