HIPAA for HIT and EHRs

Latest on Meaningful Use and EHR Certification: For Privacy and Security Professionals

Donald Bechtel, CHP
Siemens Health Services
Patient Privacy Officer

Fair Information Practices

- Fair Information Practices (FIP) as a Privacy Framework
  - Code of Fair Information Practices was first developed in the early 1970s by Department Health, Education, and Welfare, now known as Department of Health and Human Services (DHHS)
- HIPAA Privacy Rules were built on the foundation of FIP
- Meaningful Use requires that EP and EH must comply with HIPAA privacy and security requirements
- ONC Adopted the FIP for the Nationwide Health Information Network
- HIT Policy Committee recommends FIP - to build public trust and participation in health information technology and electronic health information exchange.
  - Individual Access
  - Correction
  - Openness and Transparency
  - Individual Choice or *Right to Informed Consent*
  - Collection, Use, and Disclosure Limitation
  - Data Quality and Integrity
  - *Security* Safeguards
  - Accountability
  - *Availability*

ONC's EHR Standards, Implementation Specifications, and Certification Criteria Final Rule versus HIPAA

- Identified nine privacy and security criteria for a certified EHR System
  - 170.302(o) Access Controls - Unique User ID and Tracking
  - 170.302(p) Emergency Access
  - 170.302(q) Automatic Log-off
  - 170.302(r) Audit Log (stronger than HIPAA specific content)
  - 170.302(s) Integrity (stronger than HIPAA requires hashing standard)
  - 170.302(t) Authentication
  - 170.302(u) General Encryption (stronger than HIPAA required method)
  - 170.302(v) Encryption when Exchanging eHI (stronger than HIPAA required)
  - 170.302(w) Accounting of Disclosures (Optional for Stage 1)
- These also tie very well with HIPAA Security Safeguards
- New NIST test scripts version 1.1 were recently issued

Protect Electronic Health Information
Access Controls vs Data Controls

- Access Controls, User ID and Passwords (authentication of user)
  - Policies and procedures to assign and remove user IDs
    - Termination procedures executed immediately
  - Policies and procedures for strong password requirements
  - Policies and procedures to designate and maintain user authorizations
  - Optionally support for tokens or “smart cards”
  - User authentications procedures through global logon to authorized apps
  - Network access controls – Firewalls, routers, etc.
  - Environmental security controls
  - Restricted access to users and applications
  - Vendor’s application in-depth security controls
- Data at Rest – restricted access controls
  - Optionally encryption based on risk assessments
- Data in transit – must be encrypted, including private point-to-point lines
- Audit logs – capture and report information, detection and alerts

Connectivity

- User and System Authentication (trusted trading partners)
  - Cross enterprise access controls
- Individual identification remains a key concern
- Trading Partner Agreements or other contracts between organizations
  - Should help to spell out controls for interconnectivity and authentication
  - HISPs, HIOs (a.k.a. HIEs) RHIOs, etc will need to develop these agreements and define the methods that they will support.
  - As with HIPAA today, ensure that all entities are protecting data equally, and are only using and disclosing health information as permitted
    - With the new HITECH rules it is now clear that Business Associations when in possession of PHI must protect it with the same safeguards as a Covered Entity.
- Sending encrypted email and documents has challenges
- NHIN and NHIN Direct are working on these issues

Sharing documents (individually identifiable health information)

- What information should be sent for minimum necessary
  - OCR to issue Guidelines (still pending)
  - Should rely on standards like HL7 and CDA Templates and others where available
    - Medication list, Allergy List, Vital Signs, Lab Results, Submission to Immunization Registries, Public Health Surveillance
- Ensure that the information is protected when sent (encrypted)
- Will patient consent be required for Stage I documents?
  - Currently, under HIPAA guidelines the above reports should not require consent, when sent in the context of treatment, payment, or healthcare operations
  - More guidance on consent may come from the HIT Policy Committee
- We must know the entity requesting data and be able to authenticate them

Role of the Provider

- Implement the necessary policies and procedures to maintain an EHR system
- EHR systems provide the tools to preserve data privacy and security, but they won’t work without the provider’s policies and procedures to enable them.
- For things like:
  - Access controls
  - Authorizations
  - Identity management
  - Patient consent management
  - And so on

Questions?