Security Considerations for Health Information Exchanges

Corey Wilson, CHPC, CCISO
Mark Burnette, CPA, CISA, CISSP, CISM, CRISC, QSA

Today’s Discussion

- What is an HIE?
- Why is an HIE important?
- Security considerations for HIE’s
- Other considerations for HIE’s
What is an HIE?

The term "health information exchange" (HIE) actually encompasses two related concepts:

- **Verb**: The electronic sharing of health-related information among organizations
- **Noun**: An organization that provides services to enable the electronic sharing of health-related information

HIEs are generally not covered entities, but are considered to be Business Associates of HIPAA covered entities

- Both federal and state laws and regulations apply to HIE activities
What is an HIE?

- Types of data exchanged via an HIE:
  - Care summaries
  - ED and Inpatient episode/discharge summaries
  - Inpatient diagnosis and procedures
  - Outpatient visit summaries
  - Medication data
  - Laboratory or radiology orders and results
  - Continuity of Care Document or Care Coordination Document
  - Immunization information
  - Dictation/transcription
  - Enrollment/eligibility verification
  - Claims data

Why is an HIE Important?

- Supports the goals of HITECH Act to improve patient care and make it patient-centric through the creation of a secure, interoperable nationwide health information network.

- Facilitates and enables secure vendor-to-vendor, provider-to-provider, and provider-to-patient exchanges of data in line with the objectives for Meaningful Use Stage 2, which starts in 2014.
Why is an HIE Important? (con’t)

- HIE benefits include:
  - Reduction of duplication and operational costs
  - Improvement of quality and health outcomes
  - Improvement of public health surveillance
  - Strengthening of links between health-related research and actual practice
  - Availability of information where and when it is needed (at point of care)

There are more than 160 HIEs in the US
- Very few multi-state HIEs
- Nearly $550M in grants have been awarded through the State Health Information Exchange Cooperative Agreement Program
- Groups involved in building HIEs
  - State-led HIE efforts
  - State-sponsored public/private partnerships
  - Community-sponsored private initiatives
  - Hospital system-wide projects
  - Payers*

Security Considerations for HIE’s

Security and Privacy Challenges for HIE’s

- Safeguard the most sensitive patient data (HIV, mental health and substance abuse treatment)
- Differing patient consent models adds complexity
- Navigating a patchwork of state privacy laws when accommodating non-targeted inquiries
- Segregate patients’ self-pay treatment data in compliance with the HIPAA Omnibus Rule
Security Considerations for HIE’s

- Security of HIE data store
  - Likely to be a target since all data is in one place
  - Encryption of data in storage and transit
  - Annual independent assessment (SOC 1/2) to provide assurance to participants and patients

- Written security policies
  - Policies provided needed governance and structure
  - Adoption of and adherence to policies by participants

- Access controls
  - Federation versus unique user accounts
  - Onboarding/transfers/termination notifications

- Security monitoring and reporting
  - Monitor and control who/what/when/why

Other Considerations for HIE’s

- Technical challenges
  - Interoperability between participants
    - No single “standard” for HIE data exchange
    - Need a secure medium in a “standard” format
  - Many providers may not have an EMR system with a compatible interface
    - Additional development required (security considerations)
  - Connectivity to HIE (rural areas)

- Competitive intelligence
  - Large providers may be hesitant to participate to preserve competitive differentiators in certain markets
  - “What’s in it for me?” – Cost vs. Value

- Cost/benefit
  - Data contribution AND consumption
Other Considerations for HIE’s (con’t)

- Liability Concerns Shared Among Participants
  - Data storage and management
  - Data accuracy and completeness
  - Decisions made with inaccurate data
  - Duty to review
  - Reproducibility of data available in the HIE at particular moment in time
  - Availability of audit/access logs

- Governance of HIE
  - Who holds the HIE accountable for achieving objectives and delivering value to the patient care process and how is that measured?

Breach Notification Considerations

- Responsibility and Liability should be clearly defined
  - Contract/membership terms and conditions
  - Data ownership delineation
  - What data is allowed to be submitted by members?
  - “What happens if data in the HIE is breached?”

- State laws differ on incident handling requirements

- Impact of a breach on the HIE’s future
Summary

- HIE’s are still in the early stages of development
  - Success not guaranteed
- Success Factors for long-term viability of HIE model:
  - Establish interoperability
  - Build public trust
  - Assure stakeholder cooperation
  - Develop financial sustainability
- Security considerations that must be addressed:
  - Data ownership
  - Data protection in storage and transit
  - Security and Operational Policies
  - Access controls and security monitoring
  - Liability/contractual terms
  - Breach notification specifications