Ongoing Challenges in Electronic Health Information Exchange

James Black, MSCIS
Patricia A. Markus, J.D.

North Carolina Healthcare Information and Communications Alliance
AMC Privacy and Security Conference
Chapel Hill, NC
June 23, 2015
Overview

• HIE Challenges to Date

• Ongoing Challenges
  – Governance & Financial Sustainability
  – Participation (Data Use) Agreements
  – Privacy and Security/Data Use Issues
  – “Sensitive” or Restricted Information
  – Connecting with Other HIOs
Challenges to Date: Nomenclature

• Is HIE a noun, a verb, or both?
  – We will use “HIO” for the noun form (health information exchange organization)

• Nationwide Health Information Network
  – NHIN → NwHIN → NwHIN Exchange → eHealth Exchange (eHEX)

• NHIN defined as “network of networks”
• eHEX defined as “set of standards, services, and policies that enable secure HIE over the Internet”
Challenges to Date: Infrastructure

• Statewide HIO infrastructure financed by ARRA

• ONC created Direct in 2010 when it realized small, rural providers unlikely to adopt expensive interoperable EHRs soon
eHEX and HIE in 2015

- eHealth Exchange has 89 Participants in production and over 100 million patient records
- Instead of “network of networks” focus, more local exchanges built upon in-demand services
- Private networks thriving, whereas some statewide HIOs, which are required to cater to all comers, are unable to find niche/value proposition
Ongoing Challenges - Governance

Office of National Coordinator for Health IT

- “Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information”

Office for Civil Rights

- Fact sheets clarify how HIPAA privacy rule may be used in structuring policies for electronic health information exchange.

These two initiatives seek to establish specific principles for the purpose of health information exchange.
## Fair Information Practice Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual Access</td>
<td>Provide individuals access to their PHI in a timely manner including provision of access, denial of access, and documentation.</td>
</tr>
<tr>
<td>Correction</td>
<td>Provide patient means to dispute accuracy or integrity of their PHI.</td>
</tr>
<tr>
<td>Openness and Transparency</td>
<td>Ensure policies, procedures, and technologies that impact individuals or their data open and transparent</td>
</tr>
<tr>
<td>Individual Choice</td>
<td>Provide patients with opportunity to make informed consent of identifiable health information exchange.</td>
</tr>
<tr>
<td>Collection, Use, and Disclosure Limitation</td>
<td>PHI should only be collected, used, or disclosed to the extent necessary to fulfill specified purpose “minimum necessary”.</td>
</tr>
<tr>
<td>Safeguards</td>
<td>Identifiable health information should be protected with reasonable administrative, technical and physical safeguards.</td>
</tr>
</tbody>
</table>
Governance - Subject Matter Experts (SME)

• Basis of Advisory Committee
  – Privacy
  – Security
  – Health Information Management (HIM)
  – Information Technology
  – Compliance
  – Legal Counsel
Governance - Collaborative Relationships

• Clinical & Administrative
  – Care Coordination
  – Policy & Procedure

• Exchange/Trading Partners
  – Technical Capabilities
  – Purpose of Exchange
  – Accountability
## Governance – Policies & Procedures

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance Board</td>
<td>• Charter&lt;br&gt;• Mission, vision and values&lt;br&gt;• Membership&lt;br&gt;• Roles and responsibilities&lt;br&gt;• Type of exchange model&lt;br&gt;• BA provisions&lt;br&gt;• Data ownership</td>
</tr>
<tr>
<td>Sanctions</td>
<td>• Consistent application regardless of user role&lt;br&gt;• Reconcile varying breach sanctions at different institutions&lt;br&gt;• Dissatisfaction of dispute resolution</td>
</tr>
</tbody>
</table>
Ongoing Challenges - Financial Sustainability

• Participants will only pay for value
  – Public utility model versus enterprise model
• Can certain providers pay for others’ technology?
• Phased-in services approach
• Subscription fees/tech sublicenses/sale of de-ID’d data
Ongoing Challenges – Participation (Data Use) Agreements

• Multi-party agreements intended to be scalable so that hundreds or thousands may agree to terms without individual negotiation

• Numerous types of participants, purposes

• Connecting requires trust and streamlining Participation Agreements to create common requirements (incl. flow-down responsibilities)

• Permitted access to/use of data

• Participant and HIO requirements
Ongoing Challenges – Participation (Data Use) Agreements (cont’d)

• Participant requirements:
  – maintain privacy and security
  – have policies and procedures
  – provide education and training for authorized users

• HIO requirements:
  – maintain privacy and security
  – audit and monitor
  – coordinate opt-in or opt-out
  – maintain infrastructure
  – handle disputes
Ongoing Challenges – Participation (Data Use) Agreements (cont’d)

• “Participants” can range from only health care providers to include public health, government agencies, payors, and individuals

• “Message Content” or “Patient Information”: what types of info may be exchanged? Sensitive info? Substance abuse info? CCRs? Clinical notes?

• “Permitted Purpose” for exchange: most permit for treatment, public health, and as required by law; others permit for payment and some operations; NC permits for all of these plus research
Ongoing Challenges – Participation (Data Use) Agreements (cont’d)

• Use of/Access to Data:
  – permitted uses and disclosures of PHI
  – who is an authorized user and how authorized users are granted access and have access restricted
  – terms of data access, including availability of data
  – ownership of data and future uses of data
Ongoing Challenges – Participation (Data Use) Agreements (cont’d)

• Privacy and security safeguards
• Term, termination, and suspension
• Disposition of data after termination
• Warranties/limitations of liability
• Insurance/indemnity (against other participants and HIO)
• Breach notification
• Amendment
Ongoing Challenges - DURSA

• (Restatement I to the) Data Use and Reciprocal Support Agreement (“DURSA”)
  – Each Participant complies with “Applicable Law”
  – Participants can request information only for Permitted Purposes
  – Incorporates by reference technical standards and operating policies and procedures
Ongoing Challenges - DURSA (cont’d)

• Participants that request data for treatment purposes also must respond to requests for treatment purposes; may respond to other requests

• No indemnity; each Participant responsible for own acts/omissions

• Mandatory multi-step dispute resolution process
Ongoing Challenges - DURSA (cont’d)

• DURSA Privacy and Security Requirements
  – Participants must maintain, use, and redisclose data in compliance with Applicable Law and record retention policies
  – Participants maintain and have end users comply with their own access and disclosure policies
  – Participants must validate user applicants, authenticate users, and either contract with users or require users to abide by policies requiring compliance with DURSA requirements
Ongoing Challenges – DURSA (cont’d)

• DURSA Privacy and Security Requirements
  – Participants must comply with HIPAA
  – Participants must protect data from malware
  – Participants must audit access and use and discipline those who violate privacy and security requirements
  – Breach notification: Participants must notify the Coordinating Committee within one hour after discovering potential breach, 24 hours after confirmed breach
# Privacy & Security - Policies & Procedures

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
</table>
| Access Control                | • Who requires access?  
  – Existing P&P  
  – Role Based  
• Access Audit Considerations  
• Access Functionality        |
| Accounting of Disclosures     | • HIPAA’s Requirements  
  – Upon request  
  – Account for disclosures even for TPO  
• ARRA’s Requirements  
  – Must account for disclosures of business associates  
• Processes for accounting of disclosures and who manages request  
• Report Format and Time Frames |
## Privacy & Security - Policies & Procedures (cont’d)

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Education</td>
<td>• Trust in electronic health information exchange</td>
</tr>
<tr>
<td></td>
<td>– Quality of Care Benefits</td>
</tr>
<tr>
<td></td>
<td>– Faster and more reliable</td>
</tr>
<tr>
<td></td>
<td>– Helps control costs</td>
</tr>
<tr>
<td></td>
<td>– Notice of Privacy Practices</td>
</tr>
<tr>
<td>Data Integrity and Quality</td>
<td>• P&amp;P ensure high integrity &amp; quality of data.</td>
</tr>
<tr>
<td></td>
<td>• Data standards between entities</td>
</tr>
<tr>
<td></td>
<td>• Management of data processes</td>
</tr>
<tr>
<td></td>
<td>• Data Omissions</td>
</tr>
<tr>
<td></td>
<td>• Accountability</td>
</tr>
<tr>
<td></td>
<td>• Use existing data standards when possible</td>
</tr>
<tr>
<td></td>
<td>• Data is used for patient care decisions</td>
</tr>
</tbody>
</table>
## Consideration Policy/Procedure

### Data Loss Protection
- Policy should incorporate HIPAA administrative, physical and technical safeguards
- Security awareness and training
- Contingency planning (data backup & downtime)
- Technical standards
- Designate Responsibility
- Recognize all access and removal points

### Data Retention
- Define requirements
- Pass through or stored
- Types of information being stored
- Purpose of information being stored
- Archiving, purging, and destruction
## Privacy & Security - Policies & Procedures (cont’d)

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
</table>
| Identity Management/                  | • Patient identification capabilities  
| Patient Correlation                    | • Correct patient identification  
|                                        | • Does identification process disclose patient data?  
|                                        | • Query process  
|                                        | • Traits to be used  
|                                        | • Detecting medical identity theft  
|                                        | • Resources, staffing, and responsibilities for managing manual interventions                                                                                                                                 |
| Record Amendments                      | • Privacy Rule  
|                                        | • ONC’s Correction principle  
|                                        | • Management of Amendment Requests: who accepts requests and from whom, approves or denies request  
|                                        | • Management of Amendment: Retention of original entry, retrieved on demand, and linked to amendment request                                                                                                  |
Ongoing Challenges - What’s a Breach

• In an HIO?
  – Like health systems, HIEs are comprised of multiple—
    but often unrelated—entities
  – Improper uses and disclosures in HIE should be
    treated like those between covered entities
  – Don’t confuse HIE contractual breach notification
    requirements with HIPAA requirements

• Purpose of HIE requirement is to permit affected entities to
  decide whether to suspend participation in HIE temporarily
## Breach & Consent - Policies & Procedures

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
</table>
| Breach Notifications                 | • Responsibilities for breach notification  
|                                      |   – Notification process  
|                                      |     o Who is notified?  
|                                      |     o Who notifies?  
|                                      |     o How do they notify?  
|                                      |     o Entity Roles  |
| Consent/Authorization Process        | • Opt In / Opt Out  
|                                      | • Education  
|                                      | • Centralized, Federated, & Hybrid  
|                                      | • New or existing forms  
|                                      | • Storing Forms  
|                                      | • “Break the glass” (Emergency Exception)  
|                                      | • Managing revocation of prior decisions |
Ongoing Challenges - Patient Opt-Out

• Not addressed in DURSA

• North Carolina HIE enabling legislation permits opt-out

• Opt-out can be exercised at provider level; opt-out can be rescinded

• Emergency providers can “break the glass”

• Providers can’t deny treatment to individual based upon individual’s decision to opt-out

• Providers want the HIO to educate consumers and administer the opt-out process
Ongoing Challenges - “Sensitive” or Restricted Information

• Disclosure by federally assisted substance abuse treatment centers - subject to stringent patient consent requirements (42 CFR Part 2)

• Limited exceptions – disclosures to:
  – Law enforcement if immediate threat to health or safety exists
  – Providers for emergency treatment
  – Under a Qualified Service Organization Agreement
Ongoing Challenges - “Sensitive” or Restricted Information (cont’d)

• Difficult to satisfy specific consent requirements when using electronic systems:
  – Specific person who receive data
  – How much and what kind of data to be disclosed
  – Purpose of disclosure
  – When consent will expire (must insure that consent lasts no longer than reasonably necessary for purpose stated)
Ongoing Challenges - “Sensitive” or Restricted Information (cont’d)

• 42 CFR Part 2 and similar state laws:
  – Make it almost impossible for information from treatment centers to share data through HIOs
  – EHRs not granular enough to limit disclosures of certain data to specified people for time period specified in consent
Ongoing Challenges - “Sensitive” or Restricted Information (cont’d)

• Treatment information of minors
  – Minors typically can consent to certain health services and therefore must permit parents to access info about those services
  – How do providers address this with patient portals and in HIOs?
Ongoing Challenges - “Sensitive” or Restricted Information (cont’d)

• NC law on release of certain “sensitive” info was amended in 2011 to align with HIPAA

• Now:

  – Info maintained by DHHS and local health departments, HIV/AIDS information can be released for TPO and research

  – Mental health info may be exchanged between “facilities” for TP and some O, but release to non-facility requires opportunity for patient to object

  – Mental health information received by non-facility may use/disclose the info as permitted by HIPAA
“Sensitive” or Restricted Information - Policies & Procedures

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Policy/Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limitations of Technology</td>
</tr>
<tr>
<td></td>
<td>– Age &amp; impact to who controls privacy of medical record</td>
</tr>
<tr>
<td></td>
<td>– Emancipation</td>
</tr>
<tr>
<td></td>
<td>– Patient portals</td>
</tr>
<tr>
<td></td>
<td>• State versus federal</td>
</tr>
<tr>
<td></td>
<td>• Resides in one state but receives care in another</td>
</tr>
<tr>
<td></td>
<td>• Additional authorization</td>
</tr>
<tr>
<td></td>
<td>• Lack of consistency</td>
</tr>
</tbody>
</table>
Ongoing Challenges – Connecting HIOs

• Connections between HIOs
  – Connecting requires trust and streamlining Participation Agreements to create common requirements (incl. flow-down responsibilities)
  – Consent model and HIO model
  – Does each HIO have similar technology (e.g., CCD, master patient index)?
Upcoming Opportunities

- Better treatments and better care
- Streamline costs
- Provider and consumer demand for data
- HIE 2.0
  - HIE 1.0 tried to be all things to all people, numerous use cases, top-down approach
  - HIE 2.0 more decentralized, consumer-focused, led by consumer demand, organic growth
Questions??

James Black, MSCIS
jblack@vidanthealth.com

Patricia A. Markus, J.D.
trish.markus@smithmoorelaw.com