Health Data Exchange Interoperability: Opportunities for Cross-Initiative Learning and Optimizing Infrastructure Investments

August 22, 2016

Raja Kailar, Founder & CEO
Overview

Thesis
- Many specifications for health data transport and security are in use or emerging
- Transport and security requirements are common or similar, hence standards can be payload agnostic
- Common design patterns and approaches to transport and security standards across public-health, clinical, administrative domains can help improve reuse, ROI
- No single transport and security standard meets all functional needs across these sub-domains, hence a “catalog” approach may be necessary based on functional, security and scalability needs
- Successful patterns and lessons learned from initiatives are useful and can be applied across initiatives to improve effectiveness
- Reuse of infrastructure components across data exchange implementations can help optimize investments

Session Outline
- Review Major Health-IT Data Exchange and Interoperability Initiatives with a focus on Transport and Security
- Identify Successful Patterns and Lessons Learned and their Potential Application to New Data Exchanges
- Identify Opportunities for Reusable Common Infrastructure Components to Optimize Investments

Intended Audience
- Healthcare IT (Public health, Clinical and Administrative) Interoperability and Security Regulation, Policy, Standards and Architecture and Implementation leads
Discussion Scope

In Scope

– B2B Transport and Security
– Standards, Specifications, Policies and Regulations
– Public Health, Clinical and Administrative domains

Out of Scope

– Data Content standards (e.g., HL7v2 vs v3, CDA)
– Semantic and process level interoperability
– Architecture comparisons (e.g., SOA vs API/Micro-Services)
– Device level Interoperability & Security
– IoT, Mobile and Cloud Technologies
– Legal and Trust frameworks
– Adoption Level Statistics, Return on Investment (ROI) Analysis
– Drivers for adoption: Voluntary vs Program requirement vs Regulatory mandates
Review of Recent Major Interoperability Initiatives on Health Data Transport and Security
Public Health – CDC

Transport Standards in Use or Emerging:
ebXML (PHINMS), SOAP, SMTP+SMIME (Direct), REST/Micro-Services (MTS)
## Public Health: Transport and Security Specifications

<table>
<thead>
<tr>
<th>Specification/Profile</th>
<th>Primary Use</th>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| **PHIN MS**           | • Mostly “push” notification use cases  
                         • Multiple CDC programs  
                         • MU-2 (Syndromic Surveillance Reporting, Lab Reporting) | • Loose coupling between transport and data content  
                         • Strong security (transport and data content)  
                         • Strong reliability (guaranteed delivery)  
                         • Large install base | • Based on ebXML, which is not in widespread use  
                         • No Normative XSD/WSDL  
                         • Complexity despite availability of free reference implementation  
                         • On-boarding/security infrastructure is CDC centric |
| **ONC Direct**        | National Health Safety Network (NHSN) | • Handles “push” well  
                         • DirectTrust/NATE and HISP infrastructure simplifies provider on-boarding, security, scales well to a national network | “Pull” and “publish-subscribe” are not well supported |
| **SOAP / Web-Services** | EHR-Immunization Information Systems Interoperability project (Expert Panel recommends SOAP after evaluating ebXML, SMTP+SMIME, SFTP, HTTPS POST/REST and SOAP) | • SOAP is well understood  
                         • Normative XSD/WSDLs  
                         • WS-Security and SAML for envelope level authentication / authorization  
                         • Good tooling support in most languages | Maybe considered heavy for public facing API use cases (e.g., mobile apps) |
| **Micro-services (RESTful approach, similar to HL7 FHIR)** | • Surveillance Data Platform (SDP)  
                         • PHIN MS Next-Gen (MTS)  
                         • Vocabulary access (VADS) | • Lightweight, easy to develop  
                         • Based on HTTP transport, well understood  
                         • Significant industry activity  
                         • Pilot projects underway: Argonaut, CommonWell (common services) | • Draft (DSTU), evolving, will take time to stabilize  
                         • Currently not designed for mediated exchange (e.g., no message envelope, payload level security specified) |
Clinical Focus: Nationwide Health Information Network / HealtheWay / eHealthExchange / Sequoia

Transport Approaches in Use or Emerging:
SOAP, SMTP+SMIME (Direct), REST/Micro-Services
## Clinical Data Exchange Specifications and their Characteristics

<table>
<thead>
<tr>
<th>Specification/Profile</th>
<th>Primary Use / Regulatory Adoption</th>
<th>Underlying standards</th>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| eHealthExchange / NwHIN / HealtheWay | EHRs – Interactions with HIEs, Federal government (MU-2) | IHE XDR (SOAP over HTTP/S) | • Mature specifications  
• Strong security including transport and payload  
• Reference implementation (CONNECT)  
• Legal/trust framework (DURSA)  
• HIE infrastructure, scales to a national network  
• Technical / operational support (Sequoia Project) | High Technical Complexity despite reference implementation (CONNECT). Suitable for inter-agency exchanges. |
| ONC Direct | EHRs – transitions of care (MU-2) | SMIME, XDM | • Handles “push” well  
• DirectTrust/NATE and HISP infrastructure simplifies provider on-boarding, security, scales well to a national network | “Pull” and “publish-subscribe” are not well supported |
| RESTful APIs (e.g., HL7 FHIR) | Public facing APIs from EHRs (MU-3 has API requirements for VDT but does not require FHIR) | HTTP/S REST, XML/JSON | • Lightweight, easy to develop  
• Based on HTTP transport, well understood  
• Significant industry support  
• Pilot projects underway: Argonaut, CommonWell (common services) | • Draft (DSTU), evolving, will take time to stabilize  
• Currently not designed for mediated exchange (e.g., no message envelope, payload level security specified) |

Legacy Standards in use: MLLP, Secure FTP, VPN
Transport Approaches in Use or Emerging:
SOAP, HTTP+MIME
## Administrative Transport and Security Standards/Specifications

<table>
<thead>
<tr>
<th>Specification/Profile</th>
<th>Primary Use</th>
<th>Underlying standards</th>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| CAQH CORE Connectivity and Security Operating Rules | Exchanging HIPAA Administrative transactions (mandated for HIPAA covered entities by Affordable Care Act for some EDI transactions) | SOAP, HTTP+MIME, X.509  | • “Bottom-up” voluntary and consensus based specifications development by industry members based on business needs  
• Mature specifications, well aligned with clinical transport (e.g., IHE XDR)  
• Health Plans are required to implement for compliance with ACA | • Certificate trust policy / infrastructure is not specified, left up to trading partners  
• By design, Operating Rules are based on mature open standards, so may not leverage newer technical developments (e.g., Direct, REST, OAuth) |

Legacy Standards in widespread use: Secure FTP, VPN and others (e.g., batch transactions like Healthcare Claims)
Summary of Transport and Security Specifications across Initiatives
Broad Categorization of Health Data Exchange Approaches

- **Data Exchange Approaches**
  - **HTTP Based**
    - OSI Model Level 4
      - SOAP based approaches
        - IHE XDR (NwHIN/eHealth Exchange),
        - CAQH CORE Connectivity,
        - PHINMS (ebXML)
    - OSI Model Level 5 & 6
      - REST based approaches
        - HL7 FHIR (CommonWell, Argonaut)
      - PHINMS (ebXML)
  - **SMTP Based**
    - SMTP + SMIME + Metadata
      - Direct with XDM Metadata
    - SMTP + SMIME
      - Direct without XDM Metadata
  - **Legacy (SFTP, VPN etc)**
## Broad Categorization of Transport Approaches and their Characteristics

<table>
<thead>
<tr>
<th>Underlying Standard/Approach</th>
<th>Example Standards/Specifications</th>
<th>Characteristics</th>
<th>Ideally Suited for</th>
</tr>
</thead>
</table>
| **SOAP based** (SOA/Web Services) | IHE XDS/XDR (eHealthExchange)  
                             • SOAP+WSDL (CAQH CORE Connectivity Rules)  
                             • ebXML (PHINMS)  | • Can support push, query/response or publish-subscribe  
                             • Metadata and security tokens in the message envelope improve routing, reliability and security  
                             • Transport and data content are loosely coupled  | B2B interactions with strong trading partner contracts, envelope level strong security (WS-Security and SAML for envelope level authentication / authorization) |
| **REST based** (API/Micro-services) | HTTP, JSON/XML (HL7 FHIR, Argonaut, CommonWell)  | • Can support push, query/response or publish-subscribe  
                             • C2B granular data accessed using resources and HTTP verbs  
                             • Decouples “resource” access from transport  
                             • Application to B2B data exchange and trust models yet to be fully fleshed out  | Public facing APIs with small implementation footprints, relatively simple security requirements and high performance requirements |
| **SMTP based** (Secure Email) | SMTP + SMIME  
                             IHE XDM metadata (ONC Direct)  | • Not suited for query/response  
                             • Routing/security infrastructure (HISPs) makes onboarding relatively simple  
                             • Simple infrastructure needs - need not have a “server” to perform sending and receiving (client is sufficient)  | B2B Push of documents |
Data Exchange Models and Trust

Peer-to-Peer

Examples of Peer-to-Peer:
1) PHINMS “Direct-Send” between Labs and State Dept of Health
2) Provider-Payer interactions without Clearinghouses

Mediated and Centralized

Examples of Mediated and Centralized:
1) CDC Route-not-Read Hub
2) Provider-Payer interactions via single Clearinghouse

Mediated and Decentralized

Examples of Mediated and Decentralized:
1) ONC Direct (SMTP based) using 2 or more HISPs
2) Clinical data exchange using HIEs
3) Provider-Payer interactions via multiple (e.g., provider side and payer side) Clearinghouses
# Data Exchange Models: Operational and Security Trust Scalability Considerations

<table>
<thead>
<tr>
<th>Model</th>
<th>Operational Scalability</th>
<th>Security Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Peer-to-Peer</strong> (e.g., PHINMS Direct Send)</td>
<td>Limited operational scalability, suited for small scale networks (e.g., Labs to States)</td>
<td>• Can Support High Degree of security (e.g., end-to-end encryption) and trust</td>
</tr>
<tr>
<td></td>
<td>• Can Support High Degree of security (e.g., end-to-end encryption) and trust</td>
<td>• Could use Centralized Trust but typically use Peer-to-peer Trust/Security</td>
</tr>
<tr>
<td></td>
<td>• Can Support High Degree of security (e.g., end-to-end encryption) and trust</td>
<td>Reason: No industry-wide policy on central trust source.</td>
</tr>
<tr>
<td><strong>Mediated and Centralized</strong> (e.g., PHINMS RnR)</td>
<td>• Scalable to medium scale networks (e.g., for program requirements or for regional networks)</td>
<td>• Typical to use Centralized trust model</td>
</tr>
<tr>
<td></td>
<td>• Higher operational scalability is possible at relatively low security (e.g., public facing APIs typically fall here but could be designed to use decentralized trust model)</td>
<td>• Higher degree of security and trust is possible but can limit operational scalability</td>
</tr>
<tr>
<td><strong>Mediated with Decentralization</strong> (e.g., Clearinghouses, HIEs, ONC Direct with HISP infrastructure)</td>
<td>Scalable to national network (e.g., using HIE /HISP infrastructure)</td>
<td>• Typical to use De-centralized trust</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delegates some of the security functions to trusted intermediaries.</td>
</tr>
</tbody>
</table>

Regardless of security trust models, business level service agreements and Data Sharing Agreements are almost always Peer-to-Peer, which has been a bottleneck for nationwide scalability.
Maturity Levels of Data Exchange Approaches

Hype Cycle for Healthcare Technologies
(Courtesy: Gartner)

See Gartner report at: https://www.gartner.com/doc/3086917/hype-cycle-healthcare-provider-technologies

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Advantages</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relatively mature specifications (e.g., Operating Rules, eHealthExchange specifications, MU/ACA regulations)</td>
<td>Relatively stable, enables interoperability</td>
<td>Lags new technologies (e.g., mobile, cloud) and market trends by several years</td>
</tr>
<tr>
<td>New / emerging specifications (e.g., HL7 FHIR)</td>
<td>Better aligned with new market needs and trends</td>
<td>Evolving quickly, stability of specifications can be a challenge for interoperability</td>
</tr>
</tbody>
</table>
## Key aspects of Interoperability Initiatives that can add value to other Initiatives

<table>
<thead>
<tr>
<th>Initiative / Program</th>
<th>Key/Unique aspects that can add value to other initiatives</th>
</tr>
</thead>
</table>
| CDC (PHINMS/MTS)                           | - Reliability (e.g., guaranteed delivery, duplicate elimination, chunking)  
- Strong security (encryption, signature)  
- Route-not-Read architecture            |
| eHealthExchange / HealtheWay / NwHIN / Sequoia | - HIE specification (including normative XSD/WSDLs) and HIE infrastructure  
- Data Use and Reciprocal Services Agreement (DURSA) – legal trust framework |
| CAQH CORE Connectivity Rules               | - Normative envelope (XSD) and message interaction (WSDL) specifications  
- Separation of Real-time and Batch requirements  
- Stakeholder types and technical role definition (e.g. Provider has minimum technical role of a client, Health Plan has minimum technical role of server)  
- System availability, Response Times |
| ONC Direct                                 | - Secure SMTP (SMIME) based interoperability profile  
- Nationally scalable Health Information Service Provider (HISP) infrastructure for simplified on-boarding and delegation of authentication  
- Trust Bundles (DirectTrust) simplifies establishment of trust |
| HL7 FHIR / Argonaut                        | - Definition of common set of health data “resources” that can be accessed via HTTP verbs  
- RESTful architecture makes it useful for smaller implementation footprints (e.g., for public facing applications) |
| CommonWell                                  | Centralized services for patient lookup using REST                                                                           |
| National Association for Trusted Exchange (NATE) | User focused data exchanges, trust framework and trust bundle                                                                                   |
Legacy, Current and Emerging Standards, Potential for Convergence

Clinical

MLLP
SMTP+SMIME (Direct)
REST + JSON/XML + OAuth (FHIR)
SOAP
SFTP
VPN

Public Health

ebXML (PHINMS)

Administrative

Legacy
Emerging

HTTP+MIME
Implementation Level Considerations and Potential for Optimization using Reusable Infrastructure Components
Drivers for Implementation Level Choices for Transport and Security

- Regulatory requirements (e.g., Meaningful Use, Affordable Care Act)
- Program requirements (e.g., CDC PHIN)
- Project functional (e.g., push/pull) and security (e.g., payload encryption) requirements
- Specifications already implemented / supported by organization and trading partners
- Availability of COTS or reference implementations
- Emerging Technologies, Hype curve
- Availability of Developers
- Timeline and budget
- Build vs Buy
Potential for Implementation Level Optimization via Reusable Infrastructure Components Across Health Data Exchange Types

**Data Exchange Gateways**
- Supporting multiple interoperability standards
- Common management approach
  e.g., BNETAL SureDeliver (SureDeliver.com)

**Security Infrastructure**
- Authentication, Authorization, Signatures
- Digital Certificate Management, Perimeter security
  e.g., BNETAL ManageSecure (ManageSecure.net)

**Monitoring for Reliability**
- Uptime and Performance
- Receipt of Scheduled Batch files
  e.g., BNETAL SureVigil (SureVigil.com)
Common Infrastructure Component Example: BNETAL SureDeliver

Healthcare Provider

Or

State Health Dept

Or

Health Information Exchange (HIE)

NwHIN Exchange
ONC DIRECT

HIE/NwHIN

CDC PHIN

Public Health

CAQH CORE Connectivity

Payers

NCPDP Connectivity

Pharmacies

CMS esMD

Medicare

SFTP, WSRM

All
Common Infrastructure Component Example:
BNETAL ManageSecure for Security Resource Management

ManageSecure
Security Resource Management

- Deployed/Testing Certificates
- Deployed/Testing KeyStores
- Deployed/Testing TrustStores
- Deployed/Testing Passwords
- CRLs
- Application Licenses
- User Identities
- Roles, Privileges
- Web Servers
- App Servers

Relationships among resources (e.g., Certificates, Keystores, Trust Stores, CRLs, Passwords)
Expiration and Error Notifications (e.g., certificate / keystore expiration, trust chain validations)
Web Authentication / Authorization (RBAC, SSO, Single and Multi-factor Authentication)
## Specifications / Profiles: Primary Use, Timeline and Status

<table>
<thead>
<tr>
<th>Specification/Profile</th>
<th>Primary Use</th>
<th>Underlying standards</th>
<th>Current Status, Adoption into regulations</th>
</tr>
</thead>
</table>
| CDC PHINMS            | Public Health | ebXML over HTTP/S     | • In production since 2003  
• Adopted into Meaningful use Stage 2 (Syndromic Surveillance, Lab Reporting) |
| eHealthExchange / NwHIN / HealtheWay | Clinical, Public Health, administrative (CMS esMD) | IHE XDR (SOAP over HTTP/S) | • In production since 2004  
• Adopted into Meaningful Use Stage 2 (Certified EHR for transitions of care) |
| ONC Direct            | Clinical, Public Health | SMTP, SMIME, XDM | • In production since 2010  
• Adopted into Meaningful Use Stage 2 (Certified EHR for transitions of Care) |
| CAQH CORE Phase II Connectivity and Security Operating Rules | Administrative | SOAP over HTTP/S HTTP+MIME | • In production since 2012  
• Adopted into Affordable Care Act #1104 (mandated for HIPAA covered entities for Eligibility, Claim Status, ERA) |
| RESTful APIs (e.g., HL7 FHIR) | Clinical, Public Health | HTTP/S REST, XML/JSON | • FHIR is Draft Specification for Trial Use version 2 (DSTU2).  
• FHIR pilots in progress (Argonaut, CommonWell) |
## Data Exchange Interoperability Testing Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| Centralized Testing (e.g., CORE Certification, Drummond Group) | • Technical requirements can be uniformly applied to all entities testing  
• Can establish conformance/compliance | • Conformance does not mean interoperability  
• Some interoperability issues only surface on peer-to-peer testing  
• Interpretation/implementation errors at central tester can propagate across all implementations |
| Peer-to-Peer Testing (e.g., IHE Connectathon) | • Goes a long way in establishing interoperability                  | • Without significant vetting by central authority, risk of pair-wise improper interpretation and agreement, resulting in significant rework and retesting |

### Effective Path:
Centralized testing to establish conformance, followed by peer-to-peer testing to establish interoperability. Results from peer-to-peer testing used to improve centralized testing.