ISO 21089 – Health Informatics – Trusted End-to-End Information Flows

Presentation to S&I DPROV Community
Gary L. Dickinson
20 November 2014
ISO 21089 – Trusted End-to-End Information Flows

Lifespan and Lifecycle Events

• First HIT Standard to focus on health data/record:
  – **Lifespan** – point of origination to point of destruction/deletion
  – **Lifecycle events** occurring at various points in the lifespan
ISO 21089 – Trusted End-to-End Information Flows

Data/Record Lifespan and Lifecycle

• First balloted/published in 2004
  – Acts/Actions documented in Act Record (original term)

• Currently in revision
  – Approved ISO TC215 New Work Item in September 2014
  – Acts/Actions documented in Record Entry(ies) (new term)
ISO 21089 – Trusted End-to-End Information Flows

Data/Record Lifespan and Lifecycle

Figure 12.1  Key Trace/Audit Points in Trusted End-to-End Information Flow (Example)

(Act Performance)
Act Record Origination

Record Verification

Record Amendment

Record Disclosure, Transmittal

Record Access/Use

Record Archival

Record Loss, Destruction or Deletion

Health Record Instance - Origination, Retention, Stewardship
(Per Instance of Health Service Act)

APP1 - Record Originator

Act Record & Data Definition

APP2 - Record Receiver

APP3 - Record Receiver

Interfaces

Record Translation

Record Receipt

Record Convergence, Reporting

Record De-Identification, Aliasing

20 November 2014

ISO 21089 - Trusted End-to-End Information Flows
Derivations of Record Lifespan/Lifecycle include:

2007 – HL7 EHR Interoperability Model DSTU
2008 – HL7 CDA R2 Implementation Guide for EHR Interoperability DSTU
2008 – HL7 EHR Lifecycle Model DSTU
2009 – HL7 Records Management/Evidentiary Support Functional Profile (of EHR-S FM R1.1)
2014 – ISO/HL7 10781 EHR-S FM R2
2014 – ISO/HL7 16527 PHR-S FM R1
2014 – Record Lifecycle Events using HL7 Fast Health Interoperability Resources (FHIR)
Dimensions of End-to-End Flow

Record Lifespan

1. Within Single System
   - **Starting** at point of origination, in Source System, **OR**
   - **Starting** at point of receipt, in Receiving System
   - **Ending** at point of deletion

2. Across Multiple Systems
   - **Starting** at point of origination, in Source System
   - **Traversing** one or more Points of Exchange
   - **Ending** at point of deletion, in each System
## Record Lifespan – End-to-End

### Within Single System

<table>
<thead>
<tr>
<th>Start</th>
<th>Intervening Record Lifecycle Events (0 to many)</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source System</strong></td>
<td>(2) Amend&lt;br&gt;(3) Translate&lt;br&gt;(25,4) Verify, Attest&lt;br&gt;(5) View/Access&lt;br&gt;(6) Output/Report&lt;br&gt;(7) Disclose&lt;br&gt;(8) Transmit&lt;br&gt;(10) De-Identify&lt;br&gt;(11) Pseudo-nymize&lt;br&gt;(12) Re-Identify&lt;br&gt;(13) Extract&lt;br&gt;(14,15) Archive, Restore&lt;br&gt;(17,18) Deprecate/Retract, Re-Activate&lt;br&gt;(19,20) Merge, Unmerge&lt;br&gt;(21,22) Link, Unlink&lt;br&gt;(23,24) Place, Remove Legal Hold&lt;br&gt;(26,27) Encrypt, Decrypt</td>
<td>(16) Destroy</td>
</tr>
<tr>
<td><strong>Receiving System</strong></td>
<td>(9) Receive/Retain Record Entry</td>
<td>(16) Destroy</td>
</tr>
</tbody>
</table>
# Record Lifespan – End-to-End

## Across Multiple Systems

<table>
<thead>
<tr>
<th>Start</th>
<th>Intervening Record Lifecycle Events (1 to many)</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Source/Originating System</td>
<td></td>
<td>1 or more Receiving System(s)</td>
</tr>
<tr>
<td>(1) Originate/Retain Record Entry</td>
<td></td>
<td>(9) Receive/Retain Record Entry</td>
</tr>
<tr>
<td>... (6) Output/Report</td>
<td></td>
<td>... (5) View/Access</td>
</tr>
<tr>
<td>(7) Disclose</td>
<td></td>
<td>(6) Output/Report</td>
</tr>
<tr>
<td>(8) Transmit</td>
<td></td>
<td>(13) Extract</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>(16) Destroy</td>
<td></td>
<td>(16) Destroy</td>
</tr>
</tbody>
</table>

Repeated at each point of exchange to each Receiving System…

---

20 November 2014

ISO 21089 - Trusted End-to-End Information Flows
Traceability

• Forward Traceability
  – Source perspective
  – Point to point downstream: to whence it goes

• Backward Traceability
  – User perspective
  – Point to point upstream: from whence it came
As the health record subject (e.g., patient, health plan member)...

How might I be assured (trust) the persistent integrity and authenticity of my health record and its content?

How might I be assured that access/use of my health record is based on "need to know" principles?

How might I be assured that routine access/use of my health record is according to my consent agreement? Other disclosures according to my specific authorization?

With regard to my health record, how might I be assured (trust) that accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

- Record origination, amendment, verification, translation?
- Record access/use?
- Record disclosure and transmittal?
- Record receipt, retention and stewardship?
- Record de-identification or aliasing?
- Record archival, destruction?
As an accountable provider of health(care) services (as ascribed in the health record)... As an accountable author, scribe and/or verifier of health record content...

How might I be assured (trust) the persistent integrity and authenticity of health record content ascribed to me?

With regard to health record content ascribed to me, how might I be assured (trust) that subsequent accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

- Record origination, amendment, verification, translation?
- Record access/use?
- Record disclosure and transmittal?
- Record receipt, retention and stewardship?
- Record de-identification or aliasing?
- Record archival, loss or destruction?

Trusted information flow - from Point of Record Origination to Point of Access/Use
Typical downstream flow paradigm

Perspective: Accountable Party for health record content as VIEWED DOWNSTREAM

Downstream Information Flow and Trust Perspective
Health Record Author/Originator
As an accountable user of health record content...

How might I be assured (trust) the persistent integrity and authenticity of health record content which I access and use?

With regard to health record content, how might I be assured (trust) that accountable actions by accountable parties are ascribed, authenticated and traceable, including key points in the record lifecycle:

• Record origination, amendment, verification, translation?
• Record access/use?
• Record disclosure and transmittal?
• Record receipt, retention and stewardship?
• Record de-identification or aliasing?
• Record archival, loss or destruction?
Complementary ISO/HL7 Standards

**Scope**

<table>
<thead>
<tr>
<th>ISO/HL7 10781/16527 – EHR/PHR System Functional Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Originate, retain Record Entry</td>
</tr>
<tr>
<td>(8) Transmit Record Entry(ies)</td>
</tr>
<tr>
<td>(9) Receive, retain Record Entry(ies)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO 21089 – Trusted End-to-End Information Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source System</td>
</tr>
<tr>
<td>Sending System</td>
</tr>
<tr>
<td>Course of Exchange</td>
</tr>
<tr>
<td>Receiving System</td>
</tr>
</tbody>
</table>

(#{) Lifecycle Event}
## ISO 21089 – Trusted End-to-End Information Flows

### Pre/Post Events 1-9

<table>
<thead>
<tr>
<th>Pre Event State</th>
<th>Resource @ Event</th>
<th>Post Event State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>+ Provenance</td>
<td>X</td>
</tr>
<tr>
<td>[Record Entry as persisted, indivisible and immutable since previous Lifecycle Event]</td>
<td>1 Originate/Retain</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>2 Amend</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>3 Translate</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>4 Attest</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>5 Access/View</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>6 Output/Report</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>7 Disclose</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>8 Transmit</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>9 Receive/Retain</td>
<td>X</td>
</tr>
</tbody>
</table>

20 November 2014

ISO 21089 - Trusted End-to-End Information Flows

14
### ISO 21089 – Trusted End-to-End Information Flows

#### Pre/Post Events 10-18

<table>
<thead>
<tr>
<th>Pre Event State</th>
<th>Resource @ Event</th>
<th>Added Event Evidence</th>
<th>Retained Pre Edition Unaltered</th>
<th>Added New Edition</th>
<th>Signed as Author</th>
<th>Signed as System</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Record Entry as persisted, indivisible and immutable since previous Lifecycle Event]</td>
<td>SecurityEvent + Provenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10 De-Identify  
11 Pseudonymize  
12 Re-Identify  
13 Extract  
14 Archive  
15 Restore  
16 Destroy/Delete  
17 Deprecate  
18 Re-Activate  

- [none]

20 November 2014
### ISO 21089 – Trusted End-to-End Information Flows

#### Pre/Post Events 19-27

<table>
<thead>
<tr>
<th>Pre Event State</th>
<th>Resource @ Event</th>
<th>Post Event State</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Record Entry as persisted, indivisible and immutable since previous Lifecycle Event]</td>
<td>19 Merge</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>20 Unmerge</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>21 Link</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>22 Unlink</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>23 Add Legal Hold</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>24 Remove Legal Hold</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>25 Verify (new event)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>26 Encrypt (new event)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>27 Decrypt (new event)</td>
<td>X</td>
</tr>
</tbody>
</table>
# Record Entry Lifecycle

**Lifecycle Starts:** at Point of Origination/Creation as New Event

<table>
<thead>
<tr>
<th>Prior Event Added…</th>
<th>During Interval between Events Retains (at rest): Indivisibly+Immutably</th>
<th>PRE At New Event Adds…</th>
<th>POST Becomes Prior Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SecurityEvent instance</td>
<td>1 or more SecurityEvent instances &gt;&gt; One per each prior Record Lifecycle Event</td>
<td>➔ 1 SecurityEvent instance</td>
<td></td>
</tr>
<tr>
<td>1 Provenance instance</td>
<td>1 or more Provenance instances &gt;&gt; One per each prior Record Lifecycle Provenance Event</td>
<td>➔ 1 Provenance instance</td>
<td></td>
</tr>
<tr>
<td>1 or more other resource instance(s)</td>
<td>1 or more other FHIR resource instances &gt; Corresponding to Action(s) Taken &gt; As documented in Record Entry(ies)</td>
<td>➔ 1 or more other resource instance(s)</td>
<td></td>
</tr>
</tbody>
</table>

Pre/Post Entry Content and…

20 November 2014

ISO 21089 - Trusted End-to-End Information Flows
ISO 21089 – Trusted End-to-End Information Flows

Contact/Links

• Gary L. Dickinson
  – Director, Healthcare Standards, CentriHealth
  – Co-Chair, HL7 EHR Work Group
  – Co-Facilitator, HL7 EHR Interoperability Work Group
  – (+1) 951-536-7010
  – gary.dickinson@ehr-standards.com

• HL7 EHR Interop Wiki:
Health Record Trust Stakeholders

- **Individuals**
  - Health record subjects, subjects of care
    - Patients, health plan members
  - Health(care) professionals, caregivers, record authors, scribes, verifiers, record users

- **Organizations**
  - Providers, health plans, employers…

- **Business units**
  - Departments, services, specialties…
ISO 21089 – Trusted End-to-End Information Flows

Trust Stakeholders

<table>
<thead>
<tr>
<th>Trust Stakeholders for health record content, including individually identifiable information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stakeholder</strong></td>
</tr>
<tr>
<td>Subject of Care, Health Plan Member</td>
</tr>
<tr>
<td>Next of Kin, Emergency Contact</td>
</tr>
<tr>
<td>Healthcare Professional, Caregiver</td>
</tr>
<tr>
<td>Care Assistant</td>
</tr>
<tr>
<td>Transcriptionist</td>
</tr>
<tr>
<td>Department, Service, Specialty</td>
</tr>
<tr>
<td>Healthcare Provider</td>
</tr>
<tr>
<td>Integrated Delivery Network (IDN)</td>
</tr>
<tr>
<td>Payment Guarantor, Health Plan, HMO</td>
</tr>
<tr>
<td>Value Added Network, Claims Clearinghouse</td>
</tr>
<tr>
<td>Employer</td>
</tr>
<tr>
<td>Public Health Agency</td>
</tr>
<tr>
<td>Regulatory Agency</td>
</tr>
<tr>
<td>Accreditation Agency</td>
</tr>
<tr>
<td>Research</td>
</tr>
<tr>
<td>Professional Education</td>
</tr>
<tr>
<td>Others</td>
</tr>
</tbody>
</table>
5 Overview - Characteristics Essential to Trusted End-to-End Information Flows

Interchange Content, e.g.,
- Patient/member health records, protected as individually identifiable
- Patient account, insurance records
- Clinical data
- Administrative and operational data
- Measures/indicators: performance, quality, compliance, utilization, productivity, costs

Auditability, Traceability, Audit Trails
- Access/use record
- Originate/amend/verify/translate record content
- Disclose/transmit/receive record content
- Process/aggregate/derive/summarize/extract record content

Authentication
- User: proof of individual identity
- Source/Origin: proof of source/origination, authorship
- Validation: proof of verification (e.g., automated device input)
- Data Exchange: proof of transmittal & receipt

Data Integrity
- Accuracy, consistency, continuity, completeness, context, comparability

Persistence of Health Record
- Permanence, Indelibility, revision by amendment only
- Data states: initial and each subsequent amendment

Persistent Health Event/Act Contexts
- Accountability • Data Integrity • Clinical • Administrative/Operational

Privacy/Confidentiality: Individually Identifiable Information
- Individually Identifiable, De-identified or Aliased

Interchange Content: e.g.,
- Personal health records
- Claims, attachments
- Public health reporting
- Measures/indicators
- Research extracts

Accountability, of:
- Individuals: Healthcare Professionals, Authors, Scribes, Verifiers...
- Business units: Departments, Services, Specialties
- Organizations: Providers, Health Plans...

X12N EDI
EDIFACT
HL7 v2.x

Figure 5.1: Example Scenario for Trusted End-to-End Information Flows