Knowledge Network
Data Provenance in Cross-Enterprise Exchange

23 March 2018
Knowledge Network

What is the Knowledge Network?

Peer assistance program and forum for collaboration

Monthly webinars
  – Presentations by Members or guest speakers
  – Discussion on topics of importance to Members
  – Member meetings

Send topic ideas info@ca-hie.org

Visit www.ca-hie.org/resources/knowledge-network for more information including past recordings, and additional resources

23 March 2018 CAHIE Knowledge Network Webinar
Reminder

Webinars are recorded and made available on our web site

Mute yourself if you do not wish to be recorded.
Data Provenance provides information on ownership, origin, and chain-of-custody for medical records. RAIN's ONC-sponsored Data Provenance Toolkit was recently employed by multiple systems at HIMSS 2018 to demonstrate cross-vendor provenance exchange. This month's presentation will discuss lessons learned at HIMSS, how provenance can benefit health information systems moving forward, and how provenance can work with both legacy repositories and next-generation Blockchain infrastructures to deliver smarter results and overcome policy barriers to interoperability.

RAIN Live Oak was a Phase 2 winner of ONC's "Oh the Places Data Goes: Health Data Provenance" Challenge for this ground-breaking work.
Data Provenance In Cross-Enterprise Exchange

- Improve trust & security
- Track granular origin & authorship
- Seamlessly support legacy & next-gen technology
- Leverage emerging tools: FHIR and Blockchain
Introduction

- **RAIN Live Oak Technology**
  
  - Over two decades advancing community technology & telemedicine.
  
  - Participant in IHE, HL7 & HIMSS programs supporting interoperability.
  
  - Award-winning participant in the ONC *Oh, The Places Data Goes* initiative to develop innovative data provenance solutions.
What is *Data Provenance*?

- Data Provenance is an industry-spanning concept. Found in physics, finance and art collection, "Provenance" refers to verifiable data about an object or document. It provides information on ownership, origin, and a chain-of-custody as the target object/data moves.

- In health information provenance is applied to medical records – in whole or granularly – to create portable metadata serving as certificates of authenticity.

- **Strong provenance gives two important pieces of assurance:**
  - **Context:** Where did the care event occur, which physicians & technicians participated, and what hardware was employed.
  - **Authorship:** Guarantee the point of origin for the data – either to an organization or an individual physician.
Provenance For Document Security

- More than metadata, provenance provides security backing for diverse documents. Using provenance, each time a record is updated a digital signature is generated – this signature is published and travels with the document, allowing recipients to cryptographically verify (1) that the document's authorship is genuine and (2) that the document is still in its original form – it hasn't been modified, corrupted or tampered with.

- This is a powerful tool for cross-enterprise exchange: signatures ensure security when documents are exchanged over regular Internet connections.

- As a patient's record traverses multiple health systems, provenance maintains historical chain-of-custody so updates can be traced back to their origin.
As part of the ONC *Oh, The Places Data Goes* challenge RAIN set out to develop a portable, cross-platform Data Provenance Toolkit that can easily integrate into health information systems to quickly enable provenance use, including generation and validation of provenance documents from any source.

The Data Provenance Toolkit is a software library or plug-in which can be imported into a host system and used to create and consume provenance documents within the host's information infrastructure.

Multiple cryptography standards are supported, giving flexibility in the storage and type of keys/certificates used, and the Toolkit can process documents regardless of source: provenance generated by another software tool can still be consumed and analyzed.
Cross-Enterprise Provenance: Lessons learned at HIMSS 2018

- RAIN partnered with five leading health IT vendors to participate in the HIMSS 2018 Interoperability Showcase. During the *Collaborative Community Cancer Care* scenario we demonstrated the use of diverse protocols to enable exchange of records across multiple vendors & systems.

- RAIN's Data Provenance Toolkit and FHIRelate document server were used to act as a patient record repository. Our Provenance Toolkit was integrated into both our own user client and into the Qvera Integration Engine.

- As part of the demonstration, the Qvera Integration Engine generated a diagnostic report and ultrasound image which were stored in our repository. The Provenance Toolkit was used to generate metadata and signature to also store, without Qvera having any native support for provenance.

- On the receiving side, our client leveraged the Toolkit to consume the provenance and confirm ownership by the Qvera certificate.
In keeping with our commitment to technical advancement, development of the tools used at HIMSS has focused on the FHIR standard. As FHIR gains industry support its security mechanisms will become increasingly prominent.

- FHIR defines a Provenance resource (document structure) which links to a target resource (such as a diagnostic report) and carries context information and signature for it.

- Provenance is stored as a separate document but references a specific record version, so as documents are updated new provenance is generated to track each change.

- This provides greater flexibility and security: a client system can query a FHIR server using the powerful RESTful API and – either in a joint query or separately – retrieve provenance for resources considered mission-critical.
FHIR is an emerging specification, parts of which are still under development. Even as support for it grows there will remain extensive legacy repositories of pre-FHIR documents; some may be translated to FHIR but others will remain in their original format (such as CCD/C-CDA and HL7).

The mix of new & old documents in multiple formats creates the opportunity for multiple approaches to provenance implementation:

- **Backporting**: Provenance can be generated & stored for existing documents, though this has limits due to the age of data available.
- **New Provenance**: With support for diverse formats systems can maintain provenance records for multiple document types, storing each as appropriate.
- **Hybrid**: New standards such as FHIR support referencing or storing older formats. The FHIR Provenance resource can refer to a non-FHIR document, allowing a FHIR server to act as a provenance repository for records stored elsewhere and in other formats.
Blockchain for distributed provenance

- Multiple projects under *Oh, The Places Data Goes* explored the use of Blockchain to support provenance in health information. A distributed data model has the power to bring reliable, highly interoperable security services to the industry forefront.

- At its core provenance – especially FHIR Provenance – is database agnostic: the documents can be retrieved from or stored in any type of repository. This enables a flexible approach to provenance meeting the needs of implementers.

- A secure database can be rapidly deployed using a Blockchain implementation, and a provenance library will then be used to generate documents for storage in the Blockchain, and to validate records retrieved from that or other sources.

- This allows health information systems to deliver a strong provenance ledger without disrupting their existing repositories or necessitating extensive internal development to support provenance, and leverages common standards to make provenance records portable and long-lasting.
Provenance is most valuable when applied to data coming from diverse sources. What source is more diverse than patients themselves?

The adoption of provenance in consumer-facing and wearable health technology has the potential to redefine how we interact with patient generated health data.

Attaching provenance to patient-sourced data – either by a wearable device or integrated into an app/web portal – provides much greater assurance of the origin, nature and authenticity of that data. Patient generated data often travels across numerous systems, making this information extremely valuable.

Consumer devices/apps link activity to a user account, allowing these tools to accurately generate provenance signed unique for that individual, whether it be the patient themselves, a family member or a caregiver.
Overcoming Barriers

- Interoperability has come a long way. Whereas the focus was once on local data storage, cross-vendor interoperability is now baked right in to next-generation specifications, making seamless, accurate document exchange an assumed.

- Many of the remaining barriers to widespread health information exchange are policy-based: where did a document come from, who is authorized to view or edit it, and what are my organization's responsibilities regarding data authoritativness?

- Provenance alleviates these concerns by building persistent, verifiable histories for documents and discrete data elements. The presence of companion provenance will allow systems to exchange and act on records with confidence.
Authorship & Context

- Health data repositories grow every day and each new partner creates a new node in the complex web of data sourcing, storage and exchange.

- Data Provenance – portable, data-rich metadata documents – serves as sources of authority on medical records without requiring a single centralized entity to act as the "source of truth". Distributed certificate-based trust, as is already the foundation for Internet security, gives health IT systems better control over the data they use.

- Verifiable authorship protects patients from fraud, improves data security, reduces waste by giving reports an extended shelf-life, and makes it possible to find when and where a document change – authorized or malicious – was made.
THANK YOU

liveoak@rain.org

http://www.liveoaktech.net
Questions?
Next Month

Clinical Data Collection

27 April 2018

The Department of Health Care Services will talk about their efforts to advance the ability of program areas to exchange health information with trading partners throughout the state.