Data Linkage: Ready of Not, It's Here [part 2]

Save to myBoK

by Lorraine Fernandes, RHIA

As stewards of the data housed within our organizations, HIM professionals must be cognizant of ongoing work to facilitate sharing of data across networks. Such activities will gather momentum in the coming years as electronic health records become common practice. HIM professionals must endeavor to be involved in the planning of local and regional initiatives to ensure that patient data is shared appropriately and that HIM practices will support accurate data linkage.

Part 1 of this column (February 2005) discussed the background and select sections of Connecting for Health's linking work group report titled "Linking Healthcare Information: Proposed Methods for Improving Care and Protecting Privacy." This column highlights the record locator service, security and privacy, and pilot projects, with emphasis on areas of interest to HIM professionals.

Record Locator Service

The report proposes a "connection broker" to process requests for patient records among facilities. Dubbed the record locator service (RLS), this service would identify patient records in the network and provide the locations to the authorized requestor. The RLS would not routinely deliver the clinical information, although this is an option.

At all times, the release of the actual information remains in the control of the provider for the episode of care. The provider would make a two-part decision on the availability of data: whether to include the data in the RLS (and if so, what data to include) and whether to share the indexed data once a query is launched. The patient controls who is authorized to view the data. In addition to providers, the patient can authorize or delegate access to additional parties, such as a spouse or child. Further, while the work group does not advocate such, the patient can choose anonymity (not indexing the record) or pseudonymity (using fictitious demographic data) at the local level.

The RLS would hold four types of information:

- Demographic information to facilitate patient identification across the organizations holding data. This data should not include unencrypted Social Security numbers. If the RLS has the ability to identify potential matches to the query (as opposed to the highest scoring match), the Social Security number may be useful in defining the best match.
- Healthcare provider information.
- A listing of records held by healthcare providers.
- Contact information for the providers holding records.

A newly formed legal entity would take responsibility for ownership and operation of the RLS, as well as all operational and security considerations. Designing the right approach for the RLS will be a key part of pilot projects. Operational requirements for the RLS might include:

- Availability 24 hours a day, seven days a week
- Noninvasive operation (i.e., the RLS does not affect operations at the participating facilities)
- Support of real-time updates
- Support of real-time queries

The work group recommends that the RLS should:

- Survey existing technical practices and approaches for distributed synchronization of databases
- Survey existing organizational arrangements
- Develop or adopt standard legal templates for users that address privacy concerns
- Launch pilot projects involving three or more organizations

Transfer of records could be accomplished as it is commonly executed today—via fax, phone, or electronically, depending on the technical sophistication of the particular institutions involved. Record transfer practices can change over time as electronic standards-based technology becomes more prevalent.

Architectural Features

The underlying principles for the architecture include:

- Several layers of security are established and supported through encrypted data transfer.
- No clinical data will be centralized in the RLS.
- Only institutions with authorized credentials will be allowed access to the RLS.
- No national healthcare identifier is required.
- Data remains in the hands of the providers who have direct access to the patient and who originally created the data.
- Significant variation in technical sophistication among the participants is supported. The minimum requirement is the ability to list patients in an electronic format, with records at the specific institution.

Incremental Participation in Record Transfer

Since IT sophistication among healthcare providers varies widely, two scenarios were explored that would allow individual institutions to participate without significant investment in equipment or personnel. The simplest is a local gateway that would sit between the requestor and the RLS. This small computer, housed locally, would have a standards-compliant interface that would enable communication between systems. An alternative scenario is use of a proxy server. A proxy server would function similarly to a local gateway, but it would be hosted on the Internet. With this set-up, several organizations could share the cost and access; however, it increases the requirements for systemwide IT support.

The RLS and its preliminary architecture are seen as a “network of networks” that must scale to varying sophistication, volume of physicians and institutions, clinical data exchange users that rarely or never interact currently, geographic boundaries, and the lack of a national healthcare system. These challenges require exploration around interpretation of received records, defining membership in the RLS, and certification of standards conformance. Membership must address the varying technical sophistication among healthcare providers, finances of the participants, and the value received from the data recipients.

Security and Privacy

The basic tenet that security is a process, not a technology, remains intact. With that in mind, the work group contemplated an architecture that allows several layers of security and that supports confidentiality, authentication, integrity, and nonrepudiation. Security standards must support the three security domains of wire, perimeter, and content. For instance, institutions and individuals must have authorization credentials; traffic between the institutions and network would be encrypted; and communication between institutions would be encrypted or conducted outside the network. Strong policies and procedures supporting security must be used, including authentication of the users. Audit trails in the form of immutable logs documenting who has accessed specific records and the purpose should be required. The security challenges will be a key component of pilot projects, with security experts being involved in next phase of activities, as their input is vital to success.

Next: Pilot Projects

The work group’s report articulates a common conclusion reached by its members as the result of many research efforts—national-scale data linkage to support the effective interchange of patient clinical data is achievable in incremental steps using existing technology. However, much work remains, particularly around legal, architectural, and organizational fronts.

The next phase involves pilot projects to validate existing theories and identify solutions to known and unknown challenges. Effectively linking patient data can advance the goals of implementing electronic health records and providing better healthcare.

Reference

Connecting for Health. “Linking Healthcare Information: Proposed Methods for Improving Care and Protecting Privacy.” February 2005. Available online at www.connectingforhealth.org.

Lorraine Fernandes *(lfernandes@initiatesystems.com) is senior vice president of healthcare practice, Initiate Systems, Inc.*

Article citation:
Fernandes, Lorraine. "Data Linkage--Ready or Not, It's Here." *Journal of AHIMA* 76, no.3 (March 2005): 62-63.