Using Data Provenance to Manage Patient-Generated Health Data

By Vernessa Fountain, RHIA

Healthcare providers are facing a swelling tide of patient-generated health data (PGHD). Growing mobile health technology and personal electronic health records are allowing consumers to become more involved not just in making appointments with physicians, but with tracking and reporting their health as well. In addition, there are a variety of avenues for the transmission of PGHD, from secure messaging and other Internet-enabled methods or via telephone and face-to-face visits. All this data and information may be eventually loaded into the provider's electronic health record (EHR) system, where it potentially becomes a part of the patient's record.

The ability for a patient to capture and then share their health data electronically, such as data from remote monitors, has given patients a chance to more fully participate in their own care. Leading organizations such as the Mayo Clinic and Beth Israel Deaconess Medical Center have expressed interest in new technology that allows patients to be more interactive with their healthcare.

Defining PGHD

PGHD is health information such as health history, symptoms, monitoring, and other information that is captured or inferred by or from patients, their families, or others involved in the patient's care. Most notable is that the patient—not the provider—is the one who captures this data. In addition, the patient controls who receives the information. PGHD is separate from the information created in clinical settings through encounters with providers.

PGHD may be used to supplement the health data gathered directly by healthcare providers. Patients track and record changes in their health conditions using devices such as smartphones, mobile health applications, wearable technology, e-mail, and patient portals. PGHD may offer a more comprehensive picture of the patient's overall health, including vital signs and symptoms, and changes in health that occur outside the traditional clinical environment.[1] Instances where PGHD is transmitted directly to the provider prior to the patient's appointment can also help providers be more prepared for the patient's visit.

In addition, when patients share the results of a procedure or test from another provider, they can decrease the number of duplicative services. An up-to-date list of medications from all providers created by a patient, including what is being taken as compared to what has been prescribed, is important for care coordination. Finally, data in general about a patient's medications, allergies, intolerances, and outcomes not only provide for better patient outcomes, but help mitigate safety risks.

Defining Data Provenance

In order to utilize PGHD effectively in the delivery of care, providers must have processes in place for deciding what information will be used to treat the patient and how to incorporate it into the EHR. This is where data provenance comes into play. The term "data provenance" refers to an organization's ability to track and verify the origin of clinical information (i.e., from a health information exchange (HIE), personal health record (PHR), or EHR when it is first created), identify the author that created the documentation, determine who has ownership for usage of the data, and track any changes that are made to the data during its lifecycle.

The ability to identify the provenance is crucial to provider trust. However, most direct transmissions from the patient or the patient's PHR do not have data provenance tracking. Data provenance is important to PGHD that is captured in the EHR so that providers may track what data the patient, patient's family, or patient's designated caregiver documented regarding the patient's health, such as tracking vital signs or readings. Once PGHD becomes a part of the patient's health record, it becomes data that must be governed within the organization's EHR.

Integrating PGHD with Data Provenance Poses Challenges

Currently there is no uniform method of data provenance amongst EHR systems for determining the origin of information.[2] The industry lacks standards regarding data provenance provisions in EHRs that would help to make this a reality.[3]

The capability for providers to receive data from patients outside the clinical visit has not been systematically addressed. There are technical issues related to the capture, transmission, and integration of patient-generated data. In addition, most systems do not currently capture the data provenance needed. Commonly, data provenance is only at the "document" level, meaning that the provenance for each document will be inherited from the overall source versus each element, such as the medication level or problem list level. This lack of granularity creates integrity issues and undermines the overall trust of the data.

The following are only a few of the barriers that currently exist today to using data provenance to best handle PGHD:

- No dominant provenance models within health IT
- No uniform way of handling data provenance
- No harmonized standard is currently in place

Even the basic element of what data provenance metadata should be captured is challenging. For example, the question remains of who or what should be listed in the source metadata, and at what granularity should the provenance be captured—the entire document, each section, or at each record entry. Does the full record capture the source, or should each section capture the source (i.e., the medication list), or should each record entry capture the source (i.e., list each individual medication and the source)? Another consideration is how the provenance is updated or modified when it is imported or exported. Is the receiving organization now listed as the source, or does the original creator remain the source?

Some Providers Reluctant to Accept PGHD

Providers may be reluctant to receive the PGHD due to the amount of information, lack of trust, and inability to sort through the data, as well as a concern that this work may interfere with their ability to deliver quality care. There are concerns about finding the time to review and sort through the large amounts of patient-submitted data, which may lead to concerns of increased liability on the provider side and unrealistic patient expectations.

Providers are concerned about being held accountable for information that was not received or reviewed in a timely manner and information that may require an urgent response. The financial impact, the staff and physician time for reviewing, and the effort to process and analyze the data and create decision processes for potentially integrating it into the EHR all influence providers' willingness to accept PGHD.

On the other hand, patients may be concerned about their providers failing to use PGHD to meet their healthcare expectations. Concerns may include whether their providers have received and reviewed the data, integrated it into the patient's chart, or shared the information with other providers or family members as appropriate. Patients also may have concerns regarding whether the information received is secure.

Trusting the Data

In order to ensure the usefulness and integrity of PGHD, the system for bringing this data into the record should integrate clinical terminologies such as RxNorm for medication and LOINC for laboratory results. The clinical terminologies are text searchable and thus allow providers to more easily and dependably locate important information such as medicine provided to the patients. Standards should require the data to be tagged, and provide the source of the PGHD so it can be consistent across systems.

Organizations with a strong data provenance process will be able to track who has received the data, how it was sent or received, who reviewed the data, where it was reviewed, which device was used to access the patient's data, and if a consistent workflow is followed for all similar data throughout the healthcare organization.[4,5]

All data are considered an asset if they can be managed and leveraged to improve patient care outcomes and quality of care. Data provenance plays an important role with information governance to ensure all organization information is controlled,

reliable, and trustworthy, and that it accurately depicts patient care. Data provenance allows organizations to track information in all forms as it moves throughout the organization's network. As part of an overall information governance strategy, data provenance captures e-mails, patient-generated health data or self-management data, revenue cycle management, legal records, website content, videos, pictures, and traditional patient health records. This also includes structured data and unstructured data.

Information governance focuses on accuracy, validity, completeness, timeliness, and integrity of data. It also is known for ownership of data and the intended use of that data. HIM professionals working in a data stewardship role will be responsible for establishing and maintaining documentation processes and data quality standards. Quality must be monitored for compliance in how data is accessed, used, and secured. This role is accountable and responsible for the flow of patient information, from when it is captured through various media and entered into the record, to when it is accessed or moved within the record.

HIM professionals are becoming an asset to information governance efforts and have the skills to help establish programs that ensure the effective evaluation, selection, and prioritization of certified EHR systems that meet relevant organization expectations regarding information governance and data provenance capabilities. HIM professionals are poised to support the implementation of technological advancement and to help determine how metadata should be used for research and other clinical documentation, as well as implement data standards, support auditing for compliance, and ensure that a healthcare organization receives new version updates for existing legacy systems and electronic data to maintain compliance.

Current Efforts to Improve Data Provenance Use

Many EHR systems currently pose barriers to effective data provenance efforts, as they are unable to capture the origin data with sufficient granularity and specificity. There are currently initiatives underway at both the Standards and Interoperability (S&I) Framework and Health Level Seven (HL7) around data provenance. The S&I Framework data provenance initiative's focus includes:

- Establish guidance for handling data provenance in content standards, including the level to which provenance should be applied
- Establish the minimum set of provenance data elements and vocabulary
- Standardize the provenance capabilities to enable interoperability[6]

The initiative is working to identify and define guidance on the use of standards for facilitating data provenance capabilities.

The S&I Framework is also collaborating with HL7 to create standards to use when exchanging data. Though the focus is currently on defining how provenance may be used for the Clinical Documentation Architecture standard, this may be expanded into other use cases and exchanges. The initial work, the HL7 Implementation Guide for CDA Release 2: Data Provenance, Release 1 – US Realm (PI ID: 1093), was recently balloted through HL7.

Though standards for data provenance will provide the trust that providers seek regarding the data that are received from patients or from patients' PHRs, PGHD devices, and mobile health devices, policies and procedures for handling the data will still need to be developed. Processes to store the status of the information, regarding whether it has been reviewed by a physician, may not be consistent across the enterprise, much less across disparate systems.[7] It is also critical that PGHD "arrived" data cannot be altered or modified.[8]

Some questions remain. How would providers be notified when their patients' PGHD "arrived" for other providers to review? Are patients able to determine the data priority to alert their providers as to whether the data has a low, medium, or high priority?

As engaged consumers assume an increasing level of responsibility in their care, healthcare professionals must anticipate that PGHD, secure messaging, e-mails from patients to providers, and mHealth applications used by patients at the direction or instruction of their providers will become more prevalent. Data provenance, as part of an information governance strategy, will help organizations effectively track this data and thus ensure its integrity and usefulness as information that contributes to physicians' ability to better care for their patients.

Notes

1. Shapiro, Michael et al. "Patient-generated health data." RTI International. April 2012. www.rti.org/publications/abstract.cfm?pubid=20202.
2. Ibid.
3. Ibid.
4. Ibid.
5. Office of the National Coordinator for Health IT. "Data Provenance Environmental Scan." Presented at the HITPC Consumer Empowerment Workgroup Meeting. July 18, 2013. www.healthit.gov/FACAS/sites/faca/files/HITPC_ConsumerEmpowermentDataProvenance.pdf.
6. S&I Framework. "Data Provenance Initiative." http://wiki.siframework.org/Data+Provenance+Initiative.
7. Shapiro, Michael et al. "Patient-generated health data."
8. Ibid.

References

Deering, Mary Jo. "Issue Brief: Patient-Generated Health Data and Health IT." Office of the National Coordinator for Health IT. December 20, 2013. www.healthit.gov/sites/default/files/pghd_brief_final122013.pdf.

Dimick, Chris. "Governance Apples and Oranges: Differences Exist Between Information Governance, Data Governance, and IT Governance." *Journal of AHIMA* 84, no. 11 (November–December 2013): 60-62.

Vernessa Fountain (vernessa.fountain@cabanresources.com) is a HIM consultant at Caban Resources.

Article citation:
Fountain, Vernessa. "Using Data Provenance to Manage Patient-Generated Health Data" *Journal of AHIMA* 85, no.11 (November 2014): 28-30.