Trusting PHRs: The Standards That Protect the Security and Confidentiality of PHR-stored PHI

By Simone L. Pringle

To date most health information exchanges (HIEs) are sharing only institutional patient health data among providers, insurers, and pharmacies, and a minority of electronic health records (EHRs) support standards-based access to and from untethered personal health records (PHRs). However, there is a growing demand from patients who are accustomed to real-time information access and electronic service delivery in their daily lives.

The recent growth of patient-managed PHRs introduces new requirements for the security and confidentiality of protected health information (PHI) beyond the scope of what is expected for institutional data exchanges. PHRs and EHRs must rely on standards-driven approaches to allow patient access to the services they need in a secure manner that is consistent with patients' confidentiality concerns.

Several standards exist that organizations can implement to protect the security and confidentiality of PHR-stored PHI and enable patient choice in what information is disclosed.

Technical Standards for Security

For years, financial institutions have taken advantage of electronic security standards to support a customer's ability to download and consolidate his or her financial records. XML-based PHI models such as ASTM's Continuity of Care Record and HL7's Clinical Document Architecture and Continuity of Care Document make it possible to exchange an individual's health data using standardized mechanisms that ensure security and confidentiality.

Security standards and practices widely applied to health IT include:

- X.509 certificates for authentication and Security Assertion Markup Language (SAML) for authentication and authorization
- Encryption protocols such as the Transport Layer Security (TLS) and XML encryption
- Digital signatures that prevent tampering and ensure authenticity of electronic content
- Activity and transaction auditing that documents access to patient PHI

While it is possible to effectively use industry-agnostic standards to provide a baseline level of security to PHI exchanges, it is critical to recognize that healthcare workflows have unique requirements that must be considered when applying technical standards. In particular, patient participation introduces additional demands on the manner in which PHR software uses standards to properly secure a patient's PHI.

Supporting patient use of electronic health services can at times lead to situations where requirements may seem at odds with one another. For instance, consider the benefits of trusting portions of PHR-based data as originating from accredited medical sources, while at the same time supporting a patient's desire to control dissemination of certain types of information from his or her medical record.

Digital Signatures Add Reliability

Patients can increase the benefits they derive from the use of their PHRs by increasing provider confidence in the medical accuracy of the health record content.

Providers would be ill-advised, as a rule, to accept patient-sourced data without validation. Whether in electronic or paper form, providers understand that patients may incorrectly record, forget, omit, or otherwise misinterpret aspects of their medical

history. One might therefore be led to the incorrect conclusion that it is impossible for a PHR to supply information that a provider could ever treat as reliable.

While individuals may not be trusted to faithfully record and share medical records without loss or tampering, it is possible to deploy computerized systems that can by using digital signatures.

Digital signatures make it possible for providers to sign off on either the entirety or specific portions of the patient's medical record. Modifications to signed sections would invalidate the signature, flagging possible data tampering. The patient's PHR can thus become a trusted vessel of multisourced medical assessments-a historical collection of accredited medical opinions readily available for current providers.

The PHR must preserve the sections that are digitally signed. It can *reference* these sections as supporting material. For instance, a patient may document in his or her PHR a treatment that was recommended by a specialist and later confirmed by the second opinion of a different provider.

The PHR in this case would reference two digitally signed treatment records, one from each provider, while still making it possible for the patient to add his or her own annotations on the treatment.

While XML-based PHR standards can support the use of digital signatures, a successful solution cannot be implemented by PHRs alone. EHR systems must digitally sign provider-originated data, and the authenticity of digital signatures must be independently validated.

Interestingly, the granularity of the digital signature-whether it applies to the entire record or to individual subsections-may affect a patient's ability to reference medical sources, depending on whether the patient is selectively disclosing portions of his or her record.

Filters to Support Confidentiality

Patients can use their PHR-maintained data in multiple contexts, besides medical treatment. There are times when patients choose to omit or "filter out" sections of their PHI, perhaps for fear of losing their jobs or to avoid social stigma. De-identification is another example of filtering out information from one's PHI and is a recommended practice when sharing health data with untrusted systems.

While one might question the wisdom of omitting medical information in some circumstances, patients will inevitably control dissemination of the PHI they maintain in a manner they see fit. Patients have withheld disclosure of certain types of information from their health history long before the existence of electronic PHRs, primarily for privacy reasons.

Allowing a patient to filter out information on a configurable basis makes it possible for the patient's PHR to be a complete, consolidated record, while preserving the patient's confidentiality during data exchanges. Since the patient's PHR is complete, it is possible for the patient to maintain multiple filters to be applied as appropriate per the patient's wishes.

For instance, the PHR's confidentiality setting may indicate that, in cases of emergency, the complete medical record would be made available to medical staff, whereas in nonemergency circumstances, the patient chooses to omit sensitive data such as mental health history, AIDS-related treatments, or drug addictions.

Multiple mechanisms can be used to support PHI filtering, including high-level programming languages and XSLT, a standard for the transformation and manipulation of the content and structure of XML documents. Additional specifications such as OpenHealth Services (OHS) support a reusable, component-based approach to filtering, which makes it possible to decouple filtering from information exchange.

For instance, using OHS, it is possible for a patient to use the same reporting service to produce two separate medical history summary reports: one that is used with medical visits and another that filters out sensitive information.

Filtered PHI outputs must be implemented in a manner consistent with the use of digital signatures. For example, if a patient is omitting drug addiction information, the filtered PHI output must not contain a reference to a signed medical record with

information on rehabilitation treatment. Given that signed sections cannot be tampered with, the granularity of the provider's digital signature affects a patient's ability to reference a trusted medical source.

Secure Delivery of Electronic Health Services

Today's patients are more comfortable with information and service delivery technologies accessible from high-speed Internet, smartphones, and social networking sites. Patients' comfort with technology is changing patient-provider interactions.

E-mail is more commonplace, patients frequently search medical topics on the Web, and prescriptions are submitted online. Many PHRs have extended beyond healthcare support to include financial management of health expenses and wellness management.

The more patients use PHRs to participate in electronically delivered services, the greater the need to protect their identities and privacy, as well as secure their data from unwanted access.

An individual's health safety interests are better served by the ability to exchange and access pertinent health information in a timely manner. PHRs and EHRs should foster a collaborative environment where healthcare consumers have access to a wide variety of services.

Considerations for the use of standards and techniques should be guided by enabling individuals to maximize the benefits they derive from their interactions with providers in a manner that is consistent with and respectful of their personal choices.

Simone L. Pringle (simone@recordsforliving.com) is president of Records for Living.

Article citation:
Pringle, Simone L. "Trusting PHRs: The Standards That Protect the Security and Confidentiality of PHR-stored PHI" *Journal of AHIMA* 81, no.5 (May 2010): 40-41.