Developing Emergency Access Standards for EHR Systems: The HL7 Standards Development Process Helps (and Empowers) HIM Processes

by Reed Gelzer, MD, MPH, CHCC; Beth Acker, RHIA; and Sue Schneider, BA, CHIM

Many activities are under way to standardize electronic health records (EHR) systems. Among them are Health Level Seven's technical committees and special interest groups.

HL7 is an international standards development organization accredited by the American National Standards Institute. It has been instrumental in developing messaging standards for healthcare data. Through a continuous balloting and reconciliation process, the EHR technical committee has developed a model that defines basic functional standards for EHR systems.

However, the committee recognized that the first round of EHR requirements, released in early 2007, had gaps, including important functionalities that support basic records management. More specifically, US qualifications for legal admissibility were insufficient for EHRs to stand as legally valid business and clinical records. Follow-on work has addressed these needs.

One Standard Leads to Another

Organizations have addressed some areas such as signatures and amendments. For example, the Certification Commission for Healthcare Information Technology translates existing standards into requirements and testing protocols for verifying EHR capabilities. However, CCHIT currently does not include comprehensive requirements for a legally valid EHR. Finalization of pertinent additional HL7 standards will streamline and expedite uptake of these core EHR functions.

To this end, a subgroup under the EHR technical committee identified gaps in the functionalities, developed provisional requirements, and solicited extensive public comment. The HL7 Records Management and Evidentiary Support Profile Workgroup is completing the required HL7 process for review of public comments to provide an amended profile version for the subsequent steps toward eventual acceptance as part of an HL7 EHR standard.

Comments may lead to further, more in-depth review. One example is a requirement for means to, under extreme circumstances, use a secondary set of rules for protected health information (PHI) access and consent management.

Addressing Emergency Access

Access controls that support consent for clinical information are crucial in protecting patient privacy. All organizations will have a primary set of access rules that apply to the vast majority of PHI access activities. However, for defined special circumstances, a secondary rule set may be needed, often referred to as "break the glass."

Historically, the records manager or privacy officer has been the controlling entity for both ordinary and extraordinary access to the health record. As EHRs become more the norm, IT tools will offer improved governance of access controls.

The specific item in the HL7 records management and evidentiary support profile that spurred further discussion and investigation was the following:

> The system *shall* provide the ability for specified users to override the access control rules and request access to health information ("break the glass" functionality), record the reason for access and provide an administrative report.

The work group agreed that this language was too general. In the course of following up, the group found that "overriding access control roles," "requesting (extraordinary) access," and "recording reasons and generating reports" all would benefit from further elucidation. It also found that Canada has extensive experience with both standards development and with implementation challenges with this functionality.

Canada has aligned with European developments where in some places EHRs have been common for decades. From these resources, while improving the records management and evidentiary support profile, the group has identified a number of practical lessons likely to prove helpful to those relatively early in their institutions' EHR "careers."

Rules for Evaluating Organizational Policies

Lesson number one is that, in order to maintain a trustworthy healthcare information system, those organizations with individuals in health records compliance roles will not be entirely replaced by electronic gatekeepers anytime soon, if ever. Translating basic access principles into software functions approaches the very edge of technological capabilities. Future improvements will further open the way to dramatically improve security controls.

Meanwhile, as one author cautions, "We in healthcare need to include information security as part of our daily routine, and not as an afterthought as was the case in the past. It sometimes seems that the technology is not able to keep up with the fast-changing environment. Policies, procedures, and well-defined training programs can be used to fill gaps."[1]

Information security is a linchpin to all other values healthcare hopes to gain from IT, and so it must be embedded in policies and procedures and translated into proper training, use, and continuing improvement of systems tools. The healthcare industry must not dumb down security where technology has not yet developed to meet protection and accountability requirements. In the space between technology and requirements will stand the human gatekeeper. The health information manager or privacy officer is that gatekeeper.

With this in mind, organizations should review the following emergency access rules for evaluating their policies and procedures for rare events when there is enough time to access patient data that could improve outcomes but not enough time to follow the standard procedure for access. Organizations should:

1. Enable emergency access for clinical users only.
2. Evaluate the impact of emergency access on remote access (e.g., regional health, telehealth).
3. Provide a nonpermissive emergency access rule set with appropriately expedited access but with compensatory increased accountability. It is not an elimination of rules.
4. Limit access to specific users and for a defined time period. Access should be limited to a user profile level, including whether and how emergency access persists or requires renewal (extended time may allow reversion to use of primary access rules) and if and how emergency access may apply to an additional user group, such as mass casualty event triage roles.
5. Highly restrict emergency access and allow it on a very limited basis.
6. Require that, when initiated, the need for "break the glass" is documented from a pick list of policy-defined reasons for use.
7. Create automatically generated audit reports for each emergency access. Require evaluation and follow-up of each access, not react only upon investigation. The after-action review should be conducted by the HIM department or privacy officer with the emergency access initiator to provide cue training, mitigation if necessary, and ensure that it does not become semi-routine.
8. Require that more than one individual must take an action to initiate emergency access. Consider an administrative person in the secondary role.
9. Consider separate use case scenarios for different scales of extraordinary events (e.g., unconscious individual versus mass casualty event).

A Need for Oversight at the Technology Gaps

Ensuring proper PHI trustworthiness and protections will, for the indefinite future, require human oversight to make sure that rules don't get bent to accommodate the current state of technology. The rapid pace of technological change assures that

technical gaps will progressively close, and throughout, the "gatekeeper" must remain both watchful and proactive in developing and adapting oversight tools.

Furthermore, these topics will benefit from periodic review, analysis, and action, and, as HL7 found in its work, still need a greater degree of public discussion for at least two reasons:

- Since PHI access control is at the very heart of privacy and security concerns, more attention to special access requirements will accelerate improved enabling technologies.
- Narrowing but nonetheless persistent technology gaps will continue to require active oversight, protective advocacy, and operational involvement by human gatekeepers in the HIM department.

In other words, no one should give up the PHI keys to the machines just yet. Organizations must evaluate their policies and procedures for both primary and special-circumstance PHI access control; ensure preparedness for enforcing rules by whatever combination of technology and human intercession may be required; and maintain the inviolability principles we establish as absolutely, and without exception, necessary.

Note

1. Kurtz, Gary. "EMR Confidentiality and Information Security." *Journal of Healthcare Information* Management 17, no. 3 (2003): 47–48.

References

Canada Health Infoway. "Standards Collaborative Working Group (SCWG) 8—Privacy & IT Security Services." Available online at http://forums.infoway-inforoute.ca/PSCWG.

Connecting for Health. "Authentication of System Users." 2006. Available online at www.connectingforhealth.org/commonframework.

Connecting for Health. "Correctly Matching Patients with Their Records." 2006. Available online at http://connectingforhealth.org/commonframework.

Health Level Seven. "Electronic Health Record." Available online at https://www.hl7.org/ehr.

International Security, Trust, and Privacy Alliance. "Analysis of Privacy Principles: Making Privacy Operational." May 2007. Available online at www.istpa.org.

Office of the National Coordinator for Health Information Technology. "Emergency Responder—Electronic Health Record Detailed Use Case." December 2006. Available online at www.hhs.gov/healthit/usecases.

Acknowledgments

The authors thank Harry Rhodes for review and Katherine Ball and Don Simborg for "reality testing."

Reed Gelzer (rdgelzer@docintegrity.com) is COO of Advocates for Documentation Integrity and Compliance. Beth Acker (beth.acker@va.gov) is an HIM specialist with the Department of Veterans Affairs, Bay Pines Office. **Sue Schneider** (sschneider@thc.on.ca) is senior advisor data custodian with Trillium Health Centre in Mississauga, Ontario, Canada.

Article citation:
Gelzer, Reed D.. "Developing Emergency Access Standards for EHR Systems: The HL7 Standards Development Process Helps (and Empowers) HIM Processes" *Journal of AHIMA* 79, no.5 (May 2008): 52-53.