Security, Privacy, and Safety Standards in Canadian Healthcare

Save to myBoK

By Grant Gillis

In the large community of standards development organizations (SDOs) that are focused on healthcare and health informatics, the International Organization for Standardization (ISO) Technical Committee (TC) 215 Health Informatics (ISO/TC 215) is one of the leading forums. As mandated by ISO, the scope of ISO/TC 215 is broad:

> Standardization in the field of health informatics, to facilitate the coherent and consistent interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.[1]

Founded in 1998 and now covering such domains as architecture, frameworks and models, semantic content, security, safety, and privacy, ISO/TC 215 has more than 25 years invested in consensus building and requirements development. The committee has worked with public and private sector experts to enable the development of health information technology (HIT) standards. ISO/TC 215 now has more than 50 countries participating in and observing its standards development activities, and collaborates with 29 other ISO technical committees. It works closely with the International Electrotechnical Commission and International Telecommunication Union, and hosts the Joint Initiative Council, comprising various HIT standards development organizations, such as Integrating the Healthcare Enterprise (IHE), Health Level Seven (HL7), and the International Health Terminology Standards Development Organisation (IHTSDO).

ISO/TC 215 and Security, Safety, Privacy Standards

ISO/TC 215 standards play a vital role locally, nationally, and globally in facilitating the definition, collection, and availability of personal health information (PHI) in health information systems. It does this while protecting the security and privacy of PHI, and controlling authorized access by healthcare delivery organizations.

Since the inception of ISO/TC 215, Canada has been a strong participant and contributor to the committee's work, in part because of the important work that the committee does in the areas of information security, privacy, and safety standardization.

For these areas, ISO/TC 215's Working Group 4 Security, Safety and Privacy is dedicated to "standardization of methods and systems to protect and enhance the confidentiality, integrity and availability of health information, to prevent information systems from adversely affecting patient safety, to protect the privacy of PHI used in health and healthcare, and to ensure the accountability of users of health information systems."[2]

While developing an impressive body of requirements-based specifications of its own, ISO/TC 215's Working Group 4 also plays a fundamental role as facilitator and collaborator in the wider development of security, privacy, and safety standards with the International Electrotechnical Commission (IEC).

ISO Security, Safety, and Privacy Standards—The Canadian Experience

Distinctly, Canada has for many years organized its various health informatics standards engagements through the Standards Collaborative hosted by Canada Health Infoway. Bringing together such domains as architecture, information exchange, and terminologies, this organization facilitates a lifecycle-based approach to the standards-based electronic health record (EHR), including development, testing, implementation, maintenance, and conformance.

The Standards Collaborative has been particularly beneficial through its Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture. This robust, well-detailed scheme describes a secure systems design for EHRs in Canada. The conceptual architecture works to ensure that the privacy of patients is protected and that the confidentiality, integrity, and availability of their PHI is maintained in an ongoing fashion.

Within this conceptual architecture, ISO security, privacy, and patient safety standards play an important role in point-of-service solutions. For all provincial and territorial jurisdictions, as well as many crown agencies and commissions in healthcare, the standard "ISO/IEC 27799 Health Informatics – Information Security Management in Health Using ISO/IEC 27002" is widely recognized as the foundational standard for security for EHRs and all clinical and eHealth related solutions.

Based on the standard "ISO/IEC 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls," which is the international standard providing global guidance for any organization's information security standards and information security management practices, ISO/IEC 27799 provides more specific guidance in support of implementation of ISO/IEC 27002 in health informatics. In particular, ISO/IEC 27799 specifies the appropriate controls for the management of PHI, thereby sustaining a requisite level of security corresponding to an organization's circumstances and maintaining the confidentiality, integrity, and availability of PHI.

In conjunction with ISO/IEC 27799, many Canadian jurisdictions also use a variety of ISO/TC 215 security standards for their EHR requirements. For example, requirements from the standard "ISO/IEC 18028 Information Technology – Security Techniques – IT Network Security" have been used in many network environments to adapt and extend existing IT security management guidelines by specifying the necessary operations and mechanisms to implement network security safeguards and controls in a comprehensive manner.

Also, to help manage the growing need to audit accesses to PHI, the standard "ISO 27789 Health Informatics – Audit Trails for Electronic Health Records" specifies a common framework for audit trails for EHRs, in terms of audit trigger events and audit data, to keep the complete set of PHI auditable across information systems and domains. These ISO/TC 215 standards are supplemented by an array of security specifications from the IEC, HL7, as well as integration profiles from the IHE.

On the privacy side, the 10 principles as originally specified by the Organization of Economic Cooperation and Development (OECD) are closely followed as a national standard through "CAN/CSA-Q830 Model Code for the Protection of Personal Information." As a national standard of Canada, Q830 is incorporated in all domestic privacy legislation and regulation. The 10 core principles constitute the widely recognized national policy in protecting PHI in the healthcare environment in various settings.[3]

In further support of each jurisdiction's standards-based approach to privacy and security of PHI, COACH: Canada's Health Informatics Association publishes "Guidelines for the Protection of Health Information." The guidelines serve as a best practices resource to help the health sector protect the PHI they require to do their work and fulfill their professional responsibilities.

The guidelines cover topics such as:

- Requirements for consent for the collection, use, and disclosure of PHI
- Exceptions to consent requirements
- Requirements for reasonable safeguards for PHI
- How requirements apply to actors and stakeholders in the healthcare delivery space

The guidelines assist in the development of an overall privacy and security framework designed to support and sustain the proper use and protection of PHI. The 2013 Main Edition is supplemented by Special Editions covering access audits, privacy and security for patient portals, and EHR implementations.[4]

In the area of patient safety, ISO/TC 215 has been working on specifications addressing the safety of health software since 2006, with important publications centering on the classifications of safety risks involving health software (ISO Technical Specification/TS 25238), as well as measures for ensuring the patient safety of health software (ISO Technical Report/TR 27809). More recently, and with Canadian leadership, ISO/TC 215 published the standard "ISO Technical Report/TR 17791 Health Informatics – Guidance on Standards for Enabling Safety in Health Software."

Domestically, COACH has leveraged these standards and, working closely with colleagues in the US, the UK, Australia, and elsewhere, has published the "COACH eSafety Guidelines," a leading publication providing a method-based approach to ensuring the safety of electronic health IT systems (hence, "eSafety") in the larger context of patient safety. These guidelines apply across the healthcare spectrum, providing background information on eSafety and patient safety. They provide detailed recommendations on best practices and standards, checklists, templates, and much more.

Benefits of Security, Safety, and Privacy Standards

The benefits of standards that aim to ensure the security, safety, and privacy of PHI are extremely important for healthcare information systems development and professional competence. According to the Canada Health Infoway, a government created non-profit that works with the healthcare community, Canadian citizens, the government, and the technology industry to improve access to health information for better care, "good standards allow systems to interoperate seamlessly. Good standards encapsulate a great deal of knowledge and experience—some of it hard-won—and make it available to the architects of new systems. These standards make healthcare information networks possible. They protect the privacy of individuals without limiting their freedom of choice or compromising their security."[4]

For Canada and other nations, the work of ISO/TC 215, especially its security, safety, and privacy standards, is of very real value and will continue to serve as an important body of knowledge supporting healthcare professionals in ensuring the protection of PHI.

Notes

[1] International Organization for Standardization. "ISO/TC 215 Health Informatics."

[2] International Organization for Standardization. "ISO/TC 215 Health Informatics Business Plan Version 3." June 7, 2013.

[3] COACH: Canada's Health Informatics Association. *Guidelines for the Protection of Health Information: 2013 Edition*.

[4] Canada Health Infoway. "Electronic Health Record Infostructure (EHRi), Privacy and Security Conceptual Architecture. Version 1.1." June 2005.

Grant Gillis (ggillis@coachorg.com) is a member of the Canadian Standards Mirror Committee, ISO/TC 215 Health Informatics, and is executive director, forums and practices, with COACH: Canada's Health Informatics Association.

Article citation:
Gillis, Grant. "Security, Privacy, and Safety Standards in Canadian Healthcare" *Journal of AHIMA* 86, no.4 (April 2015): 44-46.