Managing PHI Content Standards

Save to myBoK

By Elaine Sawatsky and Diana Warner, MS, RHIA, CHPS, FAHIMA

Interoperability standards and their continuing adoption by e-health programs expand the capacity of information systems to capture, use, and exchange clinical data. For exchange to occur, the majority of data processing decisions need to take place both computationally and automatically. The latter requires data policies to be defined in ways that are themselves interoperable so that interactions between information systems and services delivered to a patient are consistent, and can support policy decisions regarding information management, including functions such as collection and capture, validation, storage, retrieval, exchange, disclosure, and use.

The Need for Standardized Consent

A fundamental aspect of health information sharing is the establishment of trust between the patient and healthcare provider. This trust is enabled by consent. The *Oxford Dictionary* defines consent as "permission for something to happen or agreement to do something; no change may be made without the consent of all the partners."

In the practice of medicine, "informed consent" is a fundamental bioethical concept. According to the *Miller Keane Encyclopedia and Dictionary of Medicine, Nursing, and Allied Health*, "Informed consent of a patient or other recipient of services based on the principles of autonomy and privacy has become the requirement at the center of morally valid decision making in healthcare, public health surveillance, and research." According to that definition, there are seven criteria that define informed consent:

1. Competence to understand and to decide
2. Voluntary decision making
3. Disclosure of material information
4. Recommendation of a plan
5. Comprehension of terms 3 and 4
6. Decision in favor of a plan
7. Authorization of the plan

A person gives informed consent only if all of these criteria are met. If all of the criteria are met except that the person rejects the plan, that person makes an informed refusal, according to the dictionary.

A patient who is not informed cannot provide meaningful consent and thus cannot develop a trusting relationship with the healthcare provider involved in his or her care. Consent that is not informed does not constitute valid consent. From the health information management (HIM) perspective, the provider also serves as a custodian of patient data. The health information custodian is the person who has been designated to be responsible for the care, custody, and control of the health record for such persons or institutions that prepare and maintain records of healthcare.[1]

The specific practices employed in obtaining and applying consent vary among jurisdictions and care settings because of differing legislation, patient visit types, and purposes of information use. To ensure uniformity, an effort is underway to globally align basic privacy principles and to establish a common understanding of the rights and expectations of individuals regarding how their health data should be used and shared. International alignment of consent practices is of growing importance as personal health data is communicated more frequently across organizational and jurisdictional boundaries for clinical care, research, and public health surveillance. To allow organizations to apply a fair and meaningful approach to the consent process, each organization or jurisdiction's choice of approach must meet a combination of ethical, legal, and practical requirements.

A New Standard for Information Management

A new standard was recently published by the International Standards Organization (ISO) Technical Committee (TC) 215 Health Informatics entitled “ISO 17975 Technical Specification (TS), Health informatics–Principles and data requirements for consent in the collection, use, or disclosure of personal health information.”[2] This standard describes the content frameworks and data requirements to enable information management by a custodian of patient data based on the individual’s consent to collect, use, or disclose his or her personal health information (PHI). Please note that in the context of this standard, the term “disclose” also encompasses the information exchange. The standard requires “privacy policies to be defined in ways that are themselves interoperable, so that interactions between heterogeneous systems and services are consistent from a security perspective and supportive of policy decisions regarding the processing of PHI.”

The following can be used as a definition for personal health information. Information about an identifiable person that relates to their physical or mental health, or to the provision of health services may include: [3]

1. Information about the registration of the individual for the provision of health services
2. Information about payments or eligibility for healthcare with respect to the individual
3. A number, symbol, or particular code assigned to an individual to uniquely identify the individual for health purposes
4. Any information about the individual that is collected in the course of the provision of health services to the individual
5. Information derived from the testing or examination of a body part or bodily substance
6. Identification of a person (i.e., a healthcare professional) as provider of healthcare to the individual

The standard is based on two international agreements. The first, the “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” was developed by the Organization for Economic Cooperation and Development (OECD) and forms the basis for legislation in many countries.[4] The second agreement, the “Declaration of Helsinki,” defines best practices in informational consent management.[5] Informational consent management refers to the collection, use, disclosure (to include exchange), or any data processing activities of personal information. This also includes the denial, constraints, or conditions that the individual may place on those activities.

The ISO 17975 standard has been created to address varying approaches to consent management and to support the automated flow of patients’ data. It defines “informational consent” as a form of authorization provided by the individual to allow or deny the collection, use, or disclosure of personal health information. The standard supports all interactions related to the flow of patient data and is applicable across all encounters regardless of frequency or scale of access, use, and disclosure. The informational consent conforms to privacy, security, and information management policies. The standard does not specify the legal requirements of jurisdiction, nor is it meant to challenge or support legislation or to mandate the adoption of any particular consent framework.

The latter includes the set of agreements and constraints that apply to the collection, use, or disclosure as well as the process whereby the information is managed, according to the agreement or constraint. The standard defines four informational consent frameworks:

- Express or expressed (informed) consent
- Implied (informed consent)
- No consent sought
- Assumed (deemed) consent

This standard specifies requirements common to all these frameworks for international alignment. The consent frameworks can be used by those who wish to obtain agreement from individuals in order to process their PHI.

The informational consent process is described in a record of the informational consent. Characteristics of the process record include: consent is given by individual or representative, the individual is informed, the consent is obtained voluntarily, and the consent is applied to relevant information processing activities both by collector or user and discloser. The process record is made available to those who wish to use the data or to whom the same information is later disclosed. When the request and disclosure is done without human intervention, these process characteristics can be used as part of an automated negotiation between health information systems in order to follow the consent agreement regarding the processing and exchange of information. Automatic requests would look at the consent parameters in the informational consent record and release information based on these parameters.

The ISO 17975 standard also defines requirements for: explicit and implied consent frameworks; opt-in and opt-out practices; situations in which it might not be feasible or necessary to obtain consent; and consent directives that inform decisions and support the automation of policy services, including the consent process record parameters described above. The consent frameworks facilitate compliance with legal, ethical, and information governance-based requirements to support electronic organizational practices that enable information systems to handle personal data as permitted and intended.

The standard can be used to inform the discussion of consent policies as well as the ways in which individuals and the public are informed about how PHI is processed. It can be used in the design of both paper and electronic consent forms and the design of privacy policy and security services that regulate access to personal health data. It supports the creation of appropriate working practices of those organizations and staff that obtain or use the consent for the processing of PHI.

The classification of informational consent frameworks as described by the standard can be used in conjunction with the two other ISO standards to support interoperability and automated decision making related to privilege management and data flows. Those standards are "ISO 22600:2014, Health informatics—Privilege management and access control—Parts 1–3" and "ISO/TS 14265:2011, Health Informatics — Classification of purposes for processing personal health information."

For example, an organization might apply a framework that combines implied informed consent for routine healthcare service delivery with one that requires more explicit (but also informed) consent for non-healthcare purposes of use, such as research or public health surveillance. By using these standards, the organization ensures that purposes to which data is captured, and for which data is disclosed, is done in a way with which the patient agrees, and that meets ethical and legal requirements.

The ISO 17975 standard can be used by healthcare organizations, regional health authorities, jurisdictions, and countries as an aid to the consistent management of information in the delivery of healthcare services and the communication of electronic health records across organizational and jurisdictional boundaries.

To participate in the development of international standards for privacy, security, and safety of health information at ISO Technical Committee 215 Health Informatics, contact Diana Warner at diana.warner@ahima.org.

Notes

[1] AHIMA e-HIM Work Group on Defining the Legal Health Record. "The Legal Process and Electronic Health Records." *Journal of AHIMA* 76, no. 9 (October 2005): 96 A-D [expanded online version]. http://bok.ahima.org/doc?oid=59559.

[2] International Organization for Standardization 17975 Technical Specification. "Health informatics – Principles and data requirements for consent in the collection, use or disclosure of personal health information." September 15, 2015. www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61186.

[3] International Organization for Standardization. "27799:2008 Health informatics – Information security management in health using ISO/IEC 27002." July 1, 2008. www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41298.

[4] Organization for Economic Cooperation and Development. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." 2013. www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[5] World Medical Association. "Declaration of Helsinki—Ethical Principles for Medical Research Involving Human Subjects." www.wma.net/en/30publications/10policies/b3/.

Elaine Sawatsky (elaine.sawatsky@telus.net) is a privacy consultant at E. Sawatsky and Associates Inc. Diana Warner (diana.warner@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Sawatsky, Elaine; Warner, Diana. "Managing PHI Content Standards" *Journal of AHIMA* 87, no.4 (April 2016): 38-41.

Driving the Power of Knowledge