

Standards Category: Privacy and Security Standards

Privacy and Security Standards are aimed to ensure information security, privacy and confidentiality.

Important Terms

*Adapted from the Institute of Medicine publication, “Disposition of the Air Force Health Study,” 2006.

SECURITY refers to physical, technological, or administrative safeguards or tools used to protect identifiable health information from unwarranted access or disclosure. Security is the set of actions an organization takes to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.*

PRIVACY is an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.*

CONFIDENTIALITY refers to the obligations of those who receive information to respect the privacy interests of those to whom the information relate. It is an organization’s responsibility to protect identifiable health information obtained in providing, or as a result of, a service.*

CYBERSECURITY is the ability to protect or defend the use of cyberspace from cyber attacks. Source: Committee on National Security Systems Instruction (CNSSI). CNSSI-4009

Privacy and Security standards are developed by Standards Development Organizations (SDOs).

Privacy and Security Standards			
Standard Development Organizations		Domains	Website
ASTM	American Standards for Testing and Materials	Security, Confidentiality	https://www.astm.org/
IHE	Integrating the Healthcare Enterprise	Patient Consent, Anonymization/Pseudonymization, Access Control	https://www.ihe.net/
ISO	International Organization for Standardization	Methods to Protect Security, Confidentiality and Privacy of Personal Information in eHealth Applications including Consent, Access Control, Pseudonymization, Workforce Development	https://www.iso.org/committee/54960.html

Resources

Orlova A. Health Information Technology Standards and Systems Interoperability Course. *Suarez W. Lecture 10: Privacy and Security Standards.* Johns Hopkins School of Public Health (JHSPH) OpenCourseware. Johns Hopkins University. URL: <http://ocw.jhsph.edu/index.cfm/go/viewCourse/course/InfStandards/coursePage/index/>

Standards Category: Privacy and Security Standards

ISO Technical Committee 215 Health Informatics (ISO/TC215)

Established in 1998, **International Organization for Standardization, Technical Committee 215, Health Informatics (ISO/TC215)** has over 70 member countries and liaison organizations representing millions of healthcare stakeholders worldwide. **The ISO/TC215 mission is *standardization in the field of health informatics to facilitate the capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.***

The **US delegation** at ISO/TC215 is represented by the **Technical Advisory Group (ISO/TC215 USTAG)** – a committee accredited by American National Standards Institute – that develops US national positions on international standards. Since 2011 AHIMA provides Secretariat to ISO/TC215 and serves as Administrator to the USTAG at ISO/TC215.

ISO/TC215 develops international standards for semantic (shared content), technical (shared infrastructure) and functional (shared rules) interoperability. ISO/TC215 product portfolio contains **over 200 standards** including those under development. Privacy and security standards are part of technical interoperability standards portfolio.

ISO/TC 215 Privacy and Security Standards Examples

(IS – International Standard, TS – Technical Specification, TR – Technical Report)

ISO Number	Title
ISO/TR 11633	Information security management for remote maintenance of medical devices and medical information systems
ISO/TS 13606-4	Electronic health record communication -- Part 4: Security
ISO/TS 14441	Security and privacy requirements of EHR systems for use in conformity assessment
ISO/IS 17090-4	Public key infrastructure -- Part 4: Digital Signatures for healthcare documents
ISO/IS 17090-5	Public key infrastructure -- Part 5: Authentication using Healthcare PKI credentials
ISO/TS 17975	Principles and data requirements for consent in the collection, use or disclosure of personal health information
ISO/TR 18638	Guidance on health information privacy education in healthcare organizations
ISO/TS 21547	Security requirements for archiving of electronic health records -- Principles
ISO/TR 21548	Security requirements for archiving of electronic health records -- Guidelines
ISO/IS 22600	Privilege management and access control
ISO/IS 25237	Pseudonymization
ISO/IS 27799	Information security management in health using ISO/IEC 27002
<i>Under Development</i>	
ISO/TR 21332	Cloud computing considerations for health information systems security and privacy
ISO/TR 22696	Guidance for an identification and authentication framework of networked personal health devices
ISO/TR 22697	Application of privacy management to personal health information

Resources

ISO/TC215 Standards and Projects Catalog: <http://www.ahima.org/~media/AHIMA/Files/AHIMA-and-Our-Work/ISOTC215StandardsCatalog2017.ashx?la=en>

ISO/TC215 Website at ISO: <https://www.iso.org/committee/54960.html>

ISO/TC215 Website at AHIMA: <http://www.ahima.org/about/global?tabid=ISO>