TECHNICAL REPORT

ISO/TR 18638

First edition
2017-06

Health informatics — Guidance on health information privacy education in healthcare organizations

Informatique de santé — Composantes éducatives destinées à garantir la confidentialité des informations relatives à la santé

Reference number
ISO/TR 18638:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviations ... **7**

5 Understanding information privacy in healthcare ... **7**
5.1 General concept ... 7
5.2 Information privacy in healthcare ... 8
5.2.1 Personal health information and privacy ... 8
5.2.2 Patient's rights on personal health information privacy ... 8
5.3 Privacy concerns ... 9
5.4 Organization's privacy protection program ... 9
5.4.1 Policies and practices to protect health information ... 9
5.4.2 Roles of workforce in protecting information privacy ... 10
5.4.3 Workforce education in protecting health information privacy ... 11
5.4.4 Patient's education in protecting information privacy ... 11

6 Information privacy education in healthcare ... **11**
6.1 General concepts ... 11
6.2 Target audience of the privacy education ... 12
6.3 Competencies, educational objectives and content ... 12

7 Examples of content modules ... **16**
7.1 General ... 16
7.2 Introduction to information privacy, confidentiality and security in healthcare ... 16
7.3 International guidelines and principles for information privacy protection ... 16
7.4 National legislation, regulation and policies for information privacy protection ... 16
7.5 Patient's rights on personal health information ... 17
7.6 Administrative policies for privacy protection ... 17
7.7 Technical and physical safeguards for protecting healthcare information privacy ... 18

8 Instructional methods, delivery mechanisms and evaluation ... **19**
8.1 Instructors ... 19
8.2 Instructional methods and delivery mechanisms ... 19
8.3 Delivering training ... 19
8.3.1 Orientation and on-boarding training ... 19
8.3.2 Continuing education ... 20
8.3.3 Education of patients ... 20
8.4 Evaluation methods ... 20

Annex A (informative) **ISO/TC215 Health informatics: List of standards on privacy protection** ... **21**

Annex B (informative) **Setting learning objectives (example) (Source: Triage Training Group, HIPAA training playbook)** ... **22**

Annex C (informative) **Level of Learning Objectives by Audience (Provided by South Korea)** ... **24**

Annex D (informative) **Educational methods (examples)** ... **26**

Annex E (informative) **Questions for quiz for privacy education (example) (Provided by South Korea)** ... **27**

Bibliography ... **32**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

Health information privacy concerns need to be addressed with the expanding adoption of health information technology (HIT) including the use of electronic health record (EHR) systems. Both the increasingly legislated environment around privacy and the increasing need for information sharing between patients, providers, payers, researchers and administrators contribute to the growing need for information privacy education in the healthcare sector. In spite of increasing awareness of and sensitivity to patient privacy, there are no guidelines or standardization for education on privacy of the healthcare information within healthcare organizations.

The purpose of this document is to describe the essential educational components recommended to ensure health information privacy in a healthcare organization. This document describes the concepts of health information privacy, the components of a privacy education program for healthcare organizations and basic health information privacy educational content that can be applied to various jurisdictions.

This document provides guidance for healthcare organizations for establishing and improving the health information privacy education for their workforce.

Annex A provides the list of standards published by ISO/TC 215 that may be used to develop privacy education in healthcare organizations as they convey specific content and approach health information privacy protection.

Health informatics — Guidance on health information privacy education in healthcare organizations

1 Scope

This document specifies the essential educational components recommended to establish and deliver a privacy education program to support information privacy protection in healthcare organizations. The primary users of this document are those responsible for planning, establishing, and delivering healthcare information privacy education to a healthcare organization.

This document provides the components of privacy education within the context of roles and job responsibilities. It is the responsibility of the organization to define and apply privacy protection policies and procedures and, in turn, ensure that all staff in the healthcare organization understands their privacy protection responsibilities.

The scope of this document covers:

a) the concept of information privacy in healthcare;

b) the challenges of protecting information practices in the healthcare organization;

c) the components of a healthcare information privacy education program;

d) basic health information privacy educational content.

2 Normative references

There are no normative references for this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
access
ability or means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resources

[SOURCE: ISO/TR 18307:2001, 3.1]

3.2
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[SOURCE: ISO 17090-1:2013, 3.2.1]

3.3
anonymization
process by which *personal identifiable information (PII)* (3.21) is irreversibly altered in such a way that a *PII principal* (3.22) can no longer be identified directly or indirectly, either by the *PII controller* (3.23) alone or in collaboration with any other party

Note 1 to entry: See *pseudonymization* (3.33).

[SOURCE: ISO/IEC 27038:2014, 2.1, modified]

3.4
asset
anything that has value to the organization

Note 1 to entry: There are many types of assets, including:

a) information;

b) software, such as a computer program;

c) physical, such as computer;

d) services;

e) people, and their qualifications, skills and experience, and

f) intangibles, such as reputation and image.

[SOURCE: ISO/IEC 27000: 2014, 3.6]

3.5
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

[SOURCE: ISO/IEC 29110-2-1:2015, 4.7]

3.6
availability
property of data or of resources being accessible and usable on demand by an authorized entity

Note 1 to entry: This is the definition relevant to use in computer security.

[SOURCE: ISO/TS 27790:2009, 3.10]

3.7
confidentiality
property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes or other entities

[SOURCE: ISO/IEC 2382:2015, 2126249]

3.8
control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature

Note 1 to entry: Control is also used as a synonym for safeguard or countermeasure.

Note 2 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 3 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27000:2016, 2.16]

3.9
education
knowledge, skill and understanding that you get from attending a school, college, university or vocational teaching

Note 1 to entry: The action or process of teaching someone especially in a school, college, or university.

Note 2 to entry: A field of study that deals with the methods and problems of teaching.

Note 3 to entry: Synonyms are learning, knowledge, literacy, scholarship and enlightenment

Note 4 to entry: Education (which is concept based) is different than *training* (3.39) (which is skill based).

3.10
healthcare
type of services is provided by professionals or paraprofessionals with an impact on health status

[SOURCE: ISO 27799:2016, 3.3]

3.11
healthcare organization
organization involved in the direct or indirect provision of healthcare services to an individual or to a population

[SOURCE: ISO 13606-1:2008, 3.33]

3.12
health professional
person who is authorized by a recognized body to be qualified to perform certain health duties

Note 1 to entry: The defined term is often “healthcare professional”.

[SOURCE: ISO 27799:2016, 3.5]

3.13
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity

[SOURCE: ISO 22857:2013, 3.7]

3.14
information privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 14441:2013, 3.26]

3.15
information security
protection of information from (accidental or intentional) unauthorized access, use, disclosure, disruption, modification or destruction

[SOURCE: ISO/TS 21547:2010, 3.2.24]

3.16
media
means by which information is perceived, expressed, stored or transmitted

EXAMPLE Audio, video, (animated) graphics, images, text.

Note 1 to entry: Medium (plural media).

[SOURCE: ISO/IEC 14478-1:1998, 3.2.2]

3.17
patient
subject of care consisting of one person

[SOURCE: ISO 13606-2:2008, 4.13]

3.18
personal information
information about an individual which can be used to identify that individual

Note 1 to entry: The specific information used for this identification will be that defined by national legislation.

Note 2 to entry: See *personal identifiable information (PII)* (3.21).

[SOURCE: ISO/IEC 27011:2008, 3.1.5]

3.19
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

[SOURCE: ISO 27799:2016, 3.8]

3.20
personal health record
PHR
representation of information regarding or relevant to the health, including wellness, development, and welfare of a subject of care, which may be stand-alone or integrating health information from multiple sources, and for which the individual, or their authorized representative, manages and controls the PHR content and grants permissions for access by and/or sharing with other parties

[SOURCE: ISO/TR 14639-2:2014, 2.60]

3.21
personal identifiable information
PII
information about a person that can be used to identify that individual

Note 1 to entry: The specific information used for this identification will be that defined by national legislation.

Note 2 to entry: See *personal health information* (3.19) and *pseudonymization* (3.33).

[SOURCE: ISO/IEC 27011:2008, 3.1.5]

3.22
personal identifiable information principal
PII principal
person who granted/entrusted an organization with the ability to manage his/her PII

Note 1 to entry: See *pseudonymization* (3.33).

3.23
personal identifiable information controller
PII controller
person designated by an organization to control access to PII

Note 1 to entry: See *pseudonymization* (3.33).

3.24
policy
set of rules such as legal, political, organizational which can be expressed as obligations, permissions or prohibitions

Note 1 to entry: Adapted from ISO/TS 22600-1:2014, 3.13.

[SOURCE: ISO/TR 14639-1:2012]

3.25
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[SOURCE: ISO/TS 27790:2009, 3.56]

3.26
privacy in healthcare
right of an individual to keep oneself and one`s health information concealed or hidden from unauthorized access and view by others that rests on the principle of confidentiality between healthcare providers and patients

3.27
privacy breach
situation where *personal information* (3.18) is collected, accessed, used or disclosed in an unlawful manner or in violation of one or more relevant privacy policies

[SOURCE: ISO/TS 17975:2015, 3.26]

3.28
privacy manager
individual designated as a privacy official, who manages personal information directly or via another person as part of his/her duties, who is responsible for developing and implementing its privacy policies and procedures or a contact person or contact office responsible for receiving complaints and providing individuals with information on the healthcare organization's privacy practice

3.29
privacy protection
capacity to control when, how and to what degree information about oneself is communicated to others

3.30
privacy stakeholders
individuals involved in *privacy protection* (3.29) including *PII principal* (3.22), *PII controller* (3.23), *privacy manager* (3.28) and other defined by the national regulation

3.31
procedure
specified way to carry out an activity or a process

[SOURCE: ISO 30000:2009, 3.12]

3.32
provider
person or organization that is involved in or associated with delivery of health care to a subject of care, or caring for the well-being of a subject of care

Note 1 to entry: A provider in this context includes not only healthcare providers, but also those directly involved in the provision of services to patients.

Note 2 to entry: The defined term is often "healthcare professional". A convention has been adopted in this document whereby the term "healthcare" is abbreviated to "health" when used in an adjectival form. When used in a noun form, the word "care" is retained but as a separate word (e.g. delivery of health care).

[SOURCE: ISO/TS 27527:2010, 3.6]

3.33
pseudonymization
process applied to *personal identifiable information (PII)* (3.21) which replaces identifying information with an alias

Note 1 to entry: Synonym is reduction, masking.

Note 2 to entry: Pseudonymization can be performed either by *PII principals* (3.22) themselves or by *PII controllers* (3.23). See PII, PII principal and PII controller.

Note 3 to entry: Pseudonymization can be employed by PII principal to consistently use a resource or service without disclosing his/her identity to this resource or service (or between services), while still being held accountable for that use.

Note 4 to entry: Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII principle controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

[SOURCE: ISO/IEC 29100:2011, 2.24]

3.34
review
verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to the fulfilment of specified requirements by an object of conformity assessment

[SOURCE: ISO/TS 14441:2013, 3.44]

3.35
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 10377:2013, 2.16]

3.36
risk management
coordinated activities to direct and control an organization with regard to *risk* (3.35)

[SOURCE: ISO/TS 16901:2015, 3.32]

3.37
subject of care
one or more persons scheduled to receive, receiving, or having received a health service

[SOURCE: ISO/TS 18308:2011, 3.47]

3.38
threat
potential cause of an unwanted incident that may result in harm to a system or organization

3.39
training
process by which someone is taught the skills that are needed for an art, profession or job

Note 1 to entry: The action of teaching a person or animal a particular skill or type of behaviour.

Note 2 to entry: The action of undertaking a course of exercise and diet in preparation for a sporting event.

Note 3 to entry: Exercise, exercises, working out, conditioning.

Note 4 to entry: See *education* (3.9).

3.40
workforce
people who provide a service or labor to contribute to business or organizational outcomes

[SOURCE: ISO 30409:2016, 10.1]

4 Abbreviations

EHR	electronic health record
EN	European Norm (Standard)
EU	European Union
HIT	health information technology
ID	identification
ICT	information and communication technology
OECD	Organization for Economic Cooperation and Development
PHI	personal health information

5 Understanding information privacy in healthcare

5.1 General concept

The internet and emerging health information and communication technologies are changing the way that health professionals and the public gain access to health information, resulting in an expectation for the increased use of such information. Although personal health information is personally private data, such information may be used for public health, clinical research, medical education, policy making, legislation enforcement, accreditation and other purposes for the betterment of society. Healthcare organizations should develop a comprehensive approach to enable adequate protection of health information privacy for their patients. Workforce education regarding health information privacy should be an integral part of this approach including guidance on when and how health information should be protected with regards to the specific workforce roles.

Privacy education in a healthcare organization is a set of educational resources tailored to the roles of the workforce involved in the creation, management, sharing, use and re-use of health information. The education should be built upon agreed international concepts and standards on the topic of information privacy, in general, and health information privacy, specifically. Jurisdictional legislation should be considered in the design and implementation of organizational policies and the procedures of the privacy protection program as well as being an educational component of such a program. Educational requirements need to be inclusive of local settings and legislation. Furthermore, these requirements should consider information privacy and healthcare goals in the context of clinical care and other information use.

5.2 Information privacy in healthcare

5.2.1 Personal health information and privacy

Health information contains unique sensitivity characteristics in terms of privacy. Personal health information includes wide range of patient demographics including name, identification numbers, address, phone number, education, marital status, socio-economic status and other individually identifiable data points. Personal health information also includes data about physical and mental health status, provision of healthcare services to a subject of care or payment for healthcare services provided to a subject of care. It is collected or created in the context of scheduling delivery or payment for a healthcare service including:

a) registration and identity verification of the individual for the provision of healthcare services;

b) information about the individual that is collected or created during the provision of healthcare services to the individual;

c) information about the workforce involved in the provision of healthcare services to the individual;

d) results derived during the provision of healthcare services to the individual including test or examination results, medications prescribed and other.

Such information may be considered sensitive by the person to whom it relates.

Personal health information may be shared with multiple providers involved in the provision of healthcare services to the individual. In addition, this information can be re-used for a wide array of purposes, such as clinical research, public health, training and other health related activities.

Personal health information that is collected during the delivery of healthcare services is recorded in health records. It can reside in various media including paper records, electronic records, mobile applications, films, specimens, etc. This information is collected, maintained, transmitted, stored, used and re-used by workforce involved in the healthcare delivery. Therefore, it is the responsibility of the healthcare organization as well as its workforce to protect privacy of health information for the patients.

5.2.2 Patient's rights on personal health information privacy

According to the 2002 guidelines on the protection of privacy and trans-border flows of personal data from the Organization of Economic Cooperation and Development (OECD), privacy is the right of an individual to keep oneself and one's information concealed or hidden from unauthorized access and view by others. Patients' rights for privacy of health information include:

a) right to access and obtain personal health information in a readable form and format;

b) right to permit access or disclosure before personal health information can be used and shared for specified purposes (except where otherwise permitted by legislation);

c) right to correct or amend personal health information if an individual believes the information is incorrect, incomplete or inaccurate;

d) right to receive confidential communication;

e) right to file a complaint if an individual believes rights are being denied or health information is not being protected properly;

f) right to delegate personal health information access and/or retrieval to a third party.

5.3 Privacy concerns

Privacy concerns regarding personal health information, whilst not new, are a major issue for healthcare organizations. As organizations have been increasingly sharing information electronically, the risk of patient health information being accessed by unauthorized persons or being used for unauthorized purposes by those with legitimate access raises concerns that information privacy breaches might lead to information misuse or abuse with consequences ranging from embarrassment, financial loss, discrimination and legal consequences.

5.4 Organization's privacy protection program

Privacy protection refers to the capacity to control when, how and to what degree information about oneself is communicated to others. An organization's privacy protection policies and practices are aimed to guard patient's health information. These policies and practices form the basis of organization's privacy protection program.

An organization's privacy protection program should be designed to protect patient rights with respect to information privacy and should be developed and implemented within the framework of the relevant jurisdictional laws. The program should specify:

a) policies and practices to protecting patient's privacy within an organization;

b) specific roles of the workforce involved in collection, management, sharing, use and reuse of patient health information;

c) education of workforce regarding privacy protection policies and practices;

d) education of patients regarding their right in health information privacy.

5.4.1 Policies and practices to protect health information

Information protection policies and practices performed by the workforce of a healthcare organization ensure that:

a) all uses of information are known and appropriate in accordance with jurisdictional laws;

b) health information is protected from inadvertent or deliberate misuse or disclosure;

c) health information collection, sharing and storing are legally permitted and justified;

d) patients are informed about their rights regarding health information;

e) patients are informed why, when and how their health information is collected, shared and stored prior to the beginning of collection of their information;

f) patients can expect that their data is protected by information privacy protection program;

g) patients are informed about their right to access their healthcare information.

As a part of the privacy protection program, the organization should maintain reasonable and appropriate administrative, technical and physical safeguards to prevent intentional or accidental use or disclosure of personal health information which may violate jurisdictional privacy legislation. This includes limiting incidental use and disclosure pursuant to otherwise, permitted or required use or disclosure of the information; as well as appropriate use of patient consents and directives regarding

information capture, management, sharing, use and re-use. Education of workforce is critical part of the organization's privacy protection program.

5.4.2 Roles of workforce in protecting information privacy

An organization's privacy protection program's policies and practices are carried out by workforce involved in managing patient health information in various roles. The roles of the workforce fall into the following groups:

a) health professionals;

b) healthcare information managers;

c) administrative staff;

d) researchers;

e) IT, security and privacy workforce;

f) other workforce involved in patient's care;

g) other workforce that support operation of healthcare organization.

Table 1 presents the roles of workforce in protecting health information privacy by group.

Table 1 — Roles of workforce in protecting health information privacy in healthcare organization

Group	Roles
Health professionals	Individuals who provide healthcare services, such as physicians, nurses, allied health professionals, medical technicians and other directly involved in the generation, sharing and use of information within the episode of care to support care delivery. They are also involved in establishing organizational policies and procedures related to care delivery using clinical guidelines and best practices.
Health information managers	Individuals such as medical record staff and others who maintain health records created during the care delivery. They are involved in the collection, access, validation, verification, codification, audit, protection, retention, storage and disposition of information, i.e. support of the information lifecycle within an organization. They support information management for the provision of direct care, as well as information exchange/sharing including the release of information (disclosure) to the authorized users. In addition, they participate in planning, implementation and operation of information systems including EHR and ancillary systems that contain health information. They are also involved in establishing healthcare information management (HIM) policies and procedures for the health information lifecycle, including policies and procedures for protecting information privacy.
Administrative staff	Individuals who use healthcare information for non-clinical administrative duties including an organization's operation and financial management, business decision-making to support tasks related to operational policy development and evaluation. They may be employees of the healthcare organization as well as business associates, e.g. contractors that perform operational, non-clinical services.
Researchers	Individuals who use healthcare information for research purposes, e.g. clinical research, population health surveillance, monitoring of health risks, health services utilization research and others. They may be involved in the development of educational materials for care delivery and disease prevention for health care provider and patients as well as the development and delivery of health education to health professionals including health information managers.

Table 1 *(continued)*

Group	Roles
IT, security and privacy workforce	Individuals who implement and support the operation of health information systems and applications to enable electronic collection, management, sharing and use of healthcare information. Such individuals may include those who have specific roles in information security and information privacy.
Other workforce involved in patient care	Outsourcing agents, contractors, pastoral care workers, counselors, volunteers, social workers, students and others who may be involved in healthcare delivery and information management services.
Other workforce that support organization's operation	Sanitation workers, guards, maintenance technicians and others who provide daily operational support to the healthcare organization. They are not directly involved in patient care and are not allowed to access patient records. However, as employees of healthcare organization they need to be aware about general organizational policies regarding information privacy protection of patients.

To ensure the protection of patient rights for information privacy, an organization may establish a committee of representatives from these workforce groups to define and implement organizational policies and procedures as well as specific responsibilities of each group in privacy protection. This committee, in turn, may define specific educational content, training formats and periodicity for each of these groups of workforce as described in 5.4.3 and 5.4.4.

5.4.3 Workforce education in protecting health information privacy

Organization's privacy protection program's policies and practices contribute to a privacy culture and help form the basis of privacy education for the workforce involved in information creation, management, use and re-use. Education should help workforce to ensure the protection of patient rights for information privacy. Clause 6 provides guidance regarding workforce's education in protecting health information privacy in a healthcare organization.

5.4.4 Patient's education in protecting information privacy

Prior to collection of health information, the patient and/or his/her legal representative should be informed about why, when, with whom and how their personal health information is shared, used and re-used. The patient and/or his/her legal representative have to express via consent directives, why, when, with whom and how personal health information may be shared, used and re-used. Therefore, an organization's privacy protection program should include an educational component for patients and/or their legal representatives on how patient information privacy is protected by the organization. This includes execution of consent directives. Clause 6 provides guidance for privacy education.

6 Information privacy education in healthcare

6.1 General concepts

Healthcare organizations have an obligation to educate their workforce, business partners and stakeholders as well as patients and/or their legal representatives themselves regarding health information privacy protection. Health information privacy education should be an integral part of the overall healthcare organization workforce training. It should be based on international and jurisdictionally-relevant educational standards, ethics and core competencies on privacy protection tailored to the applicable legislation and organizational policies and procedures. Privacy education can be delivered through existing organizational educational programs or as a specialized program of its own.

The healthcare organization should maintain and update the privacy education curriculum as needed according with the changes in privacy protection technology and standards. It is important to keep educational materials up to date and ensure that workforce renew their training periodically according to the organizational policy for the workforce continuing education. The organization should also document evidence of workforce compliance with the privacy protection policies and practices as well as retain proof of such compliance.

6.2 Target audience of the privacy education

The target audience for health information privacy education includes the seven groups of organization's workforce as described in Table 1. These consist of six groups (groups 1 to 6) who are involved in managing patient healthcare information and group 7 who are involved in the general support of the organization's operation.

In addition, health information privacy education should be delivered to patients or their legal representatives.

6.3 Competencies, educational objectives and content

According to the Global Academic Curricula Competencies for Health Information Professionals (2015), privacy education should be aimed at the overall information protection including data privacy, confidentiality and security. The central theme of these competencies is that information is viewed as a strategic organizational asset that requires high level oversight in order to be able to effectively use it for safe care delivery, organizational decision-making, performance improvement, cost management and risk mitigation. From these perspectives, workforce of the organization as well as its customers (patients) carries out specific roles and responsibilities in protecting health information privacy.

Annex B provides detailed description and examples of setting learning objectives under the four levels of comprehension as follows:

a) awareness;

b) understanding;

c) practice;

d) habit.

In general, the academic educational objectives are to assure that trainees

— understand applicable healthcare law, regulation and standards related to information protection from the perspectives of various stakeholders;

— be able to develop and implement related privacy, security and confidentiality organizational policies;

— be able to develop and maintain an organizational infrastructure on information protection including privacy protection;

— be able to educate stakeholders on health information protection methods and their responsibilities.

Though the Global Competencies were developed for the academic education, they may be applicable to vocational (on-the-job) training at the healthcare organizations as well. Thus, overall educational objectives of the privacy education in a healthcare organization are aimed to enable workforce to:

a) understand the concepts of patient's information privacy, confidentiality and the recommended safeguards to protect that information;

b) understand the importance of patient's privacy protection;

c) understand the relationship between information privacy and information security in a continually changing healthcare environment;

d) recognize potential threats to patient privacy;

e) acquire knowledge of legal, administrative, technical and physical safeguards for privacy protection;

f) learn effective approaches for protecting patient privacy in relation to patient information;

g) understand the actions required to safeguard personal health information;

h) understand the roles of workforce in protecting patients' privacy when managing patient information;

i) apply knowledge obtained in item a-h above in protecting information privacy on the job.

The specific types of training modules, the depth and the degree of comprehension upon training completion for each workforce's group depend on the role and responsibilities with regards to access, management, sharing, use and re-use of the patient information.

Table 2 presents examples of the competencies themes as well as curriculum considerations that should be tailored to a specific role of the workforce's group described above in Table 1.

Table 2 — Privacy education: Examples of the competences themes and curriculum considerations

Competencies themes	Curriculum considerations
Foundational concepts	
Patient's rights to privacy and access to health information	— Patient rights to privacy standards, laws and regulations — Patients' rights to access
The concept of physician/patient confidentiality and how it demands privacy and security measures to protect health information	— Physician/patient relationship — Trust — Comfort — Confidentiality — Safeguards (disclosures, HIPAA, Hippocratic Oath, etc.) — Physical and automated/electronic Privacy and security safeguards (passwords, pins, accessibility, physical safeguards)
Information exchanges in healthcare	— Local, regional, national and international health information exchanges — Patient-generated data, personal health records — Patient safety — Health information systems interoperability (semantic, technical and functional) — Information availability, quality, integrity and protection
Practice of health information protection; legal concepts, principles and document	— Health information/record laws and regulations — Healthcare legal terminology — Information protection, transparency, compliance — Patient consents: (a) consent for treatment, retention, privacy, patient rights, advocacy, health power of attorney, advance directives, etc. and (b) consent for information sharing — Legal health record — Electronic discovery (e-Discovery)

Table 2 *(continued)*

Competencies themes	Curriculum considerations
Information access and disclosure of confidential health information	— Principles for releasing personal health information — Consent for information sharing — Permitted disclosure without authorization — Re-disclosure — Required elements of an authorization — Designated record set — Institutional Review Boards (IRBs) — Tracking disclosures
Confidentiality, privacy and security measures, policies and procedures for data capture, management, exchange, use and re-use to protect health information privacy (regardless of format)	— Information protection — Professional obligations related to privacy protection of health information — Internal and external standards, regulations, and initiatives on health information privacy — Patient verification — Medical identity theft — Data security concepts, processes and monitoring — Administrative, physical and technical safeguards
Retention and destruction policies for health information	— Information retention — Data storage and retrieval — Information archival, data warehouses — Incident reporting
Security and privacy policies for departmental and organizational information management practices	— Information protection — Data breaches — Privileged communications — Policies for authorized users — Security processes and policies — Systems quality and data quality
Policies and procedures to manage access and disclosure of confidential health information	— Privacy and security laws and regulations — Systems integration, interfaces and data reliability — Information security measures, policies and procedures — Risk assessment, evaluation and management — Business continuity planning — Audit techniques and principles — Principles for releasing PHI — Required elements of an authorization — Designated record set — IRBs — Re-disclosure — Tracking disclosures — Encryption/electronic access — Anonymization and pseudonymization — Systems quality and data quality

Table 2 *(continued)*

Competencies themes	Curriculum considerations
Risks to health information privacy and management of breaches of policies/procedures and protocols	— Local, regional, national and international health information exchanges — Information protection — Case risk analysis, management and mitigation — Breach analysis and notification requirements — Gap analysis of current policies and procedures
Record and system disaster recovery and management protocols and procedures	— Patient safety — Contingency planning — Downtime policies, procedures and processes — Systems quality and data quality
Additional educational components for employees in information privacy, security and confidentiality	— In-service programs for employees — Code of Ethics — Organizational policies and procedures

Privacy education should be developed as a part of the overall organizational privacy protection program. Specific training modules may be developed at the institutional level as well as they may be aimed at a specific target group and/or role/functional level of participants in the target group (see Table 1). When developing the educational content for a specific group of workforce, the following recommendations may be considered.

— Develop educational materials and training formats using best educational practices, e.g. Global Competencies described above.

— Focus on examples (cases) relevant to the organization at large as well as to specific roles and responsibilities of the workforce involved.

— Choose attention-getting themes, e.g. patient-centered focus.

— Use appropriate outside resources.

To ensure continuity of the privacy education as a part of the organizational culture, the following practices should be pursued.

a) Focus on training as part of risk reduction strategy to ensure continuing awareness of the staff with what is protected information.

b) Conduct continuing awareness campaigns to provide organizational reinforcement including surveys of organization's staff including contractors as well as patients as follows:

   1) surveys of workforce to assess their knowledge about the privacy protection efforts within the organization;

   2) surveys of patients to assess their satisfaction with the privacy protection efforts within the organization.

c) Provide feedback to staff on both staff and patients' surveys.

d) Identify champions of privacy protection awareness, offer awards, incentives or both.

e) Update educational modules as needed based on the feedback from the staff and patient/client surveys.

7 Examples of content modules

7.1 General

Training overview, learning objectives, expectations, and administrative matters.

Sections that follow provide specific examples of educational modules that should be included in a privacy education program built from the global competencies described in Table 2.

7.2 Introduction to information privacy, confidentiality and security in healthcare

a) Definitions of information privacy, confidentiality and security in healthcare;

b) Current and future trends of eHealth:

   1) Health information and communication technology (HICT) in healthcare;

   2) Health information exchanges: local, regional, national and international;

   3) International and national standards for HICT systems interoperability and information sharing.

c) Patient information privacy protection: legislation, policies, guidance, principles and best practices;

d) Threats to patient information privacy in eHealth environment;

e) The role and responsibility of a healthcare organization in protecting privacy of patient health information:

   1) Risks to patient information privacy in an organization;

   2) Mitigations of risks in protecting patient information privacy including reporting a privacy violation incident;

   3) Administrative, technical and physical security safeguards to protect patient information privacy;

   4) Consequences for violations of safeguards for patient information privacy.

7.3 International guidelines and principles for information privacy protection

These international guidelines and national laws play a major role in assisting healthcare organizations and consumer representatives in their efforts to protect health information privacy and personal data. Examples of international and national regulations include:

a) OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data;

b) United Nations Guidelines for the Regulation of Computerized Personal Data Files;

c) European Union Data Protection Directive (Directive 95/46/EC).

7.4 National legislation, regulation and policies for information privacy protection

National regulation and guidelines on information privacy protection. For example:

a) Australian Privacy Protection Principles;

b) US Health Insurance Accountability and Portability Act (HIPAA), 1996.

7.5 Patient's rights on personal health information

a) Patient's rights on personal health information

b) Organizational policies and procedures to protect patient's information privacy

   1) Notice of information privacy

   2) Confidential communications

   3) Access to information

   4) Amendments to correct information in the record

   5) Access or amendment refusal

   6) Consents

   7) Request forms to access personal health information

   8) Complaints

7.6 Administrative policies for privacy protection

a) Patient`s rights on the use, access to and disclosure of personal health information within an organization (compliance with applicable legislation, regulation and policies)

b) Job responsibilities and patient information

c) Collection, use and disclosure of personal health information including information provenance (additions, modifications, disclosures)

   1) Categories of personal health information to which access is needed

   2) Authorized workforce to access and manage personal health information

   3) Verification of authority and identity of individuals requesting personal health information

d) Patient consents

   1) Explicit and implied consent

   2) Consent for procedure

   3) Consent for information sharing

   4) Consent withdrawals

   5) Exclusions and exceptions

e) Record retention and destruction

f) Privacy breaches

   1) Unauthorized collection of personal health information

   2) Unauthorized disclosure of personal health information

      i) loss (a file is misplaced)

      ii) theft (a laptop is stolen), or

      iii) mistake (a letter addressed to one person gets faxed to the wrong person)

   3) Unauthorized access

4) Unauthorized or unsecured disposal of personal health information

g) Privacy policies violations

1) Disciplinary actions including termination of employment

2) Fines

3) Criminal charges

h) Documentation of organizational policies and procedures

i) Workforce training

7.7 Technical and physical safeguards for protecting healthcare information privacy

a) Information security threats

1) Human errors, e.g. erasure, accidental damage, deliberate acts, improper disposal of data

2) Natural disasters, e.g. fire, flood, lightning, earthquake, etc.

3) Technical errors, e.g. lack of back up, system failure, malware, loss of power, etc.

4) Deliberate errors, e.g. unauthorized disclosure, modification, information leaks, etc.

5) Media handling

b) Technical safeguards

1) Network security

2) Access management

i) ID and password management

ii) Photo and Biometrics IDs

iii) Access logs

iv) Screen saver

3) Data encryption and secure transmission

4) Data back-up

c) Physical safeguards

1) Facility access control (locks, electronic access control systems, security workforce)

2) Designated physical storage locations

3) Electronic storage devices and equipment

4) Equipment/workstation security and theft protection at the facility and in transit

5) Media protection from theft at the facility and in transit

6) Workspace security

7) Protection from natural disaster

Annex C provides comparison of the levels of learning objectives (1 - Awareness; 2 - Understanding; 3 - Practice; 4 - Habit) by workforce groups described in Table 1, including patient or legal representative, with respect to specific content modules/topics in educational curricula.

8 Instructional methods, delivery mechanisms and evaluation

8.1 Instructors

Instructors should have in-depth conceptual and practical knowledge of

a) the subject of protecting individual's privacy in healthcare;

b) jurisdictional regulation and organizational policies regarding maintaining patient privacy and confidentiality;

c) information security and its role in protecting personal information;

d) national and international HIT standards used in health information systems and applications to protect personal information.

Qualifications and eligibility criteria for instructors should be determined by jurisdictional legislation and organizational policies. For example, instructors should have experience in enterprise information management and healthcare administration as well as possess basic knowledge of teaching skills. Instructors should develop and deliver educational sessions under the supervision of a privacy program committee and a designated person responsible for the implementation, management and enforcement of privacy protection program in the healthcare organization.

8.2 Instructional methods and delivery mechanisms

Depending on the audiences' roles and responsibilities, prior education, working experience and knowledge, a variety of instructional methods may be used to address the specific learning objectives of the privacy education program in order to meet the needs and desired outcomes for the identified target group.

Various training delivery mechanisms may be used including traditional face-to-face classes, online e-learning, and/or a combination of both. Instructional methods should take into account the characteristics of the various delivery mechanisms, training methods and the capabilities of the target audience as elaborated in Annex D.

It is important to vary the instructional methods to keep the target audience's interest and allow them to interact with the content in a variety of ways, e.g. videos, role play, animation, etc.

8.3 Delivering training

Privacy education may be included in staff orientation and on-boarding and sustained through associated continuing education. When delivering the training, the following administrative practices should be pursued.

a) Set up the appropriate training format and schedule for the affected workforce.

b) Document attendance.

c) Document training completion by issuing certificate or acknowledgement documents.

d) Grant access to patient health information only after completion of the training.

e) Make information privacy education a precondition for any credentialing processes.

8.3.1 Orientation and on-boarding training

Orientation and on-boarding training should address the basic knowledge of

a) patient health information;

b) patient's information privacy rights;

c) how health information privacy is protected in a healthcare organization including the legal aspects and responsibilities of the workforce in protecting patient information privacy;

d) specific job responsibilities of the employee in his/her position with regard to protecting health information privacy in a healthcare organization.

In addition, other organizational policies and practices regarding to the management of patient healthcare information may be added to the on-boarding training as needed based on the person's role including patient consents, confidentiality agreements and information security statements; their periodic renewal according to the jurisdictional regulation and organizational policies; and other topics.

8.3.2 Continuing education

For continuing education, more detailed information regarding specific topics may be included in the periodic training sessions based on the person's role within the organization and expanded educational content from the specific competencies and educational modules provided above.

8.3.3 Education of patients

In addition to educating workforce, the organization have to develop and delivery educational materials to patients and/or their legal representatives. The educational format may include booklets, posters, interactive videos and mobile applications, etc. describing how patient's privacy is protected and explain the patient's role in protecting privacy of his/her information. It is important to develop these materials at a level to be understood by a lay audience, e.g. at the 3rd-4th grade reading level or using drawings and cartoons for the audience that may not know how to read.

It is important to include patient's education in workforce training because clinicians, information managers and other workforce may likely deliver these educational materials to the patients.

8.4 Evaluation methods

Evaluation of the effectiveness of the privacy education program depends on the organizational need and available resources. There are a series of steps that help learners understand how to apply knowledge obtained during the training. The competency-based learning approach allows trainees to demonstrate mastery and provides for personalized learning opportunities.

The training should include tasks, exercises, quizzes, surveys, exams and other techniques to access learner's knowledge gained through the completion of the training. Annex E presents the examples of quizzes under privacy education.

For further improvement of the training content and delivery, it is important to solicit continuing feedback from workforce as well as patients via surveys on the quality of privacy education, e.g. training topics, materials, format, etc. so the improvement could be timely made as needed.

Annex A
(informative)

ISO/TC215 Health informatics: List of standards on privacy protection

ISO Document Type, Number and Year	Title
ISO/TS 25237:2008 (Ed 1)	Health informatics — Pseudonymization
ISO/TR 11633-1:2009 (Ed 1)	Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis
ISO/TR 11633-2:2009 (Ed 1)	Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 2: Implementation of an information security management system (ISMS)
ISO/IS 22600-1:2014 (Ed 1)	Health informatics — Privilege management and access control — Part 1: Overview and policy management
ISO/IS 22600-2:2014 (Ed 1)	Health informatics — Privilege management and access control — Part 2: Formal models
ISO/TS 22600-3:20014(Ed 1)	Health informatics — Privilege management and access control — Part 3: Implementations
ISO/TS 21547:2010 (Ed 1)	Health informatics — Security requirements for archiving of electronic health records — Principles
ISO/TR 21548:2010 (Ed 1)	Health informatics — Security requirements for archiving of electronic health records — Guidelines
ISO/TS 14265:2011 (Ed 1)	Health informatics — Classification of purposes for processing personal health information
ISO/TS 13606-4:2009	Health informatics — Electronic health record communication — Part 4: Security
ISO/TS 14441:2013 (Ed 1)	Health informatics — Security and privacy requirements for compliance testing of EHR systems — Part 1: Foundation
ISO/IS 22857:2013 (Ed 2)	Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data
ISO/IS 20301 (Ed 2)	Health informatics — Health cards — General characteristics
ISO/IS 20302:2014 (Ed 2)	Health informatics — Health cards — Numbering and issuer identification
ISO/IS 17090-4:2014 (Ed 1)	Health informatics — Public key infrastructure — Part 4: Digital signatures for healthcare documents
ISO/IS 22600-1:2014 (Ed 1)	Health informatics — Privilege management and access control — Part 1: Overview and policy management
ISO/IS 22600-2:2014 (Ed 1)	Health informatics — Privilege management and access control — Part 2: Formal models
ISO/IS 22600-3:2014 (Ed 1)	Health informatics — Privilege management and access control — Part 3: Implementations
ISO/TS 17975:2015 (Ed 1)	Health informatics — Principals and data requirements for consent in the collection, use or disclosure of personal health information
EN-ISO/IS 27799:2016 (Ed 2)	Health informatics — Information security management in health using ISO/IEC 27002
ISO/IS 27789:2013 (Ed 1)	Health informatics — Audit trails for electronic health records

Annex B
(informative)

Setting learning objectives (example) (Source: TriageTraining Group, HIPAA training playbook)

Level 1 Awareness: Knowledge from facts and data

The purpose of this level is to develop familiarity with the subject matter (learn concepts and terms). The demonstration of knowledge includes the ability to recall or recognize concepts.

In terms of learning objectives, some verbs that are common to this level are: show, label, collect, examine, tabulate, quote, name, recall, recognize, reproduce, select, state, list, match and outline.

Level 2 Understanding: Comprehension from instruction

The purpose of this level is to understand the meaning and interpretation of instructions. The learner should be able to state a problem in his/her own words. A demonstration of understanding includes the ability to recall and explain in different words, knowledge of the major ideas, understand information, grasp meaning, compare and contrast.

In terms of learning objectives, some verbs that are common to this level are: comprehend, contrast, defend, define, describe, differentiate, discuss, distinguish, estimate, explain, extend, generalize, interpret, paraphrase, predict, rewrite, summarize and translate.

Level 3 Practice: Application and analysis

At this level, people begin to use information such as methods, concepts and theories in new situations. They begin to solve problems using acquired skills, notice patterns and organize information. They can recognize hidden meanings and identify components. A demonstration includes using a concept in a new situation or giving an example. The learner can separate the information into its component parts so that the structure may be understood and can distinguish between facts and inferences. The learner can also apply what was learned in the classroom into new situations in the workplace.

In terms of learning objectives, some verbs that are common to this level are: analyse, apply, calculate, categorize, change, compose, complete, demonstrate, design, discover, examine, experiment, illustrate, modify, plan, produce, relate show and solve.

Level 4 Habit: Judgment, ethics and wisdom from synthesis and evaluation

The learner at this level is able to demonstrate a complete understanding of the information and can use old ideas to create new ones, relate knowledge from several areas, predict and draw conclusions, compare and discriminate between ideas, assess the value of the theories and presentations and make choices based on arguments. The demonstration of this level includes building a structure or pattern from diverse elements, putting parts together to form a whole, with emphasis on creating a new meaning or structure or making judgments about the value of ideas or materials.

In terms of learning objectives, some verbs that are common to this level are: assess, combine, conclude, convince, criticize, critique, decide, defend, evaluate, formulate, integrate, interpret, invent, judge, rank, recommend, support and test.

Table B.1 and Table B.2 provide examples of setting learning objectives regarding personal health information and new security policy for computer password management. Please note that the level of learning objective depends on the workforce role and responsibilities. For example, health information managers (see Table 1, group 2) who work directly with personal health information should be trained at level of Practice up to level of Habit.

Table B.1 — Learning objectives: Meaning of personal health information

Learning objective	
Level	**Description**
Awareness	Identify the definition of personal health information.
Understanding	Describe forms of personal health information that you come in contact with.
Practice	Decide whether the information asked for by a family member is personal health information and if it can be shared with the family.
Habit	Evaluate the actions of new staff members regarding their use and disclosure of personal health information.

Table B.2 — Learning objectives: Proper actions regarding password management

Learning objective	
Level	**Description**
Awareness	Recall your organization's policy on computer security password management.
Understanding	Explain in your own words the meaning and importance of computer security password management.
Practice	Apply the password management policy to your daily work.
Habit	Assess how your organization's policy protects patients' rights.

Annex C
(informative)

Level of Learning Objectives by Audience (Provided by South Korea)

Table C.1 provides metrics for comparison of the levels of learning objectives described in Annex A (1 - Awareness; 2 - Understanding; 3 - Practice; 4 - Habit) by workforce groups (see Table 1) as well as patient or legal representative with respect to specific topics in educational curricula.

Table C.1 — Metrics for comparison of the levels of learning objectives

Curricula topics	Health professionals	Health information managers	Admin. staff	Researchers	IT staff	Others involved in care	Others supporting operation	Patient or legal representative
7.1 Training overview, learning objectives, expectations and administrative matters	4	4	3	2	2	1	0	0
7.2 Introduction to information privacy, confidentiality and security in healthcare	4	4	4	4	4	4	4	1
7.3 International guidelines and principles for information privacy protection	4	4	3	3	4	1	0	0
7.4 National legislation, regulation and policies for information privacy protection	4	4	4	4	4	4	1	1
7.5 Patient's rights on personal health information	4	4	4	4	4	4	1	2
7.5 b) 1) Notice for information privacy	4	4	3	3	3	1	0	2
7.5 b) 2) Confidential communications	4	4	3	3	3	2	0	2
7.5 b) 3) Access to information	4	4	3	3	3	1	0	2
7.5 b) 4) Amendment	4	4	3	3	3	1	0	2
7.5 b) 5) Access or amendment refusal	4	4	3	3	3	1	0	2
7.5 b) 6) Consent	4	4	3	3	3	1	0	2
7.5 b) 7) Request forms to access personal information	4	4	3	3	3	1	0	2
7.5 b) 8) Complaint	4	4	3	3	3	1	0	2
7.6 Administrative policies for privacy protection								
7.6 a) Patient's rights on the use, access to and disclosure of personal health information within the organization: Organizational policy and procedure and compliance with applicable legislation, regulation and policies	4	4	3	3	4	1	1	1

Table C.1 *(continued)*

Curricula topics	Health professionals	Health information managers	Admin. staff	Researchers	IT staff	Others involved in care	Others supporting operation	Patient or legal representative
7.6 b) Job responsibilities and patient information	4	4	3	3	4	2	1	1
7.6 c) Collection, use and disclosure of personal health information including information provenance (additions, modifications, disclosures)	4	4	2	3	3	2	0	2
7.6 d) Patient consent	4	4	2	3	2	2	0	2
7.6 e) Record retention and destruction	4	4	3	3	4	2	1	2
7.6 f) Privacy breaches	4	4	3	3	4	2	1	2
7.6 g) Privacy policies violation	4	4	3	3	4	2	1	2
7.6 h) Documentation of organizational policies and procedures	4	4	4	4	4	4	4	2
7.6 i) Workforce training	4	4	4	4	4	4	4	0
7.7 Technical and physical safeguards for protecting health information privacy								
7.7 a) Information security threats	3	4	3	3	4	1	0	0
7.7 b) 1) Technical guards: network security	3	3	3	2	4	1	0	0
7.7 b) 2) Technical guards: Access management (IS and password management, screen saver)	4	4	4	3	4	1	0	1
7.7 b) 3) Technical guards: Data encryption and secure transmission)	3	3	3	3	4	1	0	0
7.7 b) 4) Technical guards: Data back-up	3	3	3	3	4	0	0	0
7.7 c) 1) Physical Guards: Facility access control	4	4	4	3	4	2	2	1
7.7 c) 4) Physical Guards: Equipment/workstation security	4	4	4	3	4	2	2	1
7.7 c) 5) Physical Guards: Media handling	4	4	4	3	4	2	2	1
7.7. c) 7) Physical Guards: Protection from natural disaster	4	4	4	3	4	2	2	1

Annex D
(informative)

Educational methods (examples)

A variety of methods may be employed to address the specific learning objectives for the target audience. Training methods and schedules should meet the learners' needs.

Examples of methods are:

a) case study;

b) discussion of issues;

c) scenarios or role play;

d) computer-based training;

e) videotaped instruction;

f) interactive technology;

g) handouts, audiovisuals, references, self-study information;

h) briefings and lectures;

i) reviews during performance evaluations;

j) network (e-mail) briefings.

Training can be delivered on both traditional (in-class) as well as in on-line formats. Table D.1 presents characteristics for the two training formats.

Table D.1 — Characteristics of training delivery formats for privacy education

Characteristics	Traditional (in-class) training	Online training
Training format	Lectures, seminars	Recorded lectures, interactive webinars
Number of participants	Over 30 persons - Lecture Less than 20 persons - Seminar	Unlimited
Type of participants	Groups of workforce with similar roles and responsibilities	
Frequency	Defined by organizational policies	
Learning objectives level	Based on workforce group roles and responsibilities	
Grading criteria of trainees	Grade for participation or grade based on merit upon completion of assignments	
Course evaluation	Survey of trainees and other type of feedback to the instructor to assess and strengthen the education content as needed	
Course updates	Modification of education content based on the results from course evaluation according to the schedule set by the organizational policies	