

PD CEN ISO/TS 14441:2013

Incorporating corrigendum February 2014



BSI Standards Publication

Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This Published Document is the UK implementation of CEN ISO/TS 14441:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 85785 0

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 December 2013.

Amendments/corrigenda issued since publication

Date	Text affected
28 February 2014	Implementation of CEN correction notice 18 December 2013: CEN Endorsement Notice inserted

English Version

Health informatics - Security and privacy requirements of EHR systems for use in conformity assessment (ISO/TS 14441:2013)

Informatique de santé - Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité (ISO/TS 14441:2013)

Medizinische Informatik - Sicherheits- und Datenschutzerfordernungen für die Konformitätsprüfung von EGA-Systemen (ISO/TS 14441:2013)

This Technical Specification (CEN/TS) was approved by CEN on 7 April 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

This document (CEN ISO/TS 14441:2013) has been prepared by Technical Committee ISO/TC 215 “Health informatics” in collaboration with Technical Committee CEN/TC 251 “Health informatics” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 14441:2013 has been approved by CEN as CEN ISO/TS 14441:2013 without any modification.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	9
5 Security and privacy requirements	9
5.1 General	9
5.2 Theoretical foundation	9
5.3 Privacy and security requirements	12
5.4 Common Criteria	28
6 Best practice and guidance for establishing and maintaining conformity assessment programs	30
6.1 Concepts	31
6.2 Conformity assessment processes	33
Annex A (informative) Conformity assessment programs — Design considerations and illustrative examples from member countries as of 2010	36
Annex B (informative) Comparison of jurisdictional requirements	54
Bibliography	112

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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.

ISO/TS 14441 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

As local, regional and national EHR infostructures develop, electronic patient record systems are being implemented at the many points of care where patients are seen [point-of-service (POS) clinical systems]. In addition to institutional settings like hospitals, where the systems in various departments (e.g. nursing units) are typically integrated into a single patient record, smaller single purpose systems such as electronic medical records (EMRs) are also being implemented in physician offices and other non-institutional settings such as public health where the sophistication of the systems and the local IT support infrastructure is much less. As countries begin to connect these POS clinical systems to EHR infostructures (or directly exchange clinical information with other POS clinical systems through system-to-system communications), the security and privacy of these systems becomes much more critical and complex than when the systems operated in a disconnected or 'stand-alone' state. To ensure the required standards are implemented correctly into these systems, so that they will securely interact with EHR infostructures and maintain the privacy of patient information, many countries are implementing certification and conformance testing programs to provide objective evidence of conformity with these requirements.

This Technical Specification identifies the security and privacy requirements, harvested from the above mentioned standards and international experiences, which should be in place for conformance testing for interoperable POS clinical (electronic patient record) systems interfacing with EHRs.

The POS clinical systems profiled receive, store, process, display and communicate clinical data and administrative actions, as well as information related to system users (demographics, personal).

The systems are always accessed by authorized and authenticated users. These users are:

- health professionals that input, access and use patient data, clinical procedures, and statistics;
- administrative users that input and read patient's personal and demographics data, administrative and statistical information;
- administrators that control users power, perform backups, provide system configuration, including security ones;
- auditors that read audit trails;
- other EHR systems that input and receive data;
- subjects of care and their substitute decision makers, who may have restricted access to input and retrieve authorized data.

Key assumptions that apply for compliant POS clinical systems are as follows:

- the Target of Evaluation (TOE) comprises commercial off the shelf (COTS), governmental, proprietary and free and open source software;
- authenticated users recognize the need for a secure IT environment;
- authenticated users can be trusted to comply with the organization's security policy;
- business security processes are implemented with due regard for what can (and cannot) be reasonably accomplished in a clinical setting;
- competent security administration is carried out in relation to the system's installation and ongoing operations.

This Technical Specification draws from international standards, which have been developed by ISO/TC 215 for EHRs, as well as other ISO standards such as such as ISO/IEC 27001 and the ISO/IEC 17000 series of standards developed by the ISO Committee on conformity assessment (CASCO). This Technical Specification also reflects the experience that various countries have had to date in implementing certification and conformance testing programs in addressing privacy and security requirements in the

context where electronic patient record (clinical) systems at the point of care are interoperable with regional and national EHRs.

This Technical Specification includes:

- security and privacy requirements that should be met to ensure that information is protected as well as the main categories of attack;
- discussion of the theoretical foundations underpinning the requirements;
- guidance on best practice for establishing and maintaining conformity assessment programs;
- description of the conformity assessment process, including the key concepts and processes.

[Annex A](#) provides more detailed information on conformity assessment models and processes, plus examples of conformity assessment programs in four example countries at a point in time (2010).

[Annex B](#) provides a detailed examination of the privacy and security requirements in place in five jurisdictions at the time that this Technical Specification was written. This analysis was used to derive the security and privacy requirements in [Clause 5](#).

This Technical Specification is to be used by agencies which accredit or operate programs for certifying health software products through conformity assessment against privacy and security standards, software suppliers demonstrating their compliance with those requirements, and purchasers of those systems who want assurance that the requirements have been met.

Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment

1 Scope

This Technical Specification examines electronic patient record systems at the clinical point of care that are also interoperable with EHRs. Hardware and process controls are out of the scope. This Technical Specification addresses their security and privacy protections by providing a set of security and privacy requirements, along with guidelines and best practice for conformity assessment.

ISO/IEC 15408 (all parts) defines “targets of evaluation” for security evaluation of IT products. This Technical Specification includes a cross-mapping of 82 security and privacy requirements against the Common Criteria categories in ISO/IEC 15408 (all parts). The point-of-service (POS) clinical software is typically part of a larger system, for example, running on top of an operating system, so it must work in concert with other components to provide proper security and privacy. While a Protection Profile (PP) includes requirements for component security functions to support system security services, it does not specify protocols or standards for conformity assessment, and does not address privacy requirements.

This Technical Specification focuses on two main topics:

- a) Security and privacy requirements ([Clause 5](#)). [Clause 5](#) is technical and provides a comprehensive set of 82 requirements necessary to protect (information, patients) against the main categories of risks, addressing the broad scope of security and privacy concerns for point of care, interoperable clinical (electronic patient record) systems. These requirements are suitable for conformity assessment purposes.
- b) Best practice and guidance for establishing and maintaining conformity assessment programs ([Clause 6](#)). [Clause 6](#) provides an overview of conformity assessment concepts and processes that can be used by governments, local authorities, professional associations, software developers, health informatics societies, patients’ representatives and others, to improve conformity with health software security and privacy requirements. [Annex A](#) provides complementary information useful to countries in designing conformity assessment programs such as further material on conformity assessment business models, processes and other considerations, along with illustrative examples of conformity assessment activities in four countries.

Policies that apply to a local, regional or national implementation environment, and procedural, administrative or physical (including hardware) aspects of privacy and security management are outside the scope of this Technical Specification. Security management is included in the scope of ISO 27799.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*

ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

3 Terms and definitions

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

3.1 **accountability**

principle that individuals, organizations, and the community are responsible for their actions and may be required to explain them to others

[SOURCE: ISO 15489-1:2001, definition 3.2]

Note 1 to entry: This requires that all users of PHI be traceable.

3.2 **access control**

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

[SOURCE: ISO/IEC 2382-8:1998, definition 08.04.01]

3.3 **accreditation body**

authoritative body that performs accreditation

Note 1 to entry: The authority of an accreditation body is generally derived from government.

[SOURCE: ISO/IEC 17000:2004, definition 2.6]

3.4 **anonymization**

process that removes the association between the identifying data set and the data subject

[SOURCE: ISO/TS 25237:2008, definition 3.2]

3.5 **asset**

anything that has value to the organization

Note 1 to entry: In the context of health information security, information assets include health information, IT services, hardware, software, communications facilities, media, IT facilities, and medical devices that record or report data.

Note 2 to entry: Adapted from ISO/IEC 27000:2012, definition 2.4.

3.6 **assurance**

result of a set of compliance processes through which an organization achieves confidence in the status of its information security management

3.7 **attestation**

issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated

Note 1 to entry: The resulting statement, referred to in this Technical Specification as a “statement of conformity”, conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees.

Note 2 to entry: See also scope of attestation.

Note 3 to entry: Adapted from ISO/IEC 17000:2004, definition 5.2.

3.8 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

Note 1 to entry: While “audit” applies to management systems, “assessment” applies to conformity assessment bodies as well as more generally.

[SOURCE: ISO/IEC 17000:2004, definition 4.4]

3.9 availability

property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2012, definition 2.10]

3.10 certification

third-party attestation related to products, processes, systems or persons

Note 1 to entry: Adapted from ISO/IEC 17000:2004, definition 5.5.

3.11 compliance

the action of doing what is necessary to meet a specified requirement

3.12 confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989, definition 3.3.16]

3.13 conformity assessment

demonstration that specified requirements relating to a product, process, system, person or organization are fulfilled

Note 1 to entry: Adapted from ISO/IEC 17000:2004, definition 2.1.

3.14 conformity assessment system

rules, procedures and management for carrying out conformity assessment

Note 1 to entry: Conformity assessment systems may be operated at international, regional, national or sub-national level.

[SOURCE: ISO/IEC 17000:2004, definition 2.7]

3.15 data subject

person to whom data refer

Note 1 to entry: In this Technical Specification, a data subject refers to a single person (versus persons).

3.16 entity

natural or legal person, public authority or agency or any other body

Note 1 to entry: In the context outside the scope of this Technical Specification, an entity may refer to a natural person, animal, organization, active or passive object, device or group of such items that has an identity.

3.17

first-party conformity assessment activity

conformity assessment activity that is performed by the person or organization that provides the object

Note 1 to entry: See also second-party conformity assessment activity, and third-party conformity assessment activity.

Note 2 to entry: Adapted from ISO/IEC 17000:2004, definition 2.2.

3.18

health information system

repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorized users

[SOURCE: ISO 27799:2008, definition 3.1.2]

Note 1 to entry: It has a commonly agreed logical information model which is independent of EHR (electronic health record) systems.

Note 2 to entry: Its primary purpose is the support of continuing, efficient and quality integrated healthcare and it contains information which is retrospective, concurrent and prospective.

3.19

healthcare

any type of services provided by professionals or paraprofessionals with an impact on health status

[SOURCE: European Parliament, 1998, as cited by WHO]

3.20

health organization

organization involved in the direct provision of health activities

Note 1 to entry: Adapted from ISO/TR 20514:2005, definition 2.21.

3.21

health professional

person who is authorized by a recognised body to be qualified to perform certain health duties

Note 1 to entry: Adapted from ISO 17090-1:2008, definition 3.1.8.

Note 2 to entry: The defined term is often "healthcare professional". A convention has been adopted in this Technical Specification 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 healthcare).

3.22

identity

set of attributes which make it possible to recognize, contact or locate the subject of care

3.23

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 physical, physiological, mental, economic, cultural or social identity

[SOURCE: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data]

3.24

identification

recognition of a person in a particular domain by a set of his or her attributes

3.25

information governance

processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed

3.26

information privacy

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

[SOURCE: Adapted from the definition of privacy in the Generally Accepted Privacy Principles of the American Institute of Certified Public Accountants and the Chartered Accountants of Canada]

3.27

information security

preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2012, definition 2.30]

3.28

inspection

examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements

Note 1 to entry: Inspection of a process may include inspection of persons, facilities, technology and methodology.

[SOURCE: ISO/IEC 17000:2004, definition 4.3]

3.29

personal health information

PHI

information about an identifiable person that relates to the physical or mental health of the individual, or to provision of health services to the individual

Note 1 to entry: Such information may include a) information about the registration of the individual for the provision of health services, b) information about payments or eligibility for health care in respect to the individual, c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes, d) any information about the individual that is collected in the course of the provision of health services to the individual, e) information derived from the testing or examination of a body part or bodily substance, and f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

Note 2 to entry: Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymized, i.e. the identity of the individual who is the subject of the information cannot be ascertained from the information.

3.30

PHI disclosure

divulging of, or provision of access to, personal health information

Note 1 to entry: Adapted from ISO/TS 25237:2008, definition 3.20.

3.31

point-of-service (POS) clinical system

system that is used at the point of care or service in the provision of clinical services to the subject of care

EXAMPLE Electronic Medical Record (EMR), Pharmacy Management System (PMS), Hospital Information System (HIS), Public Health Information System (PHIS).

3.32

privacy breach

situation where PHI is processed in an unlawful manner or in violation of one or more relevant privacy policies

3.33

privacy control

technical and organizational measures aimed at mitigating risks that could result in privacy breaches

Note 1 to entry: Privacy controls include policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature.

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

3.34

privacy policy

specification of objectives, rules, obligations and privacy controls with regard to the processing of PHI in a particular setting

3.35

privacy preferences

specific or implied choices made by an individual about how his/her PHI should be processed

3.36

privacy principles

set of shared values governing the privacy protection of the PHI when processed in ICT systems

3.37

privacy risk assessment

analysis of the risks of privacy breach involved in an envisaged processing operation

Note 1 to entry: This analysis, also known as privacy impact assessment, is achieved to (a) ensure processing conforms to applicable legal, regulatory and policy requirements regarding privacy, (b) determine the risks and effects of processing PHI, and (c) examine and evaluate privacy controls and alternative processes for handling PHI to mitigate identified privacy risks.

3.38

privacy safeguarding requirements

criteria to be fulfilled when implementing privacy controls designed to help mitigate risks of privacy breaches

3.39

procedure

specified way to carry out an activity or a process

[SOURCE: ISO 9000:2005, definition 3.4.5]

3.40

processing of PHI

any operation or set of operations performed upon PHI (e.g. collection, storage, access, analysis, linkage, communication, disclosure and retention)

3.41

profile

set of automatically generated data characterizing a category of individuals that is intended to be applied to an individual, namely for the purpose of analysing or predicting personal preferences, behaviours and attitudes

3.42

product

result of a process

Note 1 to entry: Four generic product categories are noted in ISO 9000:2005: services (e.g. transport); software (e.g. computer program, dictionary); hardware (e.g. engine, mechanical part); processed materials (e.g. lubricant). Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element.

Note 2 to entry: The statement of conformity can be regarded as a product of attestation.

Note 3 to entry: Adapted from ISO 9000:2005, 3.4.2.

3.43

pseudonymization

process applied to PHI which replaces identity information with an alias

Note 1 to entry: Pseudonymization allows, for example, a subject of care to use a resource or service without disclosing his or her identity, while still being held accountable for that use. After pseudonymization, it may still be possible to determine the subject of care's identity based on the alias and/or to link the subject's actions to one another and as a consequence, to the subject of care.

3.44

review

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

[SOURCE: ISO/IEC 17000:2004, definition 5.1]

3.45

risk

combination of the probability of an event and its consequence

Note 1 to entry: Adapted from ISO Guide 73:2009, definition 1.1.

3.46

risk assessment

overall process of risk analysis and risk evaluation

Note 1 to entry: Adapted from ISO Guide 73:2009, definition 3.4.1.

3.47

risk management

coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73:2009, definition 2.1]

Note 1 to entry: Risk management generally includes risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

3.48

risk treatment

process of selection and implementation of measures to modify risk

Note 1 to entry: Adapted from ISO Guide 73:2009, definition 3.8.1.

3.49

sampling

provision of a sample of the object of conformity assessment, according to a procedure

[SOURCE: ISO/IEC 17000:2004, definition 4.1]

3.50

scope of attestation

range or characteristics of objects of conformity assessment covered by attestation

[SOURCE: ISO/IEC 17000:2004, definition 5.3]

3.51

second-party conformity assessment activity

conformity assessment activity that is performed by a person or organization that has a user interest in the object

Note 1 to entry: Persons or organizations performing second-party conformity assessment activities include, for example, purchasers or users of products, or potential customers seeking to rely on a supplier's management system, or organizations representing those interests.

[SOURCE: ISO/IEC 17000:2004, definition 2.3]

3.52

specified requirement

need or expectation that is stated

Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications.

[SOURCE: ISO/IEC 17000:2004, definition 3.1]

3.53

subject of care patient

one or more persons scheduled to receive, receiving, or having received a health service

Note 1 to entry: Adapted from ISO 18308:2011, definition 3.47.

3.54

system integrity

property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system

[SOURCE: ISO 27799:2008, definition 3.2.14]

3.55

target of evaluation

TOE

set of software, firmware and/or hardware possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, definition 3.1.72]

3.56

testing

determination of one or more characteristics of an object of conformity assessment, according to a procedure

Note 1 to entry: "Testing" typically applies to materials, products or processes.

[SOURCE: ISO/IEC 17000:2004, definition 4.2]

3.57

third-party conformity assessment activity

conformity assessment activity that is performed by a person or body that is independent of the person or organization that provides the object, and of user interests in that object

Note 1 to entry: Criteria for the independence of conformity assessment bodies and accreditation bodies are provided in the International Standards and Guides applicable to their activities (see Bibliography).

[SOURCE: ISO/IEC 17000:2004, definition 2.4]

3.58
threat

potential cause of an unwanted incident, which may result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2012, definition 2.77]

3.59
vulnerability

weakness of an asset or control that can be exploited by a threat

4 Abbreviations

For the purposes of this document, the following abbreviations apply:

EHR	Electronic Health Record
HL7	Health Level 7
PHI	Personal Health Information
POS	Point-of-Service
PP	Protection Profile

5 Security and privacy requirements

5.1 General

This clause is technical and establishes a set of requirements; describing what is necessary to protect (information, patients), the main categories of risks, and the broad scope of security and privacy concerns for point of care, interoperable electronic patient record systems.

5.2 Theoretical foundation

5.2.1 Overview

With growth in the adoption of health information systems by all players in the health area, (providers, governments, payers and patients), and the need for these systems to be able to exchange patient information to improve the continuity and safety of patient care, it becomes essential to ensure these computational systems are managing the security of electronic health information to ensure its integrity, availability and confidentiality.

The migration from traditional patient record keeping processes, much based on paper, to the electronic process, represents a completely new scenario. One professional may understand very well the security and privacy risks of, for example, storing and transporting a paper-based health record. However, at the moment that this information is no longer on paper and information is exchanged electronically and accessed by multiple providers at multiple care delivery locations, a completely new set of risks is involved. Is it clearly understandable for all users what the risks are of storage and transport of an electronic health record? To understand requires an appreciation of all the features of the computational systems and hardware that handle the information, plus the new processes that are performed to manage the electronic system.

Security goals encompass confidentiality, availability and integrity of information (in this case, health information). Some other security concepts are also included in this broad definition, like authenticity, accountability and auditability. The consequences of security failures are diverse, and range from legal

to clinical impact, information not being available for treatment and even serious injury or death may be the result. On the other hand, good security controls allow electronic systems to work correctly and enable clinical activities to provide better treatment by having the right information available when and where needed.

Many factors affect the security and privacy of health information. In the non-electronic world, paper may be secured in locked cabinets but equally important is how securely the key to the cabinet is stored. As a parallel in the electronic environment, there are both electronic hardware and software components that can enhance security and privacy, but these are insufficient without the concomitant processes that persons must follow in manipulating the electronic information and using information systems. Robust security and privacy is the resulting combination of controls in both the electronic components and processes. If one control fails it can risk the overall protection.

An example of a security requirement for software is that the information system must record audit information on all patient record transactions, including those which create, read, update and archive information. An example of a hardware requirement is that it must record evidence of tampering. An example of a process requirement is a policy and monitoring process preventing users from leaving passwords written down and available.

The main asset is information. Health information includes:

- a) personal health and identification information,
- b) pseudonymized data derived from personal health information via some methodology for pseudonymous identification,
- c) statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data,
- d) clinical/medical knowledge not related to any specific subject of care, including clinical decision support data (e.g. data on adverse drug reactions),
- e) data on health professionals, staff and volunteers,
- f) information related to public health surveillance,
- g) audit trail data, produced by health information systems, that contain personal health information or pseudonymous data derived from personal health information, or that contain data about the actions of users in regard to personal health information, and
- h) system security data for health information systems, including access control data and other security related system configuration data, for health information systems.

It is important to note from the list above that patient information is not the only confidential information in a healthcare environment. The extent to which confidentiality (and hence, patient privacy), data integrity and system availability must be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data may not be confidential, but protecting its integrity may be important to the organization. Likewise, audit trail data may not require high availability but its content may be highly confidential.

The scope of this Technical Specification is focused on security and privacy requirements for health software systems. Hardware and process controls are outside the scope.

As described in ISO 27799:2008, Annex A, the threats to the privacy, confidentiality, integrity and availability include:

- a) masquerading by insiders such as health professionals and support staff by service providers and outsiders, including hackers,
- b) unauthorized use of a health information application and data stored within,
- c) introduction of damaging or disruptive software, including viruses, worms, and other “malware”

- d) misuse of system resources,
- e) communications infiltration, such as denial of service and replay attacks,
- f) communications interception,
- g) repudiation of data origin or receipt,
- h) connection failure,
- i) accidental misrouting,
- j) technical failure of the host, storage facility, or network infrastructure,
- k) environmental support failure, including power failures and disruptions of service arising from natural or man-made disasters,
- l) application software failure,
- m) operations error,
- n) maintenance error, and
- o) user error.

Although health information privacy has been widely discussed, there is a lack of systemic investigation to identify and classify various sources of threats to information privacy. Recent policy-based studies broadly categorize privacy threats into two areas:

- organizational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting a vulnerability of the information systems; and
- systemic threats that arise from an agent in the information flow chain exploiting the data beyond its intended use.

These two types of threats are described in [5.2.2](#) and [5.2.3](#).

5.2.2 Organizational threats

These threats assume different forms, such as an employee who accesses data without any legitimate need or an outside attacker (hacker) that infiltrates an organization's information infrastructure to steal data or render it inoperable. The broad spectrum of organizational threats could be categorized into five levels, listed in increasing order of sophistication:

- Accidental disclosure: healthcare personnel unintentionally disclose patient information to others (e.g. email message sent to wrong address or inadvertent web posting of sensitive data).
- Insider curiosity: an insider with data access privilege pries upon patient's records out of curiosity or for their own purpose (e.g. nurse accessing information about a fellow employee to determine possibility of a sexually transmitted disease or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting it to the media).
- Data breach by insider: insiders access patient information and then use or transmit or disclose it to outsiders for profit or revenge.
- Data breach by outsider with physical intrusion: an outsider enters the physical facility either by coercion or forced entry and gains access to the system.
- Unauthorized intrusion of network system: an outsider, including former employees, patients, or hackers, intrudes into an organization's network from the outside to gain access to patient information or render the system inoperable.

5.2.3 Systemic threats

These threats occur, not from outside of the information flow chain, but from insiders who are privileged to access patient information. For example, insurance firms may deny life insurance to patients based on their medical conditions, or an employer having access to employees' medical records may deny promotion or terminate employment. Patients or payer organizations may incur financial losses from fraud including rendering medically unnecessary services.

5.2.4 Applicability

As previously stated, the scope of Technical Specification is focused on security and privacy of point-of-service patient record software; hardware and process controls are out of the scope. There are many different security and privacy requirements developed and published around the world, this Technical Specification does not intend to create completely new requirements, but rather it harvests the most suitable requirements already published, and adapts them to be used for conformance testing of systems.

The most well-known international security standard is the ISO/IEC 27002. Although its focus is on information security management in general, its controls apply to electronic systems. A health industry specific standard, ISO 27799, is one of several standards developed through ISO/TC 215 to support the implementation of sound security controls and practices in the health care environment.

With regard to security evaluation, one of best known standards is ISO/IEC 15408 (all parts), which provides general concepts and principles of IT security evaluation and includes the Common Criteria framework through which security requirements can be expressed.

At the same time, some countries are deploying health software systems certification processes, each one with its own set of requirements. Some examples include the US, Canada, Brazil, The Netherlands, UK, Australia and Europe.

This Technical Specification identifies the security and privacy requirements, harvested from the above mentioned standards and international experiences, which should be in place for conformance testing for interoperable POS clinical (electronic patient record) systems interfacing with EHRs.

A set of requirements must be clear and well expressed, in a manner that software developer can properly deploy them in their systems, and an evaluation process can declare that all requirements are or are not met in that specific system. This is the main reason that procedural requirements are not included, as it is not possible to ensure that they are in place merely by evaluating the software itself: it would be necessary to evaluate the operational environment in which this software is in use, including the profiles of users and administrators and knowledge of the system's use. Nevertheless, this broader issue of administration is essential for promoting security and privacy and so it is recommended that, in addition to the software certification and conformance, an environmental inspection of the system's ongoing management based on ISO 27799 be performed.

Another consideration in the process of elaborating the requirements was that they should be, as much as possible, immune to short-term technological change and evolution. Because of this, references to technical information, like cryptograph algorithms, key length, protocols and others have not been made. Supplemental information on these technical criteria may be needed.

5.3 Privacy and security requirements

5.3.1 General

This clause presents the requirements which would apply to all POS clinical systems within scope of this Technical Specification.

5.3.2 Data subject's consent to collect, use or disclose personal health information

Requirement 1 Recording consent: Where data subjects have a right, by law or custom, to withhold or revoke their consent to the use or disclosure of their personal health information, POS clinical systems:

- a) shall provide a facility to record a data subject's consent directives, including the withholding or revocation of consent;
- b) shall be able to accomplish this in a way that allows each organization to comply with its own legal or policy requirements on consent;

NOTE The consent can be for all or part of the data subject's personal health information or for a specified purpose.

Requirement 2 Minimum data recorded: where POS clinical systems record a data subject's disclosure directives, the characteristics of the directive shall be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the type of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus express consent) and the date on which the directive was given.

Requirement 3 Directives follow the data: where data subjects have a right, by law or custom, to withhold or revoke their consent to the collection, use or disclosure of their personal health information, POS clinical systems should provide a facility to transmit restrictions on further (i.e. onward) disclosure along with the data disclosed if the recipient(s) of the disclosure could not otherwise be aware of and honour the data subject's consent directives. The POS clinical system should be able to accomplish this in a way that allows the sending and receiving jurisdictions to comply with their own legal requirements or policies on consent.

Requirement 4 Emergency access: emergency medical care (such as that given to an unconscious patient) or other special situations permitted by law or policy (such as public health investigations during communicable disease outbreaks) may necessitate access to patient records stored in a POS clinical system without regard for previously recorded disclosure directives. Such emergency access capability shall only be provided to authorized users and its invocation (along with a reason the user is overriding the consent directive) shall be recorded in an audit log. Except where overriding of consent directives is allowed by law or policy, and to eliminate uncertainty as to whether a user intended to override patient consent directives, the system should either allow the user to expressly invoke emergency access or else the system should inform the accessing user, prior to granting access, that the access will constitute emergency access.

Requirement 5 Logging emergency access: POS clinical systems shall be able to:

- a) log when the processing of consent directives prohibits the disclosure of data;
- b) log the identity of any user who overrides a data subject's consent directives, the reason for the emergency access, a unique identifier that can be later used to identify the data subject, the date and time when the emergency access occurred;
- c) where an individual in the user's organization is accountable for facilitating privacy compliance, notify this individual of the emergency access.

Requirement 6 Consent given by a legally authorized representative: where a consent directive is given on behalf of a subject of care by a legally authorized representative, the POS clinical systems should be able to record the identity of this representative and the representative's relationship to the subject of care.

Requirement 7 Reporting changes to consent: POS clinical systems recording consent directives shall be able to indicate which consent directives, if any, were in force at any given point in time for any given subject of care.

Rationale

Healthcare organizations need to know that they have obtained the consent required in their jurisdiction when they collect, use or disclose PHI. The form of the consent sought by organizations may vary, depending upon the jurisdiction, the circumstances under which the information is disclosed (for example, to a healthcare specialist versus a social services agency) and the type of information disclosed (for example, mandatory reporting of communicable diseases will not likely require consent from the data subject).

It is those entering PHI into a POS clinical system within a particular jurisdiction that have the primary obligation of obtaining and recording the consent directives of data subjects and it is often at the point of collection where it is most efficient to obtain and record consent. The POS clinical system has to provide means so that the Healthcare organization can ensure that those accessing PHI only obtain access to information that is legitimately available on the basis either of consent or of legal authorization (for example, when records are disclosed in response to a court order).

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.3 Limiting use and disclosure

Requirement 8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure: personal health information should only be used or disclosed for purposes consistent with those for which it was collected. POS clinical systems should be structured so as not to store fields of data that have no clear relation to an identified data purpose such as treatment and care, medical billing, or clinical research.

Requirement 9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject: it should be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the nature of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus express consent) and the date on which the directive was given.

Requirement 10 Restricting data exports: data transmitted in electronic or printed format from a POS clinical system to another system should only occur for identified purposes such as clinical care, data backup, or for transmission to the data subject (or the data subject's agent) at the subject's request.

Rationale

This requirement is a standard and traditional fair information practice and does not impede upon health providers' ability to provide care. In jurisdictions where health data protection legislation has been introduced, these statutes typically permit or require a number of uses and disclosures of personal health related to provision of healthcare, supporting the operation of the healthcare system, or ensuring public health.

Only POS clinical system users engaged in the subject's care and support have the implied consent of the subject of care to access the subject's data. Without such consent, the data cannot normally be accessed. Systems need to ensure that access is appropriately controlled to records of a specific data subject. For example, any records of patients no longer registered at a clinic or practice should not be normally accessible to users at that clinic.

References

OECD Fair Information Practices

5.3.4 Data subject access to personal health information and correction of inaccurate information

Requirement 11 Data subject access: when a data subject challenges the completeness or accuracy of information in the subject's record, and the organization disagrees with the subject's assessment of

incompleteness or inaccuracy, the POS clinical system should be capable of recording the disagreement and/or the reason for the refusal to update the record.

Requirement 12 Accessibility: POS clinical systems should be capable of output or display of personal health information in a format that can be read by the subject of care.

NOTE In some jurisdictions, data subjects have a right to access their record and to request changes to the record.

Rationale

Healthcare organizations will typically only address errors in factual data, such as a data subject's birth date. Matters of opinion, including a diagnosis by a healthcare professional, may result in disagreements about the accuracy of a patient record. The issue of correction or addition is especially relevant if the information can make a possible difference in the treatment of a person or in decisions made about him or her.

Some corrections or amendments will have a particular relevance to a subject's ongoing healthcare and these changes should be made known appropriately. Fortunately, a developed electronic health record system will have the capability to automatically distribute the most up to date information when it is required for authorized purposes.

Reference

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.5 Data accuracy

Requirement 13 Accuracy: POS clinical systems shall include measures to ensure that PHI is accurate and complete as is necessary for the purposes for which it is to be used. Examples include implementing data input validation controls and using integrity checks such as checksums and hash totals.

Requirement 14 Subject of care identification: POS clinical systems shall accurately identify a subject of care in the system by means of unique identifiers, searchable by users, when accessing or modifying the subject's records.

Rationale

An electronic health record environment should facilitate the achievement of better quality records by building in automatic checks on data entry and making it easy to update demographic information on a subject of care.

In addition, it is of critical importance for patient safety that POS clinical system users accurately identify subjects of care prior to accessing or modifying their PHI.

Reference

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.6 User identification and authentication

Requirement 15 User identification: users of POS clinical systems shall be assigned an identifier (user ID) that, perhaps in combination with other identifiers (e.g. facility identifiers, jurisdictional identifiers) uniquely identifies each individual user and that is used in user authentication and audit logging. Where transactions extend across organizational or jurisdictional boundaries, user IDs, in combination with other user registration information (e.g. user names, addresses, facility identifiers, jurisdictional identifiers) shall:

- a) uniquely identify each user,
- b) allow access control decisions (see [5.3.7](#)), and

- c) allow the compilation of audit records (see [5.3.16](#)) that can unambiguously associate user identities with their audited user actions.

Requirement 16 User IDs: POS clinical systems shall support case-insensitive user identifiers that contain characters drawn from ISO/IEC 8859 (all parts) (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode).

Requirement 17 User authentication: POS clinical systems shall ensure that all users are securely authenticated.

Requirement 18 User authentication: POS clinical systems shall authenticate every user before access to personal health information or related POS clinical system services are granted to the user. For greater clarity, this includes access granted when not connected to a network (e.g. when the POS clinical system is available for access offline).

Requirement 19 Authentication methods: where practicable, POS clinical systems should support multi-factor user authentication.

Requirement 20 User and system authentication: POS clinical systems shall authenticate every entity seeking access to personal health information.

POS clinical systems shall ensure the authenticity of remote nodes (mutual node authentication) when communicating personal health information over the Internet or other known open networks by using a secure standards-based protocol.

Requirement 21 Protecting user profiles, passwords, and other authentication tokens: all data or parameters used in the POS clinical system user authentication process shall be stored or transported in a secure manner and protected from unauthorized access (including viewing, modification, or deletion).

Where user passwords are employed, either hash codes computed from each user's password should be stored instead of the actual password, or else the password should be encrypted with cryptographically secure algorithms.

Requirement 22 Passwords: use, quality, reset, and user changes: when passwords are used, the POS clinical system shall implement the following security controls:

- a) **Password quality:** check password quality at the time the user defines it by ensuring, for example, that passwords have at least eight characters, of which at least one should be non-alphabetic.
- b) **Frequency of password changes:** implement a function that requires users to change their password according to an adjustable maximum time period.
- c) **Password reset:** provide an administrative function that resets passwords. User accounts that have been reset by an administrator shall require the user to change the password at next successful login.
- d) **Case sensitivity:** support case-sensitive passwords that contain characters drawn from ISO/IEC 8859 (all parts) (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode).

Requirement 23 Failed Login Attempts: POS clinical systems shall enforce a limit of consecutive invalid access attempts by a user to protect against further (possibly malicious) user authentication attempts. Examples of appropriate mechanisms include locking the account/node until released by an administrator, locking the account/node for a configurable time period, or delaying the next login prompt according to a configurable delay algorithm.

Requirement 24 User feedback during authentication: the POS clinical system shall provide only limited feedback information to the user during authentication that does not assist the user in discovering user IDs and passwords.

Rationale

This requirement facilitates audit logging of user initiated events (such as access to, or modification of, a data subject's record). Authentication also helps to ensure that PHI is not compromised by access or modification by unauthorized users.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.7 Access control

Requirement 25 Access controls: POS clinical systems shall verify that every authenticated person or entity seeking access to personal health information is authorized to access such information.

Requirement 26 Authorization control: prior to carrying out a system of data function related to personal health information, POS clinical systems shall verify that the requesting user or entity has the required access privileges.

Requirement 27 Role-based access control: POS clinical systems shall support role-based access control (RBAC) capable of mapping each user to one or more roles, and each role to one or more system functions or access privileges.

Requirement 28 Other forms of access control: POS clinical systems should additionally be capable mapping each user to access rights assigned or restricted based on:

- a) working groups to which the user belongs, or
- b) the context of the transaction (for example, time-of-day, workstation-location, or emergency access).

Requirement 29 Delegation of access to the personal health information of subjects of care: POS clinical systems should be capable of maintaining an association between selected users and the records of subjects of care and permit access based on this association; i.e. POS clinical systems should be capable of granting delegated access to records based upon a user with authorized access to a subject of care's records granting access rights for those records to another user.

Where implemented, such granting of access shall not:

- a) allow a user, by system means, to grant another user access to a record if the granting user does not possess such access with respect to the record, or
- b) exceed the role-based access privileges of the user being granted the access.

Requirement 30 Reporting access privileges: POS clinical systems should be able to report, for a given user, whether the user can access the records of a given subject of care and the privileges (viewing, modification, etc.) the user has in respect of the subject's records.

Requirement 31 Restrictions on access privileges: where a user has been assigned more than one user role, the POS clinical system shall allow the user to select which of the roles allocated to the user is to be applied to that user's session.

Requirement 32 Revoking access privileges: POS clinical systems shall support revocation of a user's access privileges without requiring the deletion of the user from the system. POS clinical systems shall prevent users whose access privileges have all been revoked from logging into the system.

Rationale

At the moment that a system is ready to be used, it is able to be accessed not only by authorized users, but potentially also unauthorized ones. Systems therefore need to be designed with appropriate access controls. As well, there need to be controls that detect attempts at unauthorized access, and take action to block these attempts.

As a practical matter, users of POS clinical systems (and there could be thousands of them) cannot individually be mapped to system functions upon user registration in order to control the extent of their

user access privileges. Such a mapping is too complex and too error prone to be done on a user-by-user basis. Rather, users need to be mapped to roles, and then the roles mapped to system functions.

It is unreasonable to assume that all physicians ought to be able to access all patient records in a large POS clinical system, as this may be many tens of thousands of data subjects. Controls need to be put into place to restrict user access. There may be a need to maintain a list of one or more workgroups to which the user is a member. Examples might include surgical teams at a specific hospital or physicians with admitting privileges at a specific hospital. Such workgroups would enable a user's relationship with a subject of care to be inferred from existing relationships between the subject and other members of the workgroup.

It is important to note that delegated access control does not "trump" role based access control. For example, where permissible, a family physician can grant another physician (a specialist, say) full access to one of her patient's records. The specialist might later use that access to write an e-prescription for the patient. However, if the physician grants access to a nurse, the nurse cannot later write an e-prescription for the patient, as role based access control would typically prevent nurses from exercising such a function.

The requirement for removing access privileges is intended to provide the ability to remove a user's privileges, but maintain a history of the user in the system.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789, ISO/TS 22600 (all parts)

5.3.8 Acceptable Use

Requirement 33 Notifications to users: in each user's session, either prior or immediately following user login or other periodic intervals, the POS clinical system should display a configurable warning or login banner to remind the user of the confidentiality and appropriate use of the personal health information accessible from the system and/or applicable penalties for misuse of the system.

Rationale

Users of POS clinical systems need to be aware of their obligations (ethical and legal) in relation to the personal health information they are accessing. Several jurisdictions have implemented requirements whereby systems prominently display a message upon application start-up or upon user log in to remind users of their responsibilities and the legal constraints on the use of the system.

For administrators to have legal recourse against users who flout information privacy protections by accessing personal information unrelated to the course of their work, these administrators may need to establish that the users were clearly aware of the confidential nature and purposes of use of the information accessed. A clear message upon user login provides additional protection against the possibility of spurious claims from rogue users insisting that they were unaware of the confidential nature of the information accessed or restrictions on its use. Clear warnings help to facilitate the pursuit of penalties against unauthorized users.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.9 Session security and timeout

Requirement 34 Session security: POS clinical systems should protect unattended workstations against an unauthorized person taking the opportunity to use the workstation while the system is active with automatic timeout after a period of inactivity.

Requirement 35 User session timeout: POS clinical systems shall protect unattended workstations from being accessed by unauthorized person(s) by means of an automatic timeout after a configurable period of user inactivity. Examples of such protection include application of a screen-saver or application locking, requiring a legitimate user to re-authenticate. Automatic timeout should be pre-

warning (at a configurable interval of time) that timeout is about to take place. When a user's session has timed out, the same user should be able to return to the session by re-authenticating, or another user should be able to end the previous session (without reactivating it) in order to be able to proceed with a new session.

Requirement 36 Connection timeout: where appropriate, the POS clinical system should restrict connection duration to a configurable period of time to force a reconnect when a connection has been held open for an excessively long time.

Requirement 37 Session security: the POS clinical system should have communication session security controls to prevent the user's session from being hijacked or stolen.

Rationale

Many POS clinical systems already implement session security, at least at a rudimentary level (for example, by automatically logging out users after a period of inactivity or invoking a screen saver function that can only be unlocked after user re-authentication). Note that as some workstations are positioned in physically secure areas (for example, behind the prescriptions dispensing counter in a pharmacy), this requirement may not be universally applicable.

A requirement for connection timeout is sometimes used in high security applications to force a reconnect (and hence re-authentication) when a connection has been held open for an excessively long time. The length of time to maintain a connection varies with the nature of the application and the types of connections (e.g.: server to server or client to server).

The requirement for session security is motivated by the fact that a session can be stolen even during protected sessions (e.g. SSL/TLS). For example, if the session is controlled through a cookie in the URL, under some situations the URL of a user's session can be obtained and used by another user, assuming the personality of the prior user.

Reference

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.10 Maintaining data availability

Requirement 38 Backup: the POS clinical system shall support the generation of backup copies of the application data, security credentials, audit log files, and other data and files needed for the proper functioning of the POS clinical system.

Requirement 39 Concurrent backup: if the POS clinical system is available continuously, then the system shall have ability to run a backup concurrently with the operation of the application.

Requirement 40 Restoration: POS clinical system data restoration shall enable a user to return the system to a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and audit files, and shall also enable validation of the integrity of the data restored (see also [5.3.13 Data Integrity](#)).

Requirement 41 Reconstructing the content of an electronic health record at a prior point in time: POS clinical systems shall have the capability of displaying the content any data subject's record(s) as the record existed at any previous date or time.

Rationale

Clinical data are a valuable, expensive, and sometimes irreplaceable resource and it is essential that it be preserved.

POS clinical systems need to allow for secure copies to be made that meet the following requirements:

- export the security attributes together with the data;

- ensure that when restoring from a security copy all security attributes and their associations are automatically restored without administrator intervention;
- ensure that only authorized backup operator can export and restore a security copy making sure that access to the information is strictly limited;
- are able to run a backup concurrently with the operation of the application for those systems running continuously;
- ensure that information integrity is checked both when generating and restoring a security copy;
- the system restore functionality shall result in a fully operational and secure state that includes the restoration of the application data, security credentials, and audit files to their previous state.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.11 Protecting data during transmission

POS clinical systems shall apply industry standard cryptographic algorithms and protocols to the transmission of PHI over the Internet or other open networks in order to maintain the confidentiality and integrity of the data.

Requirement 42 Encrypting data during transmission:

In a clinical system consisting of components distributed across multiple computers or systems, the communication between those components should, (and over the Internet or other open network, shall) offer the following security components:

- a) partner authentication (e.g. client and server),
- b) data integrity, and
- c) data confidentiality.

EXAMPLE 1 POS clinical system communication sessions between a client component and a server taking place over the Internet or another open networks featuring server authentication, data integrity, and data confidentiality.

EXAMPLE 2 POS clinical system communication sessions between a client browser and a web server taking place over the Internet or another open network featuring web-based security such as Transport Layer Security (TLS) to provide server authentication, data integrity, and data confidentiality.

Requirement 43 Confirmation of data delivery:

In order to ensure that transmitted data are received, clinical systems shall implement security controls to confirm delivery or receipt of data when data communications take place outside the physical security perimeter that protects information processing facilities.

Rationale

Interception of confidential personal information is a serious risk in healthcare and its malicious alteration in transit could have severe consequences. Providing for the confidentiality and integrity of PHI transmitted by POS clinical systems is a minimum requirement.

Jurisdictional health information legislation does not typically contain specific directions regarding cryptographic protection of information during transmission, but there are some general requirements that follow from industry standards for cryptography and cryptographic protocols.

Where appropriate, the system should obtain acknowledgement of receipt during data transmission of PHI to ensure that the transmitted data was received.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.12 Protecting data in storage

Requirement 44 Protecting operational data: POS clinical systems shall ensure that personal information, audit logs, and security-related data such as user profiles, are all protected from unauthorized access and modification when stored within databases and/or file systems.

Requirement 45 Protecting data on portable media: when storing PHI on any media or device intended to be portable or removable (for example, thumb-drives, CD-ROM, PDA, or notebook computer), POS clinical systems shall support use of an industry standard encryption format.

Requirement 46 Protecting data in data repositories: clinical systems storing the following types of data shall protect this data from unauthorized access:

- a) personal information (e.g. patient demographics or other information that identifies a patient);
- b) personal health information;
- c) security critical system data (including user profile data and audit logs).

Rationale

Protection of the PHI is essential if use and disclosure of this information is to be controlled.

Encryption of data stores is still uncommon in healthcare and healthcare organizations have been slow to make use of contemporary technology for encrypting databases. Hundreds of thousands of unencrypted patient records have been lost on portable media since 2007. Encryption is essential for the protection of data on portable media and devices.

Protection of user registration data are essential to maintaining its integrity (and hence the integrity of the user authentication process). Protecting its confidentiality is also essential to maintaining the trust of healthcare providers (who, for example, do not want unauthorized disclosure of their contact details).

While physical protection of data storage will always be essential (to protect system availability), de-identification and encryption should be considered where appropriate in the design of new systems.

Reference

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.13 Data integrity

Requirement 47 Integrity of data inputs: data imported from another EHR via portable device shall be accurately associated with a subject of care and a physician in charge, location, date and time of import, and user who imported the data.

Requirement 48 Integrity of data during processing: controls shall be in place within the POS clinical system check the integrity of EHR data in order to prevent user actions or system failures from causing data inconsistencies or failures in the referential integrity of links among data records.

Requirement 49 Integrity of data outputs: POS clinical systems should ensure it is possible for a reader to check that hardcopy print-outs are complete (e.g. "page 3 of 5").

Rationale

These are minimum requirements to promote data integrity. They also prevent covert selective presentation of data.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.14 Record retention

Requirement 50 Retention: POS clinical systems shall be capable of storing data for retention periods defined by law or organizational policy. When data are no longer needed, it may be disposed of where permitted by law and organization policy. In this case, it shall be disposed securely, erased or rendered anonymous, so that disposition processes occasion no breaches of privacy and security.

Rationale

Some types of subject of care data can remain clinically relevant for many years. In several jurisdictions, there are requirements that personal health information on children or adolescents remain available for up to 10 years after the child reaches the age of majority (e.g. eighteen years of age). POS clinical systems need to be built with such archiving requirements in mind so that information can be retained for as long as needed and then subsequently disposed in a secure way.

Reference

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789, ISO/TS 21547

5.3.15 Data Labelling

Requirement 51 Labelling: POS clinical systems shall be capable of informing each user of the confidential nature and purposes of use of PHI by displaying this labelling (in a consistent location and manner) on hardcopy printouts displaying the data. POS clinical systems should either show this labelling on any screen displaying the data (in a consistent location and manner) or else display this labelling to the user upon logging into the application.

Rationale

This requirement ensures that all healthcare providers and support staff are aware that the specific information they are viewing is confidential and may only be used for specific purposes (e.g. treatment and care). This is especially important where the information is contained in email, faxes or other documents which may contain a mixture of confidential and non-confidential information.

While it is understood that confidentiality statements can be overlooked by users grown accustomed to such warnings, these statements nonetheless retain the advantage of providing grounds for prosecution should the user not treat the information with due care.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.16 Audit

Requirement 52 Audit logging: POS clinical systems shall be capable of recording events related to system use (i.e. system start and stop, user login and logout, session timeout, backup and restore, account lockout) and health information manipulation (i.e. creation, access, modification, and archiving, as well as import, export, printing, or other disclosure of personal health information).

Requirement 53 Information recorded: for each of these events, control information shall be recorded, i.e. time of event, identity and the role of the user (in those cases where a user can choose among multiple roles before commencing a user session), the identity of the subject of care, and the nature of the audited event.

Requirement 54 Protecting the audit log: the audit log files shall have appropriate security controls to prevent alteration and unauthorized access. Examples of such security controls include access controls, unique sequence numbers to prevent deletion, prevention of modification, and periodic or continuous backup.

Requirement 55 Audit interface: access to audit data shall be strictly controlled and itself subject to audit. Access should be by an appropriate information system that can enforce these controls, rather than directly to the audit trail itself. The audit system shall provide the capability and investigative tools to read audit information from the audit records and interrogate the audit log to:

- a) to identify all users who have accessed or modified a given data subject's records over a given period of time, or
- b) to identify the actions of a given user (including all access to data subjects' records) over a given period of time.

Requirement 56 Audit log retention: although the duration of retention of audit log files is a matter of organizational policy that may vary from one jurisdiction to another, the audit system shall support retention of audit log entries.

Requirement 57 Auditable events: POS clinical system audit logs shall audit the following events:

- a) subject of care record created or accessed (e.g. displayed on-screen, printed, downloaded) or updated,
- b) accesses data that is locked or masked by instruction of a patient/person (emergency access),
- c) creation and modification in the consent directives of a patient/person,
- d) data queries of personal health information,
- e) PHI import (reception) including data transmission, data exchange,
- f) PHI export, including data transmission, data exchange and printing,
- g) user, role, and group management activities, and
- h) access to audit log.

POS clinical system audit logs should also be capable of auditing the following events:

- system start and stop,
- user authentication attempts and its result (successful or not),
- user logout, session timeout, account lockout,
- backup and restore (where initiated by the system itself),
- database accesses,
- node-authentication failure,
- digital signature created/validated,
- security administration events, including password changes, and
- record disposal.

Clinical systems should allow an authorized administrator to set the inclusion or exclusion of auditable events not included in the list above.

Requirement 58 Minimum content of information recorded: POS clinical system audit log entries shall include the following information:

- a) a record of the user identity,
- b) a record of the identity of the authority – the person authorizing the entry of, or access to data, if different from the user,

- c) the role the user is exercising (in those cases where a user can choose among multiple roles before commencing a user session),
- d) the organization of the accessing user (in those cases where a user accesses information on behalf of more than one organization),
- e) the nature of the audited event and the identity of the associated data (e.g. patient ID, message ID) of the audited event,
- f) the function performed by the user,
- g) a time stamp (data and time of the event),
- h) in the case of emergency access to blocked or masked records or portions of records, a reason for the emergency access, as chosen by the user making the access,
- i) in the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker,
- j) end user device or access point (if available),
- k) In the case of password change, user whose password was changed, and
- l) a sequence number to protect against malicious attempts to subvert the audit trail by, for example, altering the system date.

Requirement 59 Audit interface: the POS clinical system should support logging to a common audit engine (for example, using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile).

The system shall provide authorized administrators with the capability to read audit information from the audit records in at least one of the following ways:

- a) the system should provide the capability to generate reports based on date and time ranges, or
- b) the system should be able to export logs in such a manner as to allow correlation based on date and time (e.g. UTC synchronization).

Requirement 60 Protecting the Audit Logs: POS clinical systems shall:

- a) prohibit users from accessing audit log entries, except those authorized users who have been granted explicit read-access, and
- b) prohibit users from modifying audit log entries.

The system shall secure access to audit records and shall safeguard access to system audit tools and audit trails to prevent misuse or compromise, including deletion or modifications.

Requirement 61 Continuous Logging:

POS clinical system audit logging shall be enabled at all times and there shall be no means for users to disable any audit logging.

Requirement 62 Preserving the History of PHI:

The clinical system shall not make deletions to records or audit log entries or changes to data subject records that prevent the reconstruction of records of a subject of care at a prior point in time.

Rationale

In health, it is accepted that organizations be able to identify who has created, updated, or accessed a record and when access or modification took place. It can be a legal requirement to have proof of who created the information in a health record. It is also common to require that health professionals justify

their need to access patient records. Depending on jurisdictional legislation and/or policy, a formal authorization of the subject of care may be required. All are examples of controls to support patient privacy and health record confidentiality while at the same time supporting the legitimate use of health records and their contents.

With electronic records, it is possible to have more control over some of these aspects than it is in the world of paper records. Automated controls can be applied to improve privacy and provide better support for legal requirements.

Logging of information transaction events and subsequent audit processes support accountability for those subjects of care entrusting their information to electronic health record systems. It also provides a strong incentive to users of such systems to conform to acceptable use policies. Effective logging followed by audit of data access and other transactions can help to uncover misuse of electronic health record systems and data and can help organizations and subjects of care to obtain redress against users abusing their access and data use privileges.

Personal health information is regarded by many as among the most confidential of all types of personal information and protecting its confidentiality is essential if patient privacy is to be maintained. In order to protect the integrity of health information, it is also important that its entire life cycle be fully protected and subsequently auditable.

Audit logs are complementary to implemented access and other transaction controls. The audit logs provide means to assess compliance with the access control policy and can contribute to improving and refining the policy itself. But as such a policy needs to anticipate the occurrence of unforeseen or emergency cases, analysis of the audit logs will for those cases become the primary means for access control.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.17 Software version control and documentation

Requirement 63 POS Clinical System version control:

All components of the POS clinical system shall be identified and have an associated software version with a single unambiguous reference (unique ID, name, supplier, and version number).

Requirement 64 POS Clinical System documentation: POS clinical systems should have available documentation that addresses system requirements and capacities, installation and testing, management and operation, known security issues, user identification and authentication, privilege management and access control, secure communications, audit, software change management, time synchronization, and data backup and restoration

Requirement 65 Changes to documentation: documentation shall contain a history of all changes, so that users can check all changes made in the latest version available.

Requirement 66 Documentation and software versions: all manuals shall clearly state in the beginning of the document the version to which they apply.

Requirement 67 Software version: POS clinical systems shall have functionality that allows users to view the version of its software components.

Requirement 68 Topics included in documentation: POS clinical systems should have available documentation that addresses all of the following:

- a) system requirements, including services and network protocols that are necessary for proper operation, as well as the dependencies upon other EHR components;

- b) system product capacities (e.g. number of users, number of subjects of care, number of records, network load) and baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity);
- c) system installation, start-up, and connection, including communication security setup;
- d) steps needed to confirm that the system installation has been properly completed and that the system is operational;
- e) system management and operation;
- f) security mechanisms and practices, including creation, modification, and deactivation of user accounts; management of roles, reset of passwords, configuration of password constraints and other aspects of privilege management; communication security, and configuration and management of audit logs;
- g) known issues or conflicts with security services, including antivirus, malware eradication, intrusion detection, and firewalls, and the resolution of the conflict where applicable;
- h) software change management and hot-fix processes;
- i) system time (clock) synchronization where applicable;
- j) system error or performance messages to users and administrators, with required actions;
- k) data backup procedures, including data integrity checks when a backup copy is being produced or restored.

Requirement 69 Documentation and version control

All POS clinical system manuals shall clearly state, at the beginning of the document, the version(s) to which they apply.

All updated POS system manuals should provide a summary for the reader of the changes since the last major revision.

Requirement 70 Changes to documentation: documentation shall contain a history of all changes in a user readable form, so that users can check all changes made in the latest version available.

Rationale

Security depends upon effective operational practices and procedures and these in turn depend upon reliable documentation. Software version control is also a significant component of operational security management.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.18 Time synchronization and time/date formatting

Requirement 71 Time format: POS clinical systems should adopt a uniform presentation of time for control and audit.

Requirement 72 Clock synchronization: POS clinical systems shall support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.

Requirement 73 Time format in exported records: all time data for control and audit found in exported data (other than time stamp requests to, or responses from, a Time Stamping Authority) shall be represented in the ISO 8601:2004 format, indicating the difference between local time and UTC

Requirement 74 Time source: POS clinical systems shall use a consistent and secure time source.

POS clinical systems shall support time synchronization using IET Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP).

Rationale

Accurate audit logging requires accurate and consistent time stamps. As well, the date and time at which data such as lab results were accessed may have clinical significance. Such time stamps may be heavily relied upon during investigations of medical malpractice.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789, ISO 8601

5.3.19 Privacy and security incident management

Requirement 75 Incident management: POS clinical systems or supporting audit systems should trigger a notification to the individual(s) in the organization accountable for managing privacy or security incidents each time a potential incidence of system misuse is detected. (See also [5.3.2](#)).

Requirement 76 Incident notification: POS clinical systems should provide an interface so that users can notify an accountable person of security incidents or issues.

Rationale

While the decision of who the responsible person would be for such notifications is a governance issue for the implementing organization, the capability of the POS clinical system to initiate such notifications (by email for example) can be a highly effective tool in rapidly resolving privacy breaches and preventing security incidents from going unnoticed.

It may be useful for POS clinical systems to provide an interface so that users can notify an accountable person of security incidents or issues.

Examples of accountable individuals include privacy officers (referred to in some jurisdictions as privacy and confidentiality officers) and designated users with administrative privileges.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, ISO 27789

5.3.20 Digital certificates and digital signatures

Requirement 77 Providing digital signatures for users: POS systems that provide functions where users are required to apply the electronic equivalent of a handwritten signature should allow such users to apply a digital signature.

Requirement 78 Validating Digital Signatures: whenever a POS system generates and receives data containing a digital signature, the system should confirm, at generation and upon receipt, that the signature is or was valid at the time it was applied.

Requirement 79 Preserving digital signatures: POS systems that allow users to apply a digital signature or that receive digitally signed data, should store, backup or archive the digital signature whenever the signed data are stored, backed up or archived; and transmit the digital signature whenever the signed data are transmitted.

Requirement 80 Digital signing

All POS systems providing functions where users are required to apply the electronic equivalent of a handwritten signature shall:

- a) allow such system users to apply a time-stamped digital signature according to ETSI TS 101 733 (Electronic Signatures and Infrastructures - ESI - CMS Advanced Electronic Signatures - CAdES) or

ETSI TS 101 903 (XML Advanced Electronic Signatures - XAdES), using a digital certificate with a key usage field that permits non-repudiation;

- b) verify at the moment of signature the validity of signer's certificate is not expired, revoked, and the certification path is valid, according with RFC 3280 (Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List - CRL Profile) or RFC 2560 (Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol – OCSP);
- c) allow all POS system users to view and confirm the information to be signed at the moment of signature.

Requirement 81 Validating, preserving and transmitting digital signatures

The POS system shall:

- a) confirm upon receipt that the signature is valid (i.e. that the associated signature certificate and all the associated chain certificates has not been revoked);
- b) store, backup or archive the digital signature and all related data (information about root certificates, certification chains, signatory certificates, and revocation information) whenever the signed data are stored, backed up or archived;
- c) transmit the digital signature together with the data or by reference whenever the signed data are transmitted;
- d) allow users to confirm, whenever they access signed data, that the signature is valid at the time of signing (i.e. that the associated signature certificate has not been revoked).

Requirement 82 Purpose of the signature and signatory role

POS systems providing digital signature functionality should include the commitment-type-indication attribute and the role of the signatory (i.e. the user's role attribute).

Rationale

This requirement is effective for fulfilling services where an electronic equivalent of an authorized pen-and-ink signature is required, like e-prescribing.

References

ISO 27799, ISO/IEC 15408 (all parts), ISO 18308, *ETSI TS 101 733*, *ETSI TS 101 903*, *RFC 3280*, *RFC 2560*.

5.4 Common Criteria

The Common Criteria (CC), published in ISO/IEC 15408 (all parts) as a three part standard, provides a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

It aims to cover all different kinds of IT products and systems and presents a broad spectrum of requirements, leaving the product or system developer the task of defining the scope, called Target of Evaluation (TOE) and the selection of the set of requirements that apply for that specific case.

Because it is a well-known international standard, it is useful to map the relationship between the requirements presented in this technical specification and the CC classes. The cross-mapping below can be useful to those already familiar with CC to better understand Technical Specification, and vice-versa.

Listed below are the Common Criteria classes:

- a) Security Audit (FAU)
- b) Communication (FCO)
- c) Cryptographic support (FCS)

- d) User data protection (FDP)
- e) (G) Identification and authentication (FIA)
- f) (H) Security management (FMT)
- g) (I) Privacy (FPR)
- h) (J) Protection of the TSF – TOE Security Functionality (FPT)
- i) (K) Resource utilization (FRU)
- j) (L) TOE access (FTA)
- k) Trusted path/channels (FTP)
- l) Security management
 - Version control
 - Documentation and procedures
 - Availability
 - Time control
- m) Privacy
- n) Protection of the Security Functionality
- o) Access control

Table 1 shows the cross-mapping between these Common Criteria categories and the requirements elaborated in the previous clause.

Table 1 — Comparison with Common Criteria

Requirement	Mapping between requirement and Common Criteria?	Common Criteria category
1. Data subject's consent to collect, use or disclose personal health information		No direct mapping to privacy (not considered in CC)
2. Limiting use and disclosure		No direct mapping to privacy (not considered in CC)
3. Data subject access to personal information and correction of inaccurate information		No direct mapping to privacy (not considered in CC)
4. Data accuracy	Yes	User data protection: Stored data integrity
5. User identification and authentication	Yes	identification and authentication
6. Access Control	Yes	Access: access control policy, access control functions
7. Acceptable Use		No direct mapping to privacy (not considered in CC)
8. Session security and timeout	Yes	Access: session locking and termination
9. Maintaining data availability	Yes	Security management
10. Protecting data during transmission	Yes	Cryptographic support: cryptographic operation
11. Protecting data in storage	Yes	User data protection

Table 1 (continued)

Requirement	Mapping between requirement and Common Criteria?	Common Criteria category
12. Data integrity	Yes	User data protection: Stored data integrity
13. Record retention		No direct mapping to a CC category
14. Data Labelling	Yes	TOE access
15. Audit	Yes	Security audit
16. Software version control and documentation	Yes	Security management
17. Time synchronization and time/date formatting	Yes	Security Management
18. Privacy and security incident management		No direct mapping to a CC category
19. Digital certificates and digital signatures	Yes	Cryptographic support

6 Best practice and guidance for establishing and maintaining conformity assessment programs

This clause provides an overview of the principles, alternate approaches and considerations involved in developing conformity assessment programs to provide assurance that point-of-service (Clinical) systems, which are to be connected to EHR infrastructures, can be tested for conformity with the types of security and privacy requirements described in [Clause 5](#). This clause does not contain requirements.

Conformity assessment services for health software are needed by countries and economies for a wide variety of purposes including:

- demonstrating to purchasers that health software meets required specifications;
- protecting the health and safety of subjects of care;
- improving international trading opportunities;
- ensuring the compatibility and interoperability of components within and between complex systems.

In context of demonstrating that security and privacy requirements are met when POS clinical systems are connected with EHR infrastructures and/or communicate with other POS clinical systems, conformity assessment or certification programs can address each of these objectives.

Countries have implemented varying approaches to their conformity assessment programs depending on their needs, and many countries are developing, enhancing or evolving their programs to address the increasingly complex interoperability requirements. This clause (and the further material provided in the introduction section of [Annex A](#)) leverages the 17000 series of standards developed by the ISO Committee on conformity assessment (CASCO), and applies these concepts to this health context, drawing from experiences that four countries have had up to a point in time (2010) in order to illustrate the various options and considerations involved in designing conformity assessment programs.

This clause will be of interest to governments, local authorities, professional chambers, software developers, health informatics societies, subject of care representatives and others who have an interest in developing and continuing to improve assessment programs to ensure conformity with their EHR interoperability requirements.