TECHNICAL SPECIFICATION

ISO/TS 14441

First edition
2013-12-15

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

Informatique de santé — Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité

Reference number
ISO/TS 14441:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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-part 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