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)

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to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn.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

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 logon.

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 preceded by a

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 recorded 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 8601:2004format, 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 infostructures, 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 infostructures 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.

6.1 Concepts

Conformity assessment is defined by ISO Committee on conformity assessment (CASCO) in ISO/IEC 17000:2004 as: "*demonstration that **specified requirements** relating to a **product (which includes software)**, process, system, person or body are fulfilled".*

There are several key components to this definition:

— there needs to be a set of specified requirements against which conformity can be assessed;

— there needs to be an objective means of demonstrating that these requirements are met;

— there needs to be a defined product, process, system, person or body involved.

In the context of this Technical Specification, the security and privacy requirements are set out in Clause 5 above. This set of requirements may be further constrained and supplemented by member countries and local agencies to address:

— their specific system contexts as defined in targets of evaluation, and

— their legal, business or technological needs, including requirements contained in suppliers' or purchasers' specifications, national, regional or international standards or governmental regulations.

In addition:

— the means for demonstrating that the requirements are met will vary between countries, but this Technical Specification will provide guidance based on CASCO's work, and the experience of member countries to date in performing conformity assessments for the integration of POS clinical systems into EHR infostructures;

— the scope of this Technical Specification focuses only on requirements for **conformity assessment,** recognizing that countries may also have additional certifications for the processes and people who develop maintain and implement these products in our complex health care technology environments.

The methods for demonstrating conformity include testing, inspection, suppliers' declarations of conformity and certification. Figure 1[1)] highlights the relationship between conformity assessment and the many components which influence its establishment through an illustrative model:

1) Figure 2 in the ISO document *Building trust: The Conformity Assessment Toolbox*, ISO Central Secretariat, February 2010

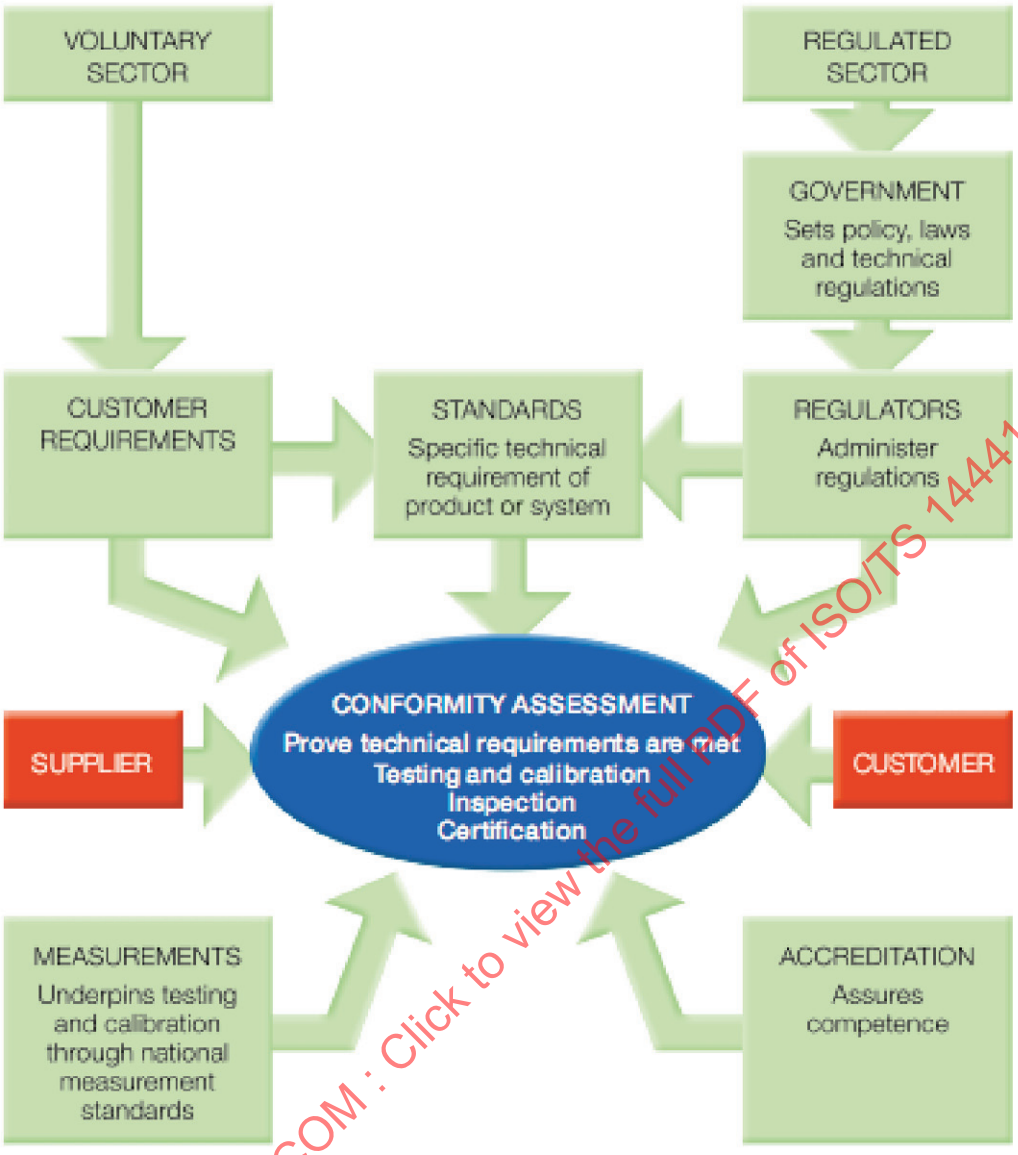

Figure 1 — Example of a conformity assessment model

Three concepts are particularly relevant here:

— **conformity assessment —** demonstration that **specified requirements** relating to a **product,** process, system, person or body are fulfilled;

— **certification** — **third-party attestation** related to products, processes, systems or persons;

— **compliance** — the action of doing what is necessary to meet a specified requirement.

One characteristic of conformity assessment is that it can take different forms, using different techniques according to the purposes for which it is being used. Whether the work is being carried out by the supplier of the products, the purchaser, or an independent body, there needs to be a clear understanding of the knowledge, skills and experience necessary for those performing the conformity assessment tasks. Every organization, whatever its role, should operate a management system in which the required competences are laid down and the means of demonstrating that individuals meet the requirements are specified. ISO/IEC 17065 provides general criteria for organizations operating product certification systems; while that standard is concerned with third-parties providing product certification, many of its provisions may also be useful in first- and second-party product conformity assessment procedures.

Too often "conformity assessment" is taken to mean certification and nothing else. In fact, conformity assessment can be undertaken by many people, including the supplier of a product or service, its purchaser and other parties which might have an interest such as insurance companies and regulatory authorities. It is convenient when talking about conformity assessment to refer to the parties as follows:

— first party: the person or organization that provides the object which is being assessed;

— second party: a person or organization that has a user interest in the object;

— third party: a person or body that is independent of the person or organization that provides the object, and of user interests in the object.

6.2 Conformity assessment processes

ISO/IEC 17000 sets out the "functional approach" to conformity assessment. The functional approach involves the basic process of selection, determination, review and attestation, plus surveillance when required.

Each stage involves the activities described below, the output from one stage being the input to the next.

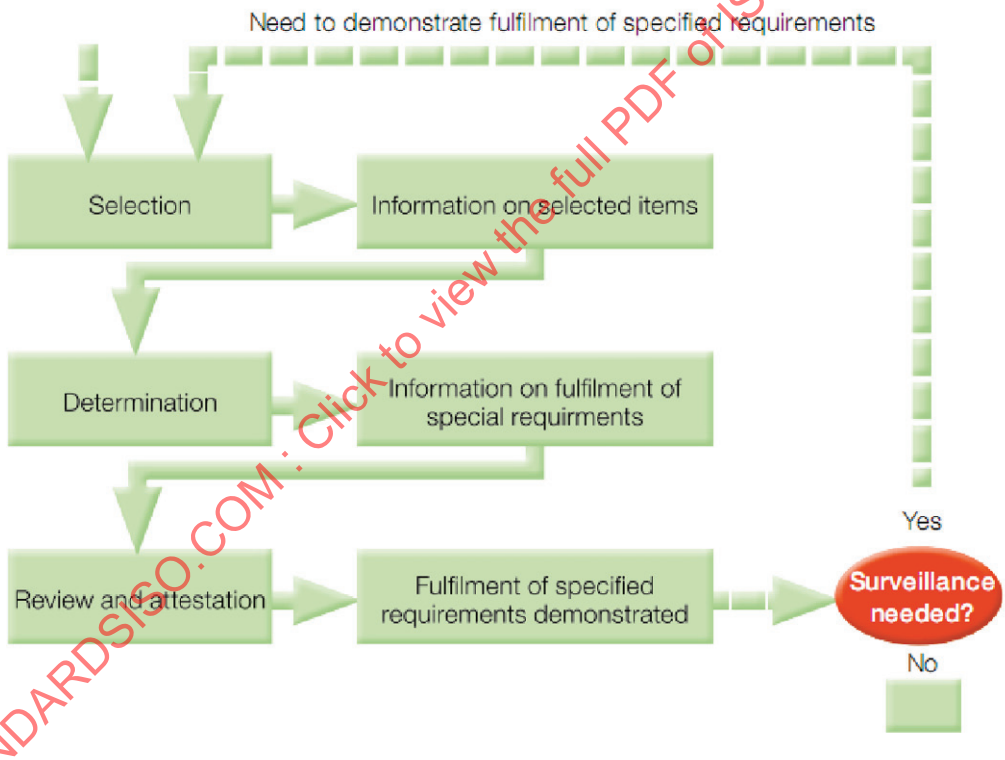

Figure 2 — Functional approach to conformity assessment[2)]

The activities carried out in each stage can include:

Selection

— Specification of the standard(s) or other document(s) to which conformity is to be assessed

— Selection of the examples of the object which is to be assessed

— Specification of statistical sampling techniques if applicable

2) The figure appears as Figure 4 in the ISO document *Building trust: The Conformity Assessment Toolbox*, ISO Central Secretariat, February 2010.

Determination

— Testing to determine specified characteristics of the object of assessment

— Inspection of physical features of the object of the assessment

— Auditing of systems and records relating to the object of assessment

— Evaluation of qualities of the object of assessment

— Examination of specifications and drawings for the object of assessment

Review and attestation

— Reviewing the evidence collected from the determination stage as to the conformity of the object with the specified requirements

— Referring back to the determination stage to resolve nonconformities

— Drawing up and issuing a statement of conformity

— Placing a mark of conformity on conforming products

Surveillance

— Carrying out determination activities at the point of production or in the supply chain to the marketplace

— Carrying out determination activities in the marketplace

— Carrying out determination activities at the place of use

— Reviewing the outcome from the determination activities

— Referring back to the determination stage to resolve nonconformities

— Drawing up and issuing confirmation of continued conformity

— Initiating remedial and preventive action in the case of nonconformities

Annex A looks at these techniques in greater detail, discussing the considerations involved in selecting techniques and providing illustrative examples of conformity assessment approaches that member countries have utilized.

Where the risks of nonconformity are high (e.g. public safety is at risk), it is usual to require an independent body to carry out some defined conformity assessment activities and at least to review the evidence of conformity and issue an attestation document such as a certificate. The body will usually charge for its services and will need to take time to complete its work.

The basic building block for conformance programs is a ***conformity assessment scheme,*** which relates to a particular group of objects having sufficiently similar characteristics that the same set of rules and procedures can be carried out under the same management for assessing conformity with the same set of specified requirements. The scheme owner will need to specify whether the work is to be carried out by one particular body or by any body which meets the scheme's requirements. Where third party conformity assessment is specified, consideration should be given to the need for these conformity assessment bodies to be accredited.

Several countries (e.g. US, UK, Brazil, and Canada) have introduced conformity assessment programs, sponsored by their national governments, for an expanding array of clinical software products and requirements as the clinical functionality and interoperability of POS clinical systems increases. These programs continue to evolve based on both experience and changing needs and Annex A represents a description of the approaches in place in the four countries at a point in time (2010). More recently,

multi-country approaches are also emerging, such as the European Patients Smart Open Services (epSOS) project.

In the case of the US, the Office of the National Co-ordinator (ONC) has accredited third party agencies to issue certifications according to conformance requirements and testing processes established by the National Institute of Science and Technology (NIST). In the other countries, certifications are provided by a single agency designated by the national government.

It should be noted that other models of conformity assessment, such as IHE, while not certification programs in and of themselves, do provide a method for software manufacturers to declare compliance and could be leveraged in a national certification program for example.

Frequently, the use of a *mark of conformity* is controlled through a licence issued by the owner of the mark or by an organization operating on behalf of the owner such as a certification body. The licence spells out the conditions under which the licensee can use the mark such as the restriction to use it only on products which the supplier has verified as conforming to the certified product type. Policing of the use of marks of conformity is vital for the interests of the owner and licensing body, since products bearing their mark are often produced under a system in which only occasional samples of product are verified by the licensing body.

The conformity assessment programs in the US, UK, Brazil, and Canada have each involved a process for issuing a certification mark and publishing a list of the health software products which passed the conformity assessment tests established for a defined list of requirements. These certifications are for both entire systems and in some cases a limited number of modules of those systems.

Annex A
(informative)

Conformity assessment programs — Design considerations and illustrative examples from member countries as of 2010

A.1 General

This annex provides further information on conformity assessment models, processes and other considerations, followed by examples of conformity assessment and certification program from four countries, in order to illustrate the alternative approaches than can be taken, depending on the circumstances in a particular country.

While most of the examples in this annex assume information sharing within national boundaries, the concepts still apply in a cross-border situation. Projects such as epSOS (European Patients Smart Open Services) in Europe offer live exemplars of this.

A.2 Conformity assessment programs — Design considerations

A.2.1 Authority

Conformity assessment techniques can be carried out by first, second or third parties: the supplier is the first party, the purchaser is the second party and an organization which has no commercial interest in the transaction is a third party. The decision as to which party should carry them out will depend on the local context. As indicated in 6.2 and illustrated in the four programs described later in this appendix, the third party assessment model involving a national certification is often adopted since the public safety risks of a nonconforming POS clinical system are considered high. However, in the absence of a national certification program, local health care organizations could, for example, adopt a second party conformity assessment process to mitigate the risks of implementing a non-conformant POS clinical system within their local EHR infostructure.

A conformity assessment *system* uses a common set of rules, procedures and management for several conformity assessment schemes. The rules and procedures may need to be detailed in different ways for different schemes, but there are advantages in terms of efficiency and consistency to working within a common framework.

Each conformity assessment scheme will have an owner. A number of different arrangements could apply and some examples are:

a) A software supplier could set up a conformity assessment scheme for its products, including testing, inspection and auditing, leading to the issuing of declarations of conformity.

b) A scheme could be developed by a certification body for sole use of its clients, in which case the certification body takes on full responsibility for the design, application, management and maintenance of the scheme. The body would be the scheme owner.

c) An organization such as a national government, a regulatory body or a trade association might develop a scheme and invite one or more certification bodies to operate it. In that case, the organization would be the scheme owner and would take responsibility for the operation of the scheme, probably through a contract or other formal agreement with the certification bodies.

d) A group of certification bodies, perhaps in different countries, might together set up a certification scheme. In that case, it would be necessary for the bodies, as joint owners of the scheme, to create a management structure so that the scheme could be operated effectively by all participating bodies.

A.2.2 Requirements for product certification bodies

The requirements for bodies certifying products, processes and services are specified in ISO/IEC 17065.

The basic purpose of ISO/IEC 17065 is to specify the requirements that should be met by a product, process or services certification body to demonstrate that it is competent, consistent and impartial. It is structured to cover the following aspects of management and operation of a certification body.

— *General requirements:* legal and contracting matters; management impartiality; liability and financing; non-discriminatory conditions; confidentiality, publicly available information.

— *Structural requirements:* organization structure and top management; mechanism for safeguarding impartiality.

— *Resource requirements:* certification body personnel; resources for evaluation.

— *Process requirements:* certification schemes; application; application review; evaluation; review; certification decision; certification documentation; directory of certified products; surveillance; changes affecting certification; termination, reduction, suspension or withdrawal of certification; records; complaints and appeals.

— *Management system requirements:* options; management system documentation; control of documents; control of records; management review; internal audit; corrective actions; preventive actions.

A.2.3 Cost and other considerations

When deciding on the appropriate conformity assessment arrangements for a particular situation, the costs of alternative approaches should be considered. While there are costs entailed in carrying out self assessment, as soon as another party becomes involved it is necessary to take account of what additional costs might be incurred and by whom. If the purchaser of a product decides to carry out their own assessment, they will generally have to bear the costs of employing their own inspectors.

If an independent body is contracted to carry out conformity assessment, the body will need to recover its costs from whomever it is working. In the case of product certification, it is usually the supplier who will engage and pay the certification body. The body's costs will not only relate to the assessors involved in the assessment work, but also all of the expenditure incurred in running its business, a proportion of which will be charged to each certification customer.

Thus the decision to establish a certification scheme can add to the costs incurred in the supply of the certified products. Similarly, a decision to require certification bodies to be accredited will add a further layer of costs as the expenditure incurred in operating the accreditation body has also to be recovered.

In addition to the direct costs of conformity assessment, there are other factors which have financial implications particularly for suppliers of certified products. The involvement of a third party can lead to delays in producing and delivering products depending on the time lag between the application for certification and the receipt of the certificate of conformity.

A.2.4 Liability

One of the basic principles of conformity assessment is that the organization which owns the object of assessment or places it on the market has the primary responsibility for its conformity with the stated requirements. The supplier of a product will have a contractual and a legal duty to the user that the product will perform its declared function and that it will not endanger the health or safety of the user, or others. Even if the supplier obtains a certificate from an independent body stating that the product conforms to the relevant specification, if anything goes wrong, the supplier remains responsible. Although the independent body might incur some degree of liability, particularly if it had been negligent in performing the conformity assessment, that would not absolve the supplier from the primary responsibility. Of course, misuse by the end user, particularly a failure to carry out proper maintenance, could absolve the supplier from liability for subsequent damage and its consequences.

A.2.5 Conformity assessment program design

The design of a conformity assessment program needs to clearly define the object of conformity assessment, including the need for sampling or selection of specimens to be used for determination activities. Selection may also include choice of the most appropriate procedures (for example, testing methods or inspection methods) to be used for determination activities. It is not uncommon that new or modified methods need to be developed to conduct determination activities. It will be necessary to select the appropriate locations, conditions, and individuals to perform the procedure(s). Finally, additional information may be needed in order to perform determination activities so that the demonstration that specified requirements are fulfilled will be effective. For example, the scope of testing to be covered by laboratory accreditation needs to be identified before appropriate determination activities can be performed.

A.2.6 Compliance statement

Regardless of whether any other parties are involved in the conformity assessment, there will always be some form of declaration of conformity by the supplier of the product or service. The declaration might take the form of an advertisement or leaflet describing the features of a product or could be incorporated in a formal document setting out the identification of the supplier and the product, the specification of the standards or other documents to which conformity is being declared, perhaps the particular regulations with which the item complies and the signature of a responsible person. Even the placing of the supplier's name, trade mark or logo on or in conjunction with the product implies that it conforms to the supplier's specification. ISO/IEC 17050 (all parts) provides guidance on the content of a supplier's declaration of conformity.

A.2.7 Determination: Testing procedures and environments

ISO/IEC Guide 67 describes seven major types of product certification systems, while noting that the elements in those systems can be combined in other ways to create additional systems. These systems may include one or more of the following components:

— samples requested by the certification body;

— determination of the relevant product characteristics by testing (ISO/IEC 17025) or assessment;

— auditing of the production process or quality system;

— review of the test or assessment reports;

— attestation of conformity;

— issue of a licence to use certificates or marks on the products;

— surveillance by testing or inspection of samples from the factory or from the market.

The experience of the four countries' conformity assessment programs (as described in Annex A) indicates that each has deployed a combination of these techniques. In recognition of the patient safety risks, countries are increasingly moving to product certification by mandated third parties, combined with increased emphasis on conformity assessment by health care delivery organizations where multiple software products need to be integrated and supported in facilitating the flow of patient information across the points of care to improve patient safety, quality and outcomes. As increasingly sophisticated and interoperable POS clinical systems are implemented, more and more attention is also being paid to the ongoing surveillance and re-assessment of systems as software and standards changes occur in the EHR ecosystem. The parallel focus in many countries of managing the patient safety risks associated with health software will also help to attenuate risks associated with software quality control, configuration, implementation and end user risks.

A.2.8 Review and attestation

In the functional approach (Figure 2 in 6.1), review and attestation are presented as a combined activity. It is possible, though, for different people to carry out each of them. What is important is that neither activity should be carried out by a person who has been involved in the determination activities. As the risks of nonconformity rise, so the degree of independence of the reviewer(s) should increase.

The reviewer needs to have the necessary competence relating to the specified requirements, the object being assessed and the determination activities that have been used. For example, knowledge of the test methods would enable the reviewer to identify anomalous results and refer the report back to the person(s) who carried out the test for it to be repeated.

The conclusion of the review stage is a recommendation for a statement of conformity to be issued. The recommendation should make reference to the report and to any other findings from the review which substantiates the conformity (or non-conformity) of the object with the specified requirements.

A.2.9 Versioning and surveillance

In the increasing interoperable world of the EHR, where POS clinical systems have an increasing number of interface points from an information (e.g. new code sets), policy (e.g. new privacy rules) and a technology perspective, it is important to have clear policies that govern the need for re-attestation when there are changes in either or both of the POS clinical system and the EHR infostructure. Re-testing of interoperability needs to take place in a disciplined way with changes being characterized as major or minor, and test harnesses and other mechanisms used to make re-testing practical and affordable during the term of the certification.

Conformity assessment can end when attestation is performed, but where there is a need to provide continuing assurance of conformity, surveillance can be used. Surveillance systematically iterates conformity assessment activities as a basis for maintaining the validity of the statement of conformity. A complete repeat of the initial assessment is usually not necessary in every iteration of surveillance to satisfy this need.

In the case that the object is found not to conform, the person or organization responsible for the object, e.g. the development engineer or, for a second or third party situation, the supplier, should be informed and invited to make the changes necessary to achieve conformity. It is important that the reviewer does not suggest possible solutions so as not to lose their objectivity when the object is returned for a further review. Discussion of the assessment results is permissible so that the person or organization responsible can understand the cause of the nonconformity.

Assuring ongoing conformance, in an increasingly complex and interoperable EHR ecosystem, is an ongoing challenge for systems suppliers, purchasers and certification bodies, all of which have responsibilities for carrying out appropriate conformity assessment activities in their respective environments. In addition to having cooperative and pragmatic processes in place to reduce and manage risks with the software suppliers and implementers that occur with product changes, sound policies are required that allow certification bodies to make principle-based judgments about the degree of re-testing that is required when changes occur. Finally a sound surveillance system that involves vigilance by suppliers, implementers and the end users of these systems, and a responsive reporting system, is a critical component.

A.2.10 Education, marketing and communications

A.2.10.1 Declaration of conformity

A statement of conformity issued by a first party, e.g. the supplier of a product, or a second party, e.g. the purchaser, is known as a **declaration of conformity**.

A.2.10.2 Certificate of conformity

A statement of conformity issued by a third party (certification body) is a **certificate of conformity**. However the term used and the specific content can vary according to the object being assessed and the nature of the specified requirements.

A.2.10.3 Mark of conformity

It is common for products to bear marks of conformity, whether these are the supplier's own trade mark, a certification mark controlled by a certification body or a conformity mark required by legislation, such as the EU's CE marking. Advice on marks of conformity is contained in ISO/IEC 17030 and ISO Guide 27. Marks need to be distinctive and their ownership and conditions of use should be clearly stated.

In particular the use of a mark should not be misleading to purchasers and users of the products. For example, a supplier which has a certified management system conforming to ISO 9001 should not place the certification body's mark on its products, since that would imply that the body had certified the products.

Frequently, the use of a mark of conformity is controlled through a licence issued by the owner of the mark or by an organization operating on behalf of the owner such as a certification body. The licence spells out the conditions under which the licensee can use the mark such as the restriction to use it only on products which the supplier has verified as conforming to the certified product type. Policing of the use of marks of conformity is vital for the interests of the owner and licensing body, since products bearing their mark are often produced under a system in which only occasional samples of product are verified by the licensing body.

The four national health software certification programs were designed with these principles in mind.

A.3 Example 1: United Kingdom

A.3.1 Certification program overview and objectives

The description in this clause relates to the information governance regime in place in the NHS in England in 2010. At the time that this Technical Specification was written, the information governance regime for the NHS in England was being revised. Results of this process will provide an opportunity for further alignment when this Technical Specification subsequently undergoes review by ISO.

NHS Connecting for Health (CFH), as part of the Department of Health Informatics Directorate, runs a number of centralized assurance processes designed to ensure that:

— the requirements of national NHS IT contracts are being met i.e. the Local Service Provider contracts e.g. CSC, the National Service Provider contracts e.g. BT Spine, the GP Systems of Choice (GPSoC) framework and the Additional Services Catalogue (ASCC);

— NHS CFH owned requirements are met as required by services at all levels e.g. Personal Demographics Service (PDS), Information Governance, (IG) and also more complex clinical requirements such as Summary Care Record (SCR) and Electronic Prescription Service (EPS);

— any systems needing to connect directly to the national spine will need to meet at least the Information Governance (IG) requirements and at least one other set to have some functionality, so will be subject to these processes.

The Common Assurance Process (CAP) is the assurance process used to ensure that NHS CFH requirements are being met as required for all non LSP and non NASP contracted solutions. LSP and NASP solutions have their own specific contract assurance processes, based on the same principles as CAP. The Common Assurance Process is governed at the operational level by the CAP Operations Board. This is made up of managers from across the assurance stakeholder base. This Board currently reports in to a Programme Board which meets by exception. The costs needed to run CAP for a specific release should be factor into an individual programme/project business cases and programme.

A.3.2 Scope of systems covered

Any system – irrespective of care setting – that needs to connect to the national (EHR) spine will need to follow an assurance process. There are more than 80 systems using the assurance processes across many care settings including primary healthcare, acute healthcare, social care, child health, pathology, X-ray.

A.3.3 Range of clinical, administrative, non-functional and interoperability requirements included

This depends on what is needed of the solution, as specific requirements are defined for specific services. That said, the clinical safety assurance process is common for all, and each system needs to meet the Information Governance requirements for security and privacy.

Compliance with the following foundation modules is a pre-requisite to applying for certification for any of the national EHR services (business domains) such as Choose and Book, Referrer Compliance, or Electronic Prescribing. The current Foundation Modules, in order of precedence, are:

— Information Governance (IG);

— Care Record System (CRS) Infrastructure (e.g. National Spine) and Standards;

— Personal Demographics Service (PDS).

These modules contain a set of generic requirements applicable to all systems seeking compliance to a business domain. All of these foundation modules are mandatory.

Compliance can be sought for a business domain and its foundation modules together or can be achieved separately.

The Information Governance requirements (security and privacy) requirements cover:

— Spine Authentication – support for single sign on and smartcards, integration with the NHS CRS Spine Security Broker (SSB) and spine session management;

— Local Authentication in the absence of a Smart Card or SSB;

— Role Based Access Control (RBAC) – support for the National set of roles and activities for authorising access to system functions and data with RBAC data retrieved from SAML assertions and/or SDS; and local RBAC requirements in the absence of Smart Cards or SSB;

— Consent – for authorising sharing of personal sensitive information held by NHS CRS about a patient;

— Legitimate Relationship Service – for authorising user access to individual patient records;

— Sealed Envelopes – allowing patients to exercise choice about the level of visibility of information stored about them;

— Content Commitment – allowing the electronic equivalent of ink signatures;

— Audit Logging – recording users' actions in relation to NHS CRS personal data;

— IT Security – time stamping, storage, testing, communications and access controls;

— Information Security Management System – ensuring appropriate governance structures and processes.

A.3.4 Establishment and maintenance of the requirements being certified against

The security and privacy requirements are owned by the IG SME team within the Technology Office, and updated on around an annual basis as reference documentation is updated, clarifications requested by suppliers are rolled in, and technical changes need to be taken account. Proposed changes largely come

from experience with operating the assurance process around the requirements, although some are as a result of policy changes around the choices offered to patients around consent, etc. The starting point several years ago was a set of security and Information Governance requirements set out at the start of the National Programme for IT.

A.3.5 Duration of the certification and management of new releases

The "certification" applies to a particular version; it is not time-dependent. No system remains unchanged for long, so that as new versions are created – either for supplier-initiated changes such as maintenance releases, or for additional Spine-related functionality is introduced – decisions are made by CAP about the degree to which a product's assurance status needs to be re-validated. In the future, when significant CFH-related changes may decline in number/frequency, it may be appropriate to consider time-based re-validation.

A.3.6 Conformance testing process

The review process begins with the vendor in the design stage. Testing is carried out in the NICA test environments, leading to a "First Of Type" implementation in controlled circumstances in production. Timescales are up to the supplier in terms of getting their system to a state in which they are allowed into the integration-test environment, and how long that testing may take.

There is a security and Information Governance baseline published which reflects the particular requirements of the programme – such as Smartcard authentication – together with industry-standard guidance over, e.g. cryptographic algorithms to protect data in transit and at rest. We include application-level penetration testing to cover more general software-related potential issues. All this is at a system, software level. At the organizational level – both for supplier organizations and for deploying organizations – there is a separate process – the Information Governance Statement of Compliance including the Information Governance Toolkit to drive compliance to ISO/IEC 27001.

A.3.7 Summary of experiences to date

The NHS has been operating the CAP program in its current form for approximately five years, during which time the processes have been tuned and updated, but not substantively changed. The UK's experience is that it is important to develop a strong working relationship with each systems vendor, with discussions beginning at the design stage where changes in the POS clinical system or the national EHR infostructure are being contemplated. CAP staff will provide advice to the vendor, but are careful not to become the designers. One a system has been certified, the track record of the vendor, together with the expected magnitude of the change, are considered in determining the level of re-testing that needs to be done by CAP in maintaining the POS clinical systems certification. Consideration is currently being given to ways in which the process could be streamlined in some situations – for example by providing vendors who have a strong track record and mature processes for meeting the CAP requirements to carry out more of the CAP processes on a self-auditing basis.

Given the focus on local system-system integration at the health care delivery organization level, a complementary approach [the Interoperability Toolkit (ITK) Accreditation Process] is being developed. ITK, however, only focuses on interface functionality for the exchange of information and does not include information governance (authentication, audit, consent), clinical safety, non-functional testing, national EHR (Spine) connectivity or general application functionality. In this approach, the systems suppliers are provided with a test harness and test cases in order to demonstrate their 'first party conformity' with the requirements.

A.4 Example 2: Brazil

A.4.1 Certification program overview and objectives

In Brazil there is a single national program for certification of electronic health record systems (EHRS), whose standards and requirements were defined by the Brazilian Health Informatics Society (Sociedade Brasileira de Informática em Saúde - SBIS) under the legislation of the Brazilian Federal

Council of Medicine (Conselho Federal de Medicina - CFM), the federal agency responsible for regulation and supervision of medical practice in the country. There are no programs in the regional or local levels.

This program started in 2002 by establishing a working group to discuss the necessary processes and requirements. This group initially published the document entitled "Safety, Content and Features Requirements for Electronic Health Record Systems", that after evolution became, in 2008, the "Certification Manual for Electronic Health Record Systems". The 2009 Edition is currently in effect and the 2010 Edition is under construction.

The Brazilian program is managed and operated by the Brazilian Health Informatics Society (Sociedade Brasileira de Informática em Saúde - SBIS), a non-profit scientific society, under delegation from the Brazilian Federal Council of Medicine (Conselho Federal de Medicina - CFM), the federal agency responsible for regulation and supervision of medical practice in the country.

A.4.2 Scope of systems covered

The Brazilian certification program is currently focused on systems for ambulatory/outpatient care. Later this year, categories will be added for hospital/inpatient care and for electronic content management (ECM) systems. In the coming years other new categories will be added.

A.4.3 Range of clinical, administrative, non-functional and interoperability requirements included

The ambulatory care category has 113 requirements defined, divided into the following groups.

Structure and content requirements:

— EHR structure

— Structured data

— Administrative data

— Clinical data

— Data types

— Reference data

— Contextual data

— Links

— Health concepts representation

— Representation of text

Features requirements:

— Support for clinical processes

— Health problems and other issues

— Clinical reasoning

— Decision support, clinical protocols and alerts

— Therapeutic planning

— Orders and service processes

— Integrated care

— Quality assurance
— Data capture
— Retrieval, queries and views
— Presentation of data
— Scalability and performance
— Message protocols
— Record exchange
— Consent
— Medico-legal
— Actors
— Clinical competence and governance
— Faithfulness
— Preservation of context
— Permanence
— Version control
— Ethical
— Patient rights
— Cultural issues
— Evolution

The security and privacy requirements have been developed in 2 levels:

a) Safety Assurance Level 1 (in Portuguese: Nível de Garantia de Segurança 1 - NGS1)

b) Safety Assurance Level 2 (in Portuguese: Nível de Garantia de Segurança 2 - NGS2)

The NGS1 applies to local or networked systems that don't provide the use of digital certificates, and therefore do not allow discarding the paper records. Every certified system must meet minimally at this level. It consists of 53 requirements divided into the following groups:

— Software version control
— User identification and authentication
— User session control
— Access authorization and control
— EHR availability
— Remote communication
— Data security
— Audit
— Documentation

— Time

— Events notification

The NGS2 applies to systems that provide the use of digital certificates for signing and authentication, and therefore allows discarding the paper records. This level is optional and, if applied, must be made in addition to NGS1. It consists of 25 requirements divided into the following groups:

— Digital Certificate

— Digital Signature

— User authentication using digital certificate

— Document scanning (for future use with then ECM category)

A.4.4 Establishment and maintenance of the requirements being certified against

Most of security and privacy requirements were based on ISO standards, especially ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 15408 (all parts).

The Brazilian Federal Council of Medicine provided initial funding in the order of USD 100 000 for the program development, with the bulk of the work carried out voluntarily by a group of shareholders from SBIS. Currently, part of the work still comes from voluntary actions, and another part funded by the fees charged for courses provided by SBIS and the fees paid by vendors on audits performed. The set of certification requirements was established and is maintained by a working group formed by members of the SBIS, and is based on national and international standards, in addition to national programs rules and relevant legislation. Before being published, the set of requirements is subject to public review, where any interested person or professional can provide feedback about or suggest changes to the proposed texts. After the discussion and fine-tuning, SBIS publishes the requirements by a new edition of the Certification Manual.

A.4.5 Duration of the certification and management of new releases

The approved systems receive a certificate and a seal, which can be used by the vendor in its promotional materials, under specified criteria in the Certification Manual and the contract between the vendor and SBIS.

Each certificate is valid for 2 years, unless it is revoked due to any violation of the program rules. There are no re-tests during this period, since the certificate is assigned to a particular system in a given release, and under a certain issue of the requirements. The supplier is obliged to report such information in its promotional materials and marketing, or should state clearly what is the name and version of the certified system and what is the year of publication of the requirements when compliance was audited.

If the supplier wants to extend the certificate to a new version of the system, then new tests will be performed, and under compliance confirmation the certificate will be extended to this new version. This action, however, is not mandatory, and the supplier can maintain an old certified version without certifying the new one.

After the expiration date, the supplier may submit the system to a new audit process, obtaining, in case of success, a new certificate for it.

A.4.6 Conformance testing process

The tests run in audit sessions, performed in person at SBIS office in Sao Paulo with the participation of 3 auditors and 3 professionals from the supplier, and have an average duration of 3 days for each system evaluated. Sessions are recorded, including the video displayed by the audited system and audio captured from the room, resulting in DVDs that are stored in SBIS for later consultation in case results are contested.

The audit utilizes test scripts defined in the "Operational Manual of Tests and Analysis for EHRS Certification", prepared by SBIS along with the Certification Manual. As the scripts run, auditors verify system compliance for each mandatory requirement from the listed categories, yielding a final result after the tests completion.

To obtain the certificate, the system must demonstrate compliance to all mandatory requirements of the listed categories; otherwise the certificate will not be granted. In case of non-compliance, the developer may apply to a complementary audit session (second cycle) within 90 days, considered as a "second chance" to solve the faults found and re-present the system with the necessary corrections.

After the end of the audit session, the results taken by the auditors (first level) are submitted to the Certification Process Manager (second level), which evaluates and submits to the Certification Committee (third level), comprising three people who ensure the whole process was conducted according to the program rules. Upon an approval, the Certification Committee grants the certificate and seal to the evaluated system. Otherwise, the developer is notified about the failure and the proper reasons.

Considering all the steps to be met from the entry of a system into the program until the final committee decision, each process takes around 60 days, provided a second audit cycle (described above) is not needed.

A.4.7 Summary of experiences to date

Theory and practice often differ – conformity assessment for EHR systems is certainly no exception. Some of the requirements, rules or processes originally devised needed to be revised when implemented, sometimes in its concept, other times in the execution mode and in the documentation. The program has matured and continues maturing.

Some key lessons learned in Brazil until now:

— It is possible to create and implement a national certification program in a high quality level, even with low resources and in a large country. We found several obstacles along this way, but none that we couldn't overcome.

— The adoption of national and international established standards was crucial to our project success.

— The program operational processes must be adapted to the national and the health sector properties, especially to its cultural and economic condition. Successful cases in other countries or sectors were not necessarily going to work well in our project. So we tailored our program operation to our conditions, which has been critical to its success.

— Radical and sudden change in the health sector could derail the entire project. Gradual implementation of changes is proving very effective, enabling the program's success.

'Certainly the biggest impact caused by the Brazilian certification program until now was the confirmation that it is indeed possible to promote a qualitative leap in the market of electronic health record systems in the country. Spoiled by never having actually been appraised since the beginning of its existence, most of the developers argued until a few years ago that the certification program would not result in anything, it would be a utopian and unworkable process, and that no supplier or consumer company would pay attention to it. Now, almost 8 years elapsed from the initial activities and almost 2 years of its effective implementation, we can state that the certification program is an unqualified success, given the high mobilization of the healthcare systems industry and their commitment in adapting their systems to the program requirements. Fundamental security, privacy and content concepts, previously ignored by the vast majority of systems, began to be discussed and implemented on an increasing scale, making us believe in a really good level for the EHR systems in the country within a few years.

As a result of this qualitative leap, institutions and health professionals have begun to benefit from the use of better and safer systems. Gradually, it will be easier and safer to choose an EHR solution, reducing the risks before experienced by users of these systems. As a final consequence, we'll be improving the health care processes supported by these solutions. All this has begun and will proceed ever more intensively, on an evolutionary path of no return.'

A.5 Example 3: Canada

A.5.1 Certification program overview and objectives

In Canada, the federal government develops nation-wide health care policy, including the definition of a common core of health services that is universally available across the country. The federal government works closely with the provinces and territories, each of which is responsible for delivering health care services within their own jurisdiction. In 2000, the federal government in collaboration with the provinces and territories in Canada developed an independent agency, Canada Health Infoway, to coordinate a consistent approach to implementing electronic health record systems in Canada. Infoway has developed a common EHR architecture, is the focal point for developing pan-Canadian standards and provides funding to assist the provinces and territories in implementing their electronic health record (EHR) systems, which follow this architecture and the associated interoperability standards. One service provided by Infoway to allow software suppliers (vendors) of component parts of the electronic health record (EHR) to demonstrate their compliance with national health IT standards is certification.

The objectives of *Infoway* Certification Services are to:

— Increase the recognition, acceptance and adoption of trusted, interoperable health information solutions in the Canadian marketplace;

— Reduce the cost and risk to vendors, purchasers and users of these solutions in Canada; and

— Ensure privacy, security and interoperability requirements are met.

A.5.2 Scope of systems covered

When Canada Health Infoway developed a certification program in 2009, its initial focus was on the pre-implementation of an emerging new breed of system - consumer health platforms. To date, one product has been certified, a Canadian implementation of the Microsoft HealthVault.

Over the last two years, certification programs have been development for components on the EHR, in keeping with the Infoway architecture and blueprint. These include:

— Consumer health applications (Nov 2009)

— Client registry (Nov 2009)

— Provider registry (Nov 2009)

— Immunization registry (Nov 2009)

— Drug information systems (July 2010)

— Diagnostic imaging/PACS/RIS (July 2010)

— Other EHR components such as Lab data repositories are expected

A certification program is now being developed for the first major group of point-of-service (Clinical) systems – electronic medical records (EMRs) to provide pre-implementation assurance of their interoperability with Canada's EHR infrastructure from a privacy and security perspective, to be able provide access patient lab and diagnostic results, do ePrescribing and access patient drug profiles, record immunizations and access a patient's current immunization status, etc. It is also expected that the Infoway certification program will then begin to include some EMR-EMR system interoperability components (such as eReferrals between GPs and specialists in 2012.

Several provinces have also developed ongoing conformance testing processes and requirements for EMRs which will connect to each province (or territory)'s own instance of the EHR infrastructure. These conformance assessment processes address interoperability at the more granular level of deploying and maintaining integration on an ongoing basis between EMRs and the EHR infostructure within each province's health system. Discussions are now underway between Infoway and provinces who have

implemented conformance assessment processes at their jurisdictional level, to align requirements, processes and test data sets and achieve as much reciprocity as possible so that software suppliers do not have to re-test their systems unnecessarily.

A.5.3 Range of clinical, administrative, non-functional and interoperability requirements included

Infoway's certification assessment criteria focus on functionality, privacy, security, interoperability and management, using accepted standards within the Canadian and international health information communities, and enhanced with input and feedback from a broad range of health industry stakeholders.

The framework for the assessment criteria is shown in Table A.1. It consists of two classes of criteria:

— **Solution** – Refers to the aspects of the health information solution's functionality, privacy, security and interoperability that are assessed.

— **Management** – Refers to how the organization providing the solution manages risk, data, system security, as well as third party services and solution accreditation.

Table A.1 — Framework for assessment criteria

Solution "The What"				Management "The How"
Functionality	**Privacy**	**Security**	**Interoperability**	**Control**
Identification	Accountability	User identity management	Diagnostic imaging	Risk management
Data accuracy	Transparency	Access control	Laboratory	Data management
	Data safeguards	Data integrity	Drug	System security
	Identifying purposes and limiting collection	Data availability	Shared health record	Solution accreditation
	Limiting use, disclosure and retention	Audit	Client demographics	Third party services
	Compliance	Logging	Provider demographics	
	Consent	Data confidentiality		

[a] A limited number of additional functional criteria may need to be added based on class requirements of each technology solution.

[b] This criterion applies for consumer health solutions.

A.5.4 Standards basis of certification

Standards used to create the assessment criteria include:

— **Functionality:** Canada Health Infoway Electronic Health Record Privacy and Security Requirements.

— **Privacy:** Canada Health Infoway Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture; Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA); The Canadian Standards Association's Model Code for the Protection of Personal Information – CAN-CSA-Q830-03.

— **Security:** Canada Health Infoway Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture; The International Organization for Standardization's Code of Practice for Information Security Management – ISO/IEC 27002; The National Institute of Standards and Technology's Recommended Security Controls for Federal Information Systems – NIST SP800-53;The USA Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

— **Interoperability:** Infoway pan-Canadian Standards and Conformance Profile Definitions for diagnostic imaging, laboratory, drug, shared health record, and demographic information.

— **Management:** The IT Governance Institute Control Objectives for Information and Related Technology (COBIT); The Information Technology Infrastructure Library (ITIL).

A.5.5 Establishment and maintenance of the requirements being certified against

The security and privacy requirements are owned and maintained by a certification team at Canada Health Infoway. Requirements are maintained and updated in accordance with pan-Canadian standards established by the Infoway Standards Collaborative, which is composed of provincial and national level stakeholders from governments, health delivery agencies, professional groups and health system vendors.

A.5.6 Certification process

The certification process consists of four steps:

a) **Certification application**: The package contains:

— an application for certification form;

— a self-assessment (that is to be completed and submitted as part of the application process);

— a copy of the pre-implementation certification legal Agreement.

b) **Product assessment: Assessment** of the product is the critical step in the certification process and the vendor has 90 days from submission of the Application Package to complete this step which includes:

— document Review – an administrative and expert review of the vendor self-assessment and supporting documentation;

— demonstration – a presentation of the solution by the vendor to experts, demonstrating that it meets the assessment criteria, typically via a web conferencing and demonstration environment.

— **Assessment report:** Infoway will assemble the assessment results into a comprehensive report and notify the vendor within five working days of the certification decision.

— **Maintenance:** To maintain certification, the vendor is required to notify Infoway of adverse events as well as any product changes that may affect conformance with assessment criteria.

The certification process is strictly confidential. Names of products and/or vendors are not published or otherwise made available by *Infoway* at any time during the process. Safeguards have been put into place such that the use and disclosure of all information submitted through the certification process including the product name, vendor, self-assessment and any supporting documentation provided during the process remains strictly confidential. In addition, the certification assessment team is bound by strict non-disclosure agreements. *Infoway* will only publish the names of products that have been successful in achieving certification, with details of that product posted on *Infoway*'s website.

All certified products receive a certification mark, which bears the Infoway logo. The certification mark can be used in marketing and promotional material related to the certified product.

A.5.7 Summary of experiences to date

Infoway has historically not provided funding for point-of-service (Clinical) systems connecting to the provincial EHR infostructures, although the pan-Canadian interoperability standards that are maintained through the Standards Collaborative hosted by Infoway do cover POS clinical system to EHR interoperability. In Canada's federated health care approach, each province/territory has implemented these standards with local adaptations and there are often legacy POS clinical systems acquired in each province prior to these standards being in place.

In 2011, however, Infoway will begin implementing a new program to provide funding to provinces and territories to stimulate the adoption of EMRs in physician offices (which will use pan-Canadian standards to integrate with provincial EHR infrastructures), Infoway has developed specifications and tools to aid POS clinical system software vendors in implementing privacy, security and data interface requirements using pan-Canadian standards and the Infoway privacy and security architecture. As this occurs, EMRs will be certified by Infoway for these privacy, security and interoperability functions. Discussions are now beginning between the provinces and Infoway to further harmonize both the way in which pan-Canadian standards are implemented and to better align Infoway pre-implementation certification processes with the conformance testing processes that provinces are investing in to ensure that point-of-service (Clinical) systems interoperate correctly with their EHR infostructures.

In summary, there a mix of approaches is developing in Canada for conformity assessment, with:

— pre-implementation certification developing at the national level through Canada Health Infoway for many of the Infoway-funded EHR services such as data repositories and registries that are required provincially, and,

— conformance assessment programs developing at the provincial/territorial level to ensure that point-of-service (Clinical) systems in physician offices, pharmacies and hospitals will interoperate with each province's unique implementation of the Infoway EHR infrastructure.

A.6 Example 4: United States

A.6.1 Certification program overview and objectives

In the United States, the federal government has both an important role in establishing national health policies and standards, as well as in providing health care directly to certain groups (such as those in the active military and for veterans). While health care delivery is delivered to the majority of its citizens through a wide range of public, non-profit and for-profit organizations, the federal government through its funding of health care organizations through Medicare (senior citizens) and Medicaid (low income people) has significant leverage by establishing reimbursement requirements and incentives.

Given the importance of improving health care quality and continuity, and the many existing barriers health care data exchange between the points of care where patients are treated due to competitive, clinical, administrative and technical barriers, in February 2009, Congress enacted the Health **Information Technology for Economic and Clinical Health (HITEC) Act** to increase the use of Electronic Health Records **(EHR)** by physicians and hospitals which allocated:

— **USD 18 billion** through the Medicare and Medicaid reimbursement systems as incentives for hospitals and physicians who are "meaningful users" of EHR systems.

— **USD 2 billion** to the Office of the National Coordinator for infrastructure necessary to allow for, and promote, the electronic exchange and use of health information for each individual in the United States, updating the Department of Health and Human Services' technologies to allow for the electronic flow of information; integrating health IT education into the training of healthcare professionals; and, promoting interoperable clinical data repositories.

— **USD 1 billion** to be made available for renovation and repair of health centres and for the acquisition of health IT systems.

— **USD 550 million** for – among other things – the purchase of equipment and services including, but not limited to, health IT within Indian Health Service facilities.

— **USD 400 million** for comparative effectiveness research on how use of electronic data impacts healthcare treatments and strategies.

— **USD 300 million** to support regional and sub-national efforts towards health information exchange.

— **USD 40 million** to be used by the Social Security Administration to use EHRs to submit disability claims.

The Office of the National Coordinator for Health Information Technology (ONC) was mandated to adopt an initial set of HIT standards, and create an incentive program for meaningful users of EHR certified technology. ONC has two advisory committees, the HIT Policy and HIT Standards committees.

— The HIT Policy Committee is charged with making recommendations to the National Coordinator for Health Information Technology on a policy framework for the development and adoption of a nationwide health information infrastructure, including standards for the exchange of patient medical information.

— The HIT Standards Committee is charged with making recommendations to the National Coordinator for Health Information Technology on standards, implementation specifications, and certification criteria for the electronic exchange and use of health information.

In July 2010, the ONC released the final rule covering the initial standards, implementation specifications, and certification criteria. The CMS final rule outlines provisions governing the Medicare and Medicaid EHR incentive programs and definitions of meaningful use.

Given the demand this is anticipated to create for certified systems, the ONC has created a temporary certification program where organizations can apply to be accredited as an ONC – Authorized Testing and Certification Body (ONC-ATCB) for one or more of the modules (including areas such as electronic prescribing, privacy and security, laboratories, quality, etc.) as defined in the Standards and Certification Criteria Final Rule. Applicants are required to include the results of self audits under ISO/IEC 17065, in addition to meeting other criteria. Currently there are five authorized testing and certification bodies, one of which is the Certification Commission for Health Information Technology (CCHIT) which further described below. The normative certification criteria and test procedures are specified by the National Institute of Standards and Technology (NIST).

NOTE In January 2011 the ONC issued a final rule to establish the permanent certification program for health information technology: "The permanent certification program provides new features that will enhance the certification of health information technology, including increasing the comprehensiveness, transparency, reliability, and efficiency of the current processes used for the certification of electronic health record (EHR) technology. Meaningful use of Certified EHR Technology is a core requirement for eligible health care providers who seek to qualify to receive incentive payments under the Medicare and Medicaid Electronic Health Record Incentive Programs as authorized by the Health Information Technology for Economic and Clinical Health (HITECH) Act …. Our goal is to make the transition to the permanent certification program as seamless as possible."

NIST will develop a laboratory accreditation program for organizations to be accredited to test health information technology for purposes of the permanent certification program. "Based on NIST's technical expertise and the strong relationship formed between ONC and NIST during the successful implementation of the temporary certification program, the use of NVLAP is expected to enhance testing under the permanent certification program and its objectivity overall".

Features of the permanent certification program include:

— organizations must first be accredited in order to test and/or certify health information technology;

— certification bodies are required to conduct post-certification surveillance perform "gap certification."

A.6.2 Scope of systems covered

Certified EHRs or modules are certified and provide assurance that they provide the necessary technological capability, functionality and security to help care providers meet the 'meaningful use' criteria and receive the incentive payments. Both hospital systems and ambulatory systems for physician clinics (EMRs) are included.

A.6.3 Range of clinical, administrative, non-functional and interoperability requirements included

The requirements cover a number of areas including:

— core data sets to support a range of clinical functions such as maintaining problem and allergy lists, prescribing, clinical quality measures/reports, and the exchange of clinical summaries;

— patient demographics and ability to provide patients with summary information on their visits;

— protecting electronic patient information, which includes more basic elements of security:

  — access control

  — emergency access

  — automatic system logoff

  — audit logs

  — authentication

  — encryption.

According to the national health IT coordinator, Stage 2 of the meaningful use requirements is expected to be "cantered around standards and certification criteria, privacy and security protections, governance of exchange and public trust and interoperability".

A.6.4 Duration of the certification and management of new releases

Since certifications under the Meaningful Use Final Rule as being provided under the Temporary Certification program, the existing certifications will not expire until the new Permanent Certification Program is in place – i.e. not before 2012-01-01.

NOTE CCHIT is one of six ONC Authorized Testing and Certification bodies (ATCBs) in the US, and continues to offer their traditional CCHIT certification based on a broader set of functional criteria. The 2011 certifications provided by CCHIT through their in-house program expire 2014-12-31.

A.6.5 Conformance testing process

ONC-ATCBs are required to use ONC-approved test procedures, developed in collaboration with NIST, to test and certify EHR technology against the standards, implementation specifications, and certification criteria adopted by the Secretary. In collaboration with ONC, the National Institute of Standards and Technology (NIST) developed the functional and conformance testing requirements, test cases, and test tools to support the proposed Health IT Certification Programs. These conformance test methods (test procedures, test data, and test tools) help ensure compliance with the *Meaningful Use* technical requirements and standards.

A.6.6 Summary of experiences to date

The US has evolved their approach significantly in recent years with the establishment of the Office of the National Coordinator (ONC) and establishment of their 'meaningful use' requirements. While the US certification program is being implemented in stages and has not reached its fully operational state, a few of the more unique elements in their approach are:

— The focus on meaningful use, which emphasizes the capture, exchange and clinical use of information to support improvements in tracking disease, coordinating care and decision support;

— A three stage approach to progressively supporting health system quality, safety and efficiency improvements, which includes significant financial incentives for health care providers and organizations who demonstrate adoption and use of systems which are certified and tailors the certification requirements to specific types of systems;

— The use of accreditation as a mechanism for establishing multiple certification bodies, coupled with a staged approach to implementing meaningful use requirements, has provided the capacity to certify a large number of systems within a relatively short time frame.

Annex B
(informative)

Comparison of jurisdictional requirements

B.1 Overview

This annex compares requirements from four separate national projects to implement EHRs in Brazil, Canada, the US, and the UK. In addition, there are selected requirements from Japan and the Russian Federation. It is organized into the following categories:

a) **Patient consent to collect, use or disclose personal health information**, including recording consent, types of consent, communicating consent, consent override in emergencies, logging consent override, data masking, consent given by a substitute decision maker, and notifying patients of changes to consent

b) **Limiting use and disclosure of personal health information**

c) **Patient access to personal information and correction of inaccurate information**

d) **Data accuracy**

e) **User identification and authentication**, including user identification; user IDs; user authentication; system authentication and network node authentication; authentication methods; protecting user profiles; passwords; failed login attempts; and user feedback during authentication

f) **Privilege management**, including access privileges, reporting access privileges, restrictions on access privileges, delegation of access privileges, and removing access privileges

g) **Acceptable use**, including notifications to users

h) **Session security and timeout**, including user session and connection timeout, and session security

i) **Maintaining data availability**, including data backup and recovery

j) **Protecting data during transmission**, including encrypting data during transmission, and confirmation of data delivery

k) **Protecting data in storage**, including protecting data in data repositories, and protecting data on portable media

l) **Data integrity**, including data integrity checking, data integrity during data import, and output data validation

m) **Record retention**

n) **Data Labelling**

o) **Auditing**, including audit logs and trigger events, interface, content, investigative tools, protection, retention, management, continuous audit logging, and reconstructing the content of an electronic health record at a prior point in time

p) **Software version control and documentation**, including software version control, and documentation requirements

q) **Time synchronization and time/date formatting**, including time format, and time synchronization

r) **Privacy and security incident management**

s) **Digital certificates and digital signatures**, including use of digital certificates, digital signatures, providing digital signatures to users, signature format, digital signing, time stamps, validating digital signatures, role of signatory, exporting digitally signed documents and records, digital signature policy, and digital signing of digitized (scanned) documents.

In the table that follows, requirements from Canada Health Infoway refer to a centralized jurisdictional repository of health records (e.g. the central repository of electronic health records for residents of Manitoba). Requirements from the UK Information Governance refer to the Spine and to Patient Data Service (PDS) – these likewise refer to a centralized jurisdictional repository of records (e.g. the central repository of electronic health records for residents of England). Requirements from Brazil refer to the Health Software Certification process managed by the Brazilian Health Informatics Society, and supported by the Chamber of Doctors.

B.2 Patient consent to collect, use or disclose personal health information

B.2.1 Recording consent

Brazil:

NGS1.04.09 Patient-added EHR access restrictions:

Enable the patient to add access restrictions to part or all of his or her EHR.

HL7 ERH-S FM IN1.4

Canada:

Canada Health Infoway Privacy Requirement 9: Recording Consent in POS Systems

POS systems connected to the EHRi where required by law, must be able to record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent.

Rationale: Healthcare organizations must know that they have obtained the consents required in their particular jurisdiction for the purposes for which they will collect, use or disclose PHI (see Privacy Requirement 5).

The form of the consent sought by organizations connecting to the EHRi may vary, depending upon the jurisdiction, circumstances under which the information was collected (e.g. medical emergencies) and the type of information (e.g. mandatory reporting of communicable diseases). In the Canadian EHR environment, the required forms of consent are largely established by various laws, most notably health data protection legislation and public sector privacy legislation. Those entering PHI into a POS system within a particular jurisdiction have the primary obligation of obtaining and recording the consent directives of patients/persons. The POS system has to ensure that those accessing this PHI only obtain access to information that is legitimately available on the basis of consent or legal authorization to use or disclose (e.g. auditing or law enforcement).

Canada Health Infoway Privacy Requirement 11: Recording Consent in the EHRi

The EHRi where required by law, must be able to record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent and must be able to do so in a way that allows each jurisdiction to comply with its own legal requirements on consent.

Rationale: Healthcare organizations must be able to determine if a patient/person has provided or withheld consent as required in their particular jurisdiction.

Consequently, those organizations wishing to disclose PHI to another jurisdiction must do so in a manner that respects the legal requirements for consent in their own jurisdiction (i.e. the jurisdiction of the disclosing organization). As a practical matter, a healthcare organization wishing to access PHI from *another* jurisdiction must do so in a manner that respects the legal requirements for consent to disclose PHI in the jurisdiction of the organization that holds the data as well as satisfy all the

legal requirements for consent to access PHI in its own jurisdiction. (Otherwise the sender cannot honour the access request). This has profound implications for the interoperability of the EHRi. Information contained within a patient/person's EHR may carry with it the legal requirements for consent from multiple jurisdictions (see Privacy Requirement 12). Before permitting accesses to PHI, the EHRi must ensure that all necessary legal requirements are upheld before transmitting data to a requestor.

UK

UK IG Requirement 3.2.2

The system shall provide a facility to capture information about a patient's consent status and decisions and update PDS accordingly.

UK IG Requirement 3.2.3

The system shall enable Users to record free text notes about a patient's decision or lack of decision regarding information-sharing over the Spine, and about the decision-making process. For the avoidance of doubt, this information will be stored locally and not stored on the Spine.

UK IG Requirement 3.16.4: Access from social care

The system must provide the ability to capture free-text notes associated with the decision-making process. The system must make it possible to provide additional details of the consent mechanism and its effect to the user as part of the interaction with the client. For example, this may be achieved by the system providing a function to display explanatory text that has previously been configured by the organization.

Russian Federation

Russian Federation Bill 2011-11-21 N323 Req 13 Physician's secrecy:

The patient's consent is not needed:

if personal health data are processed for national health insurance control and management purposes;

if personal health data are exchanged between medical organizations for diagnosis or health care;

if personal health data are used for control of health care quality and security.

B.2.2 Types of consent

UK

UK IG Requirement 3.2.4

Information captured about a patient's consent status shall include whether the patient "expressed consent", "dissent" or whether "implied consent" was assumed and the date on which this decision was made.

UK IG Requirement 3.16.2: Access from social care

The system must provide functionality to capture and record the status of an individual's preference for access to their NHS-held records from social care settings, where such access may be otherwise permitted given appropriately registered, authenticated and authorized users. The system must distinguish between "no-preference expressed", "express consent" and "express dissent". The default value for this status, prior to any information being gathered from the individual, must be "no-preference expressed". "No preference expressed" means that the question has not been asked of the client (and hence the system may prompt at appropriate points. "Express consent" allows the system to access NHS services (described below in 3.16.7). "Express dissent" records the fact that the client has been asked and has expressed their preference, and that therefore it is not appropriate

to prompt again within the same period of care (although it may be appropriate to ask again at a subsequent significant assessment). A client may choose to update their consent status at any point during a period of care.

UK IG Requirement 3.16.3: Access from social care

It must be possible for the system to support the change of an individual's consent status from "no-preference expressed" to either of "explicit consent" or "explicit dissent". If the status is "explicit consent" it can be changed only to "explicit dissent", and if the status is "explicit dissent" it can be changed only to "explicit consent".

UK IG Requirement 3.16.5: Access from social care

The system must record the identity of the user of the system recording such decisions, with the time, date and location. The system should record the identity of the end-user workstation or device used.

UK IG Requirement 3.16.6: Access from social care

The system must maintain, and provide a view of, the history of such decisions made by the individual, with any associated notes. This history must only be accessible to users with specifically granted additional rights.

UK IG Requirement 3.16.7: Access from social care

Prior to any access to PDS (or any other Spine services other than to support authentication or RBAC) the system must verify that the client's current preference setting is "explicit consent". In the absence of this setting, no such access can take place.

UK IG Requirement 3.16.8 Access from social care:

The explicit consent described in this clause must be subject to at least one of the three following forms of control:

a) Explicit consent as described in this clause applies only for the specific period of care. The system must ensure that this recorded consent is only seen within the context of that period of care (however longstanding that may be). This might be supported either by associating that consent to an explicit episodic case managed within the local care system, or (if the consent is held against the general client record) by resetting the consent flag to "no preference expressed" once the period of care has concluded.

b) Any explicit consent as described in this clause can only be seen to be applicable to the client across any and all periods of care in the future (unless explicitly withdrawn by the client at any point) if explicitly agreed with the client as part of the original interaction to gain their consent.

c) The recorded explicit consent status as described in this clause must only apply until any subsequent social care assessment (e.g. SAP contact or overview assessment, where health and social care needs are assessed jointly), at which point the consent status must be revalidated with the client.

In the absence of a client's explicit expression of consent along these lines, the system shall support a mechanism for the client to provide permission to allow access only for the duration of the login session for the current user.

B.2.3 Communicating consent

Canada

Canada Health Infoway Privacy Requirement 10: Associating Consent with PHI in POS Systems

Where POS systems connected to the EHRi record a patient/person's consent directives, including the withholding, withdrawal or revocation of consent, such POS systems must transmit these

consent directives to the EHRi, in a consistent form, whenever they transmit the associated PHI to the EHRi.

Rationale: Not all jurisdictions will require POS system to collect consent directives. Where these directives are collected, it is essential that they be transmitted to the EHRi whenever the associated PHI is to be transmitted. This will ensure proper EHRi processing of these consent directives prior to transmission of PHI to another jurisdiction. Note that this shifts the burden of ensuring compliance with the regulations of other jurisdictions from the POS system to the EHRi – a reasonable approach given the large number of jurisdictions and the varied complexities vis-à-vis consent among them.

The standards and formats of such consent data are beyond the scope of this Technical Specification, but will be discussed further in the future "Privacy and Security Standards Assessment" and the "Privacy and Security Services" deliverables (see 2.2 "Context for privacy and security requirements analysis").

Canada Health Infoway Privacy Requirement 12: Associating Consent Directives with PHI in the EHRi

When consent is required by law, whenever receiving, storing, processing, or transmitting PHI, the EHRi must be able to:

a) maintain the association between this data and the consent directives under which it may be used or disclosed;

b) process these consent directives before transmitting the associated data and block the transmission where it would violate the directives and where no exception for such a disclosure is outlined in law; and

c) notify the requestor whenever data are blocked as in b) above.

Rationale: This will allow organizations connecting to the EHRi, or hosting components of the EHRi, to *apply* a patient/person's consent directives in their jurisdiction as well as across jurisdictions. EHRi and systems connecting to the EHRi will also need a consistent representation of consent and masking/lockbox directives in support of interoperability requirements within and ultimately between jurisdictions.

UK

UK IG Requirement 3.2.5:

The system shall ensure that a User who seeks to access Sensitive Personal Data that is available through the NHS CRS, will first be informed of the consent status to NHS CRS information sharing for the patient, the last consent decision date and about the patient's consent decision. PDS shall be queried for this information rather than any local cached information.

UK IG Requirement 3.16.10: Access from social care

Prior to attempting to contribute to a client's Summary Care Record (by sending information to PSIS), systems shall verify (by using the spine Access Control Service interface) that clients have not dissented to having a Summary Care Record.

UK IG Requirement 3.16.11: Access from social care

Prior to sending any information from social care settings to NHS information services (for example CAF messages being sent to PSIS) the system shall provide for the explicit consent of the client to be gained. It is expected that the sealing mechanism (see 3.5 and references) will be used to manage this consent: assessments that are sealed and locked cannot be sent to PSIS, while assessments that are sealed can be sent but will not be ordinarily viewable by others.

B.2.4 Consent override in emergencies

USA

CCHIT IFR.02

Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.

UK

UK IG Requirement 3.2.6

The system shall ensure that a User who seeks to access Sensitive Personal Data that is available through the NHS CRS, relating to a patient who has "expressed dissent", will first be warned of the consequences before such data are output. The system shall ensure that Users register a confirmation that this is understood before the data are output. The guidance provided in NPFIT-FNT-TO-IG-DES-0114 Dissent Over-ride Dialogue Design must be followed in such circumstances

B.2.5 Logging consent override

Canada

Canada Health Infoway Privacy Requirement 13: Logging the Application of Consent Directives

The EHRi must be able to:

a) log when the processing of consent directives (cf. Privacy Requirement 12, item b) prohibits the transmission of data;

b) log the identity of any user who overrides a patient/person's consent directives, the reason for the consent override, and the date and time when the consent override occurred. and

c) alert the individual accountable for facilitating privacy compliance in the organization where the accessing user works as well as in the organization where the information was collected that such a consent override has occurred.

Rationale: Since some health data protection laws, like Ontario's *Personal Health Information Protection Act*, allow both masking, unmasking, and notice of existing masking to third parties, the EHRi and POS systems connected to the EHRi will need to track by means of an audit log the identify of anyone who unmasks or unlocks a record (see Security Requirement 38 and Security Requirement 43).

Furthermore, some health data protection legislation requires that health information custodians notify a patient/person if his or her information is stolen, lost, or accessed by unauthorized persons.38 The individual(s) responsible for facilitating an organization's privacy compliance will be greatly assisted in determining when a potential "unauthorized" access or disclosure of PHI has taken place if they are notified when an individual's consent directives are overridden. Overriding of a patient/person's consent directives must be monitored in both the organization where the PHI has been collected and the organization from which the information is being accessed.39

As logs will themselves contain confidential information, they must be made both secure and tamper-proof. Their security requirements are discussed in Security Requirement 50 (Securing Access to EHRi Audit Logs) and Security Requirement 51 (Making EHRi Audit Logs Tamper-Proof).

In addition to logging overrides of a patient/person's consent directives (Item b in the list above) and alerting accountable individuals that a consent override has occurred (item c in the list above), there is also a related requirement to notify patients/persons when access has been deemed inappropriate (see Privacy Requirement 20).

UK

UK IG Requirement 3.2.7

The system shall ensure that in the event of data being output in the circumstances as defined in requirement 3.2.6, that an event is recorded in an Audit Trail with the following data:

— the identity of the User (including role-profile identification);

— the identity of the patient;

— the date and time of the access; and

— the reason(s) for the access.

B.2.6 Data Masking

UK

UK IG Requirement 3.5.1: Sealed Envelopes

> Facilities are being developed to enable patients to exercise their choice on the visibility of information about them. As described in the Care Record Guarantee, in future, patients will be able to request that parts of their record are kept from general view, and that in specific circumstances a clinician will be able to withhold certain types of information from a patient.
>
> Sealing is supported in the Summary Care Record (SCR) from the Spine 2008-A release, and systems interacting with the Summary Care Record are now required to support sealing (at least in terms of their interactions with the SCR).
>
> Further details and guidance for suppliers are available in NPFIT-FNT-TO-REQDEL-0142 Sealed Envelopes Supplier Requirements and the accompanying spreadsheet which describes the applicability of these requirements in different contexts.

UK IG Requirement 3.16.12

> Access from social care

When accessing data from PSIS, social care systems shall filter the data available and only make it possible for users to access social-care data.

B.2.7 Consent given by a substitute decision maker

Canada

Canada Health Infoway Privacy Requirement 15: Recording Identity of Substitute Decision Makers

> Where required to do so by law, the EHRi and POS systems connected to the EHRi must have the ability to indicate when consent is given on behalf of a patient/person by a substitute decision maker (e.g. consent given by an authorized representative), as well as identify this substitute decision maker and the substitute decision maker's relation to the patient/person.
>
> Rationale: Consent can be given not only by a patient/person but also be given by an authorized representative (such as a legal guardian, a substitute decision maker, or a person having power of attorney). Establishing capacity to consent and providing for substitute decision-making are two of the most complex aspects of data protection. Provincial and territorial laws govern these activities.
>
> The determination of an individual's substitute decision maker is typically a ranking process whereby if no individual fitting the first role/relationship in the list (e.g. spouse or guardian) can be found, then the custodian must attempt to locate the next potential substitute decision maker in the ranking process (e.g. sibling).

When a suitable substitute decision make has been found, the custodian must document the relation of that substitute decision maker to the patient/person to ensure that the custodian's selection can later be audited, justified, or reappraised.

B.2.8 Notifying patients of changes to consent

UK

UK IG Requirement 3.16.9: Access from social care

The system must provide facilities to enable the organization operating the system to notify clients of changes to their consent status, and/or when it is recorded or withdrawn, in order to verify that such changes have been properly made in response to a client's wishes. This may take the form of a report being made available to system administrators, or local notifications to nominated administrators.

B.3 Limiting use and disclosure

Canada

Canada Health Infoway Privacy Requirement 18: Limiting Use and Disclosure of Personal Health Information to Identified Purposes

> Organizations connecting to the EHRi and organizations hosting components of the EHRi must only use or disclose PHI for purposes consistent with those for which it was collected, except with the consent of the patient/person or as permitted or required by law.
>
> Rationale: The Alberta *Health Information Protection Act,* Manitoba *Personal Health*
>
> *Information Protection Act* and Ontario *Personal Health Information Act* all require that custodians of PHI only collect, use or disclose as much PHI as is reasonably necessary to carry out the identified purposes. For more information, see "duty to collect, use or disclose in a limited manner" in Appendix B below.
>
> Also, this requirement is a standard and traditional fair information practice and, in places where health data protection legislation has been introduced, does not impede upon custodians' ability to provide care. Theses statutes typically permit or require a number of uses and disclosures of PHI related to provision of healthcare, supporting the operation of the healthcare system, or ensuring public health; such legislative provisions vary by jurisdiction.

UK

UK IG Requirement 3.4.1: Legitimate Relationships (LR)

> The systems and services introduced through the National Programme for Information Technology (NPfIT) being delivered by NHS Connecting for Health will process personal data about patients securely, respecting patient confidentiality. Amongst the controls is the requirement that only those users with a "legitimate relationship" (LR) with a patient will be able to access personal data about that patient.
>
> Only Users engaged in the patient's care and support have the implied consent of the patient to access the patient's data. Without such consent, the data cannot normally be accessed.
>
> Systems must ensure that access to specific patient records is controlled appropriately. For example, in the case of GP systems, any records of patients no longer registered at the practice must not be normally accessible to system users.

UK IG Requirement 3.11.7

> The Supplier shall demonstrate that it has limited the patient identifiable data transferred to portable media to the minimum required for the relevant service.

B.4 Patient access to personal information and correction of inaccurate information

Brazil

NGS1.04.08: Patient access to the RES

Ensure that the patient can have access to all his or her personal and clinical information stored in the EHR. If the EHR does not allow direct access to the EHR by the patient, there shall be a user role that allows this action in behalf of the patient.

The patient shall be able to take with him or her the information in printed or electronic format. The system shall have an interface for printing a user statement that he or she is receiving the information.

Either when the patient has direct access to the information or when another individual has direct access for the patient's information, any data exports and printing of the patient statement shall be recorded, containing at least the following information:

— User who performed this action;

— Full name of the patient;

— Location and time of the operation.

HL7 ERH-S FM IN1.4

Canada

Canada Health Infoway Privacy Requirement 25: Amending Inaccurate or Incomplete Information

Organizations connecting to the EHRi and organizations hosting components of the EHRi should:

a) amend PHI when a patient/person successfully demonstrates the inaccuracy or incompleteness of this information;

b) notify EHRi users that have accessed the information in question that the information has been amended when the amended information can reasonably be expected to have effect on the ongoing treatment of the patient/person;

c) record the substance of the unresolved challenge when the organization disagrees with the patient/person's assessment of incompleteness or inaccuracy; and

d) transmit the existence of the unresolved challenge to EHRi users accessing the information in question.

Rationale: Decisions made by Information and Privacy Commissioners (or their equivalents across Canada) have resulted in jurisprudence that emphasizes that only factual errors can be literally corrected, such as a birth date. Matters of opinion are exactly that, including a diagnosis by a healthcare professional that a patient/person wishes to contest. The issue of correction, deletion, 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.62 Depending upon the nature of the information challenged, amendment may involve the correction, deletion, or addition of information. Some corrections, deletions, or amendments will have a particular relevance to the ongoing healthcare of a patient/person, and they should be made known appropriately. Fortunately, a developed electronic health record system will automatically distribute the most up to date information when it is required for authorized purposes.

UK

UK IG Requirement 3.18.1

The Supplier shall ensure that the system maintaining Personal Data to be capable of responding to subject access requests, in accordance with the Data Protection Act 1998.

UK IG Requirement 3.18.2

The Supplier shall ensure that the system enables the patient's electronic records to be screened by Authorized Users for data that could be detrimental to a patient if viewed and/or third party information before responding to a subject access request.

UK IG Requirement 3.18.3

The Supplier shall ensure that the system enables a User to record a subject access request.

UK IG Requirement 3.18.4

The supplier shall ensure that the system provides that the data that can be recorded about a subject access request includes, as a minimum, the date the request was received, the identity of the subject, the identity of the person making the subject access request, the identity of the User and organization responsible for responding to the request, the identity of the healthcare professional consulted before the Personal Data were released, whether the request was refused, a free text reason for a refusal, a classified reason for a refusal and the date of the response to the request and such other information as the Authority shall reasonably specify.

UK IG Requirement 3.18.5

Where a subject access request is refused, the Contractor shall ensure that the Service requires that at least one reason for refusal be selected from a pre-defined list, which will be the subject of a national standard (as issued by the Authority from time to time).

UK IG Requirement 3.18.6

The system shall enforce Legitimate Relationships (LR) [see above Requirement 3.4.1] or equivalent access controls to control access to functionality described in this clause.

UK IG Requirement 3.18.7

The system shall provide functionality for monitoring SAR requests in progress and for reporting on targets for fulfilment.

Russian Federation

Russian Federation RF 2011-11-21 N323 Req 22 Health information:

The patient has rights to access his/her health data stored in a medical organization including observation data, diagnoses, etc. All this data shall be rendered in understandable form. This data shall be rendered to the patient by his/her attending physician or by the other health provider that has personally participated in treatment of this patient.

Health information cannot be rendered to the patient against his/her will. The patient or his/her legal representative has the right to read personally medical documents related to the patient's health data and to look for a second opinion based on this data.

The patient or his/her legal representative has the right to issue a written request to receive medical documents related to the patient's health data, copies of these documents and document extracts.

B.5 Data accuracy

Canada

Canada Health Infoway Privacy Requirement 22: Accuracy

The EHRi, POS systems connected to the EHRi, organizations connecting to the EHRi and organizations hosting components of the EHRi must take reasonable steps or make a reasonable effort to:

a) ensure that PHI is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used, including disclosures of PHI to third parties; and

b) accurately identify a patient/person when accessing or modifying his or her PHI

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 easier to update even the most basic demographic and location information on any patient/person.

In addition, it is of critical importance for patient safety and a number of other reasons, including the overall success of the EHRS, that EHRi users accurately identify patients/persons prior to accessing or modifying their PHI.

B.6 User identification and authentication

B.6.1 User identification

Brazil

NGS1.02.01: Identifying [and authenticating] users

All users must be identified [and authenticated] before any access is given to EHR data, including when not connected to a network; e.g. mobile devices.

HL7 ERH-S FM IN1.1; ABNT NBR ISO/IEC 27001:2005, A.11.5.2

USA

CCHIT IFR.01

Assign a unique name and/or number for identifying and tracking user identity…

Canada

Canada Health Infoway Security Requirement 55: Assigning Identifiers to Users

All organizations connecting to the EHRi must ensure that users of POS systems that connect to the EHRi are assigned an identifier (user ID) that, in combination with other identifiers (e.g. facility identifiers, jurisdictional identifiers, etc.) can uniquely identify the user within the EHRi. POS systems must support the unique identification of users.

Rationale: This requirement facilitates system-wide audit and trusted end-to-end security

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

All users shall be identified.

B.6.2 User IDs

USA

CCHIT SC 03.08: Authentication

The system shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).

ISO/IEC 15408, *CC SFR: FMT_MTD;*

HIPAA: 164.312(a)(2)(i)

B.6.3 User authentication

Brazil

NGS1.02.01: [Identifying and] authenticating users

All users must be [identified and] authenticated before any access is given to EHR data, including when not connected to a network e.g. mobile devices.

HL7 ERH-S FM IN1.1; ABNT NBR ISO/IEC 27001:2005, A.11.5.2

USA

CCHIT SC 03.01

The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.

Canadian: Alberta 1.1;

ISO/IEC 15408, CC SFR: *FIA_UAU, FIA_UID;*

NIST SP 800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION;

HIPAA: 164.312(d)

CCHIT IFR.09

Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B, row 5.

Table 2B row 5. Cross-Enterprise Authentication: Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g. IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).

Canada

Canada Health Infoway Security Requirement 71: Robustly Authenticating Users

The EHRi and all POS systems connected to the EHRi must robustly authenticate users.

Rationale: Uncontrolled user access is a frequent enabler of security breaches.

Moreover, some level of uniformity in the strength of authentication will likely be needed to support cross-jurisdictional interoperability.

It is important to note that this requirement would likely necessitate the implementation of robust authentication technologies:

a) digital certificates;

b) biometrics;

c) smart cards or other hardware tokens; or

d) standards-based secure and robust password schemes.

It is expected that the EHRi and POS systems connected to the EHRi will work together to accomplish the task of authenticating users who access the EHRi; i.e. users do not need to be authenticated twice.

UK

UK IG Requirement 3.1.2

The system shall ensure that all Users who have access to Personal Data or Sensitive Personal Data obtained from, held in or to be held in NHS CRS about patients are securely authenticated by means of the standardized Smartcard technology and credentials provided by the NASP.

Russian Federation

Russian Ministry of Healthcare recommend. 2009-12-23 req. 6.2 (optional)

All users shall be authenticated before any access to:

— operating system

— security tools

— audit Logs

B.6.4 System authentication and network node authentication

Brazil

NGS1.06.02: Access control from client to server

In a remote-access S-RES, system access should be restricted only to clients with prior permission. This access control can take place, for instance, through the client's IP address.

ABNT NBR ISO/IEC 27001:2005, A.11.4.2

NGS1.06.05: Access control between components

In an EHR consisting of several distributed components (i.e. located in different computers), in the communication between those components (e.g. a database) access to the component shall be restricted only to partners (components) with prior permission.

ABNT NBR ISO/IEC 27001:2005, A.10.9.2

USA

CCHIT SC 06.12: Technical Services

Verify that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in Table 2B row 5.

Table 2B row 5. Cross-Enterprise Authentication: Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g. IHE Cross Enterprise User Assertion (XUA) with SAML identity assertions).

CCHIT SC 06.05: Technical Services

The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using an open protocol (e.g. TLS, SSL, IPSec, XML Sig, S/MIME).

ISO/IEC 15408, *CC SFR: FPT_RCV; HITSP T17;*

HIPAA: 164.312(d); 164.312(c)(1)

Canada

Canada Health Infoway Security Requirement 65: Authenticating EHRi Network Access

Organizations hosting components of the EHRi must ensure that all EHRi connections to remote servers and applications are authenticated. This includes connections via the Internet.

Rationale: This helps to ensure that applications containing PHI are not compromised by masquerading remote servers and/or applications

UK

UK IG Requirement 3.7.2

The supplier shall ensure that all connections to remote servers and applications are authenticated.

This requirement includes connections via the Internet.

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

Network nodes shall be identified using logical names (addresses, numbers).

B.6.5 Authentication methods

Brazil

NGS1.02.02: Authentication method

Use at least one of the following authentication methods:

— Username and password;

— Digital certificate;

— One-Time Password (OTP); and/or

— Biometrics.

NOTE Any other authentication methods must be approved in advance.

— *HL7 ERH-S EM IN1.1 ABNT NBR* ISO/IEC 27001:2005, A.11.5.1

NGS2.03.02: Non-repudiation of authentications

Condition: EHR that uses digital certificate for authentication.

The authentication made through a digital certificate must generate evidence to ensure the non-repudiation of the authentication. The evidence must be stored in the system's security registers in formats compatible with the CMS standards [RFC 3852] or XMLDSIG [RFC 3275]. All elements necessary for validating the authentication (information about root certificates, certificate chains, signatory certificates, and revocation information) must be aggregated in the EHR.

NGS2.03.03: Types of users for authentication with digital certification

Condition: EHR that uses digital certificate for authentication.

All users that use digital signatures must be authenticated with their ICP-Brasil digital certificates.

NGS2.03.04: ICP-Brasil approval (Brazil Specific)

Condition: EHR that uses digital certificate for authentication.

The EHR components that use digital certification for authentication must be approved by ICP-Brasil.

NGS2.03.01: Checking the purpose of the digital certificate for authentication

Condition: EHR that uses digital certificate for authentication.

Before authenticating, check if the digital certificate to be used has a purpose of use of authentication (client authentication).

UK

UK IG Requirement 3.1.8: (UK case specific requirement on use of smart cards)

The system shall provide a mechanism to link a user's Smartcard to their user record within the system. As a minimum this shall include the SDS UserID but may include other IDs (e.g. role profile IDs) if required. The assignment of a SDS ID shall be through a restricted access system function and shall be done programatically (see pseudo code below). All such assignments shall be recorded in the appropriate system audit trail. Removal or change of such assignments shall similarly only be accessible through a restricted access function and all records of the change shall be recorded in the appropriate system audit trail.

Actors:

— Operator – person using the system who will assign a new Smartcard to a system user

— User – the person whose (new) Smartcard is being linked to their user record in the system

Pre-condition:

— The operator must have access to the secure Smartcard assignment function. They may either be authenticated by SSB or may be authenticated locally (i.e. username and password entry to the local system).

BEGIN

IF operator is authenticated by SSB THEN BEGIN

Prompt Operator to remove their Smartcard

Allow Operator to continue using system (i.e. do not log Operator out because they have removed their Smartcard or because a token listener event message is received because of this Smartcard removal)

END

Prompt for User's Smartcard to be inserted

User authenticates themselves (entry of PIN)

IF authentication successful THEN BEGIN

System retrieves the SAML assertion and programmatically extracts the SDS user ID and any required RoleProfileIDs

If appropriate, the operator should select any required RoleProfileIDs for storage

System stores the SDS User ID and any required RoleProfileIDs

END

IF operator was authenticated by SSB THEN BEGIN

Prompt Operator to insert their Smartcard and reauthenticate

Allow Operator to continue using system

END

UK IG Requirement 3.1.3 (UK case specific requirement on use of smart cards)

The system shall also support log-in independently from the SSB service if the SSB is unavailable, except that:

— user role and other access control attributes are not required to be retrieved from SDS

— the strength of authentication may be weaker than that used for SSB log-in

— the user is not permitted to access NHS CRS systems and data unless reauthenticated as described in requirement 3.1.4; however data held in local systems may be accessed during the use of local authentication when the SSB is unavailable

— where the system supports the concept of 'sensitive personal data' (or equivalent terms) local RBAC controls must include controlled access to such data.

For the avoidance of doubt: log-in that is independent from the SSB service under this requirement is intended only in situations where the SSB is temporarily unavailable.

UK IG Requirement 3.1.4 (UK case specific requirement on use of smart cards)

Where a User has logged-in independently from the SSB service, as described in requirement 3.1.3, the system shall prevent unauthorized access to NHS CRS systems and data (although data held in local systems may be accessed during the use of local authentication when the SSB is unavailable). In such situations, the system may either trigger an NHS CRS log-in and apply NHS CRS access controls when the user attempts access to NHS CRS systems, or provide an NHS CRS login function call from within the system, i.e. the user shall not be required to log-out of the system to authenticate on SSB and log back in again before NHS CRS access is granted. Once the User has successfully completed the NHS CRS log-in the User should remain authenticated to the NHS CRS for the duration of the local session, while conforming to the Spine session timeout, inactivity timeout and Smartcard removal requirements.

The only exception to this requirement is that system-initiated interactions may retrieve PDS data using PDS Retrieval or PDS Simple Trace messages. Systems shall not write any data to PDS without SSB authentication.

UK IG Requirement 3.1.9 (UK case specific requirement on use of smart cards)

Users whose Smartcard is not recorded on the system (see previous requirement) can only use local authentication and will not therefore be allowed access to system functions for which Smartcard access is required.

UK IG Requirement 3.1.10 (UK case specific requirement on use of smart cards)

Periodically the application shall check for the presence of the local ticket to ensure an authenticated smartcard is present, unless the application is performing a valid exception in allowing the smartcard to be removed for receiving another smartcard.

Russian Federation

Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

Username and password.

B.6.6 Protecting user profiles, passwords, and other authentication tokens

Brazil

NGS1.02.03: Protecting authentication parameters

All data or parameters used in the user authentication process must be stored or transported in a secure manner. For example, storing only the hash code of the user's password and ensuring that the storage location has access restrictions. Only unquestionably safe algorithms shall be used, such as SHA-1, SHA-2 or their successors, and/or cryptographic-encryption with Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) or their successors.

NOTE In technologies that employ seeds to generate the code, the seed must be protected against unauthorized access and change.

USA

CCHIT SC 03.11: Authentication

When passwords are used, the system shall support the ability to protect passwords when transported or stored through the use of cryptographic-hashing with SHA1, SHA 256 or their successors and/or cryptographic-encryption with Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) or their successors.

Canadian: Ontario 5.3.12.a (System Access Management);

ISO/IEC 15408, *CC SFR: FCS_CKM;*

NIST SP 800-53: SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT;

HIPAA: 164.312(e)(1); 164.308(a)(5)(ii)(D)

FIPS PUB 197

FIPS PUB 140-2

CCHIT SC 06.02: Technical Services

When passwords are used, the system shall not display passwords while being entered.

ISO/IEC 15408, *CC SFR: FPT_ITC;*

ISO/IEC 27002:2005, 9.2.3*;*

HIPAA 164.312(a) (1)

UK

UK IG Requirement 3.3.8

The system shall ensure that, when stored locally, user profile information which supports RBAC mechanisms is protected from unauthorized access (including view, modify, or delete).

B.6.7 Passwords

Brazil

NGS1.02.04: Password quality

Condition: Use of authentication based on username/password.

Use the following security controls:

Password quality: Check password quality at the time the user defines it. Passwords shall have at least eight characters, of which at least one must be non-alphabetic.

Frequency of password changes: The EHR shall include a functionality that forces users to change their password according to an adjustable maximum time period.

ABNT NBR ISO/IEC 27001:2005, A.11.5.3

USA

CCHIT SC 03.02: Authentication

When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.

Canadian: Alberta 7.3.12 (Security)

Canadian Ontario 5.3.12.b (System Access Management);

ISO/IEC 15408, *CC SFR: FIA_SOS, FIA_UAU, FIA_UID;*

ASTM: E1987-98;

NIST SP 800-53: IA-2 USER IDENTIFICATION AND AUTHENTICATION (no strength of password);

ISO/IEC 27002:2005, 9.3.1.*d;*

HIPAA: 164.

CCHIT SC 03.05: Authentication

When passwords are used, the system shall provide an administrative function that resets passwords.

ISO/IEC 15408, *CC SFR: FMT_MTD;*

ISO/IEC 27002:2005, 9.2.3.*b, (9.3.1.f);*

HIPAA: 164.312(d); 164.308(5) (ii) (D)

CCHIT SC 03.06

When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.

ISO/IEC 15408, *CC SFR: FMT_MTD;*

ISO/IEC 27002:2005, 9.2.3.*b, (9.3.1.f);*

HIPAA: 164.312(d); 164.308(5) (ii) (D)

CCHIT SC 03.09: Authentication

When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules (SC 03.02).

ISO/IEC 15408, *CC SFR: FMT_MTD;*

HIPAA: 164.308(a) (5) (ii) (D)

CCHIT SC 03.10: Authentication

When passwords are used, the system shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).

Canadian: Ontario 5.3.12 (b);

NIST SP 800-63;

HIPAA: 164.308(a) (5) (ii) (D)

UK

UK IG Requirement 3.15.2 (UK case specific requirement)

Any local authentication should be based on a user identity which is then authenticated at least through the use of a separate password.

UK IG Requirement 3.15.3 (UK case specific requirement)

Passwords should be managed following the recommendations in the CESG Infosec Memorandum No. 26, available by email request to esp.ig@nhs.net

UK IG Requirement 3.15.5

Systems must ensure that passwords can be enforced to a policy as defined in Reference: NPFIT-FNT-TO-IG-IGCOM-0066 Single Factor authentication password Policy

Russian Federation

Russian Ministry of Healthcare recommend. 2009-12-23 req. 6.2 (optional):

Password quality: alphanumeric password 6 chars or more.

B.6.8 Failed Login Attempts

USA

SC 03.04: Authentication

The system shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).

Canadian: Ontario 5.3.12.c (System Access Management);

ISO/IEC 15408, *CC SFR: FIA_AFL, FMT_SAE*;

NIST SP 800-53: AC-6 UNSUCCESSFUL LOGIN ATTEMPTS, AC-11 SESSION LOCK;

ISO/IEC 27002:2005, 9.3.1.*e, 9.5.2.e;*

HIPAA: 164.312(a)(1); 164.308(a)(5)(ii)C; 164.308(a)(6)

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

The system shall enforce a limit of consecutive invalid access attempts to the security subsystem by a user.

B.6.9 User feedback during authentication

USA

CCHIT SC 03.07: Authentication

The system shall provide only limited feedback information to the user during the authentication.

ISO/IEC 15408, *CC SFR: FIA_UAU;*

NIST SP 800-53: IA-6 AUTHENTICATOR FEEDBACK;

HIPAA: 164.312(d); 164.308(5) (ii) (D)

B.7 Privilege management

B.7.1 Access privileges

Brazil

NGS1.04.03: Managing users

Enable user management (create, remove, and change), role management (create, remove, and change), and group management (create, remove, and change).

NGS1.04.04: IT related roles

Support functionalities that allow at least the following activities:

Audits of the system activity logs;

System setup;

Permission management;

User management;

Produce and restore safety copy.

NGS1.04.05: Access control setup

Provide the necessary mechanisms to implement an access-control policy using access-profile setup, considering the role of the user, the groups, and the operations that can be performed, including the differences between queries and inclusions/changes. Consider that a single user can have more than one role.

HL7 ERH-S FM IN1.2;

ABNT NBR

ISO/IEC 27001:2005, A.11.6

ISO 18308:2011*(E) PRS3.3*

CCHIT SC 01.02: Access Control

The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups

Canadian: Alberta 4.1.3 (EMR);

ISO/IEC 15408, *CC SFR: FMT_MSA;*

NIST SP 800-53: AC-56 LEAST PRIVILEGE; AC-5 SEPARATION F DUTIES

HIPAA: 164.312(a)(1); 164.308(A)(3)(1); HITSP/TP20

CCHIT SC 01.03: Access Control

The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)

Canadian: Ontario 5.3.12.e (System Access Management);

ISO/IEC 15408, *CC SFR: FDP_ACC, FMT_MSA;*

ASTM: E1985-98;

NIST SP 800-53: AC-3 ACCESS AND INFORMATION FLOW CONTROL; SC-3 SECURITY FUNCTION ISOLATION

HIPAA: 164.312(a)(1); 164.308(A)(3)(1);

HITSP/TP20

Canada

Canada Health Infoway Security Requirement 58: Granting Access to Users by Role

The EHRi and all POS systems connected to the EHRi must 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.

Rationale: As a practical matter, users of POS systems connected to the EHRi (and there will be many 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 must be mapped to roles, and then the roles mapped to system functions.

There are significant issues related to using RBAC to support an interoperable EHR that must be resolved before the EHRi can make full and effective use of RBAC. These issues are summarized in Appendix A-1 Privacy and Security Implications Connected With Actors.

Canada Health Infoway Security Requirement 60: Granting Access to Users in Work Groups

The EHRi and all POS systems connected to the EHRi must be capable of assigning users to working groups and of granting access to records based on working groups.

Rationale: It is unreasonable to assume that all physicians will be able, via the EHRi, to view the EHR of all Canadian patients/persons. At a minimum, VIPs and other selected patients will require restriction of their EHRs to just those individuals who are known members of their healthcare team. This is a privacy protective feature that all Canadians might reasonably expect to protect their PHI from potential access by any arbitrary healthcare provider registered to use the EHRi. This in turn requires some mechanism for obtaining information on a patient/person's relationships with his or her healthcare providers. Such information could be extracted from the patient/person's EHR. In addition, 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 patient/person to be inferred from existing relationships between the patient/person and other members of the workgroup.

It is important to note that the EHRi cannot reasonably be the authoritative source of information for all workgroup assignments, as they are too fluid and change too quickly to manage centrally. It is expected that POS systems will track such assignments where necessary (e.g. in a hospital information system) and that the EHRi will rely on this data where available. It *is* expected that the EHRi will be capable of deducing whether a bona fide relationship exists between a patient/person and a healthcare provider where such a relationship can be inferred from the existing PHI (e.g. where a healthcare provider has already provided care to the patient/person, contributed data to the patient/person's EHR, ordered tests, prescribed medications).

Canada Health Infoway Security Requirement 63: Granting Access By Association

The EHRi and all POS systems connected to the EHRi:

a) must be capable of associating users (healthcare providers) with the records of patients/persons and allowing future access based on this association; i.e. they must be capable of granting discretionary access to records based on a registered user with legitimate and pre-existing access to a patient's record(s) granting access rights for that (those) record(s) to another registered user;

b) must not allow users to grant other users access to a record if the granting users themselves do not possess such access with respect to the record; and

Note that granting other user's access to a record does not over-ride the role based access control restrictions of those other users.

Rationale: This requirement is essential if Security Requirement 60 is to be made effectively operational. As noted above, discretionary access control does not "trump" role based access control. For example, 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.

UK

UK IG Requirement 3.3.2

The system shall implement role-based access control to authorize users' access to the system's functions and data.

UK IG Requirement 3.3.3 (UK case specific requirement)

A System which integrates with the NHS CRS RBAC framework shall obtain information about a user's allocated Role Profiles by using the SAML interfaces provided by the Spine for this purpose, as defined in the Spine External Interface Specification (EIS).

UK IG Requirement 3.3.6

A system which integrates with the NHS CRS RBAC framework shall implement the nationally-defined mapping from Job Role/Work Area to Baseline Activities as published by the authority.

The system shall implement a process for incorporating updates to the nationally defined mapping from Job Role/Work Area to Baseline Activities as published by the authority from time to time.

UK IG Requirement 3.3.7

Where an Existing Systems Supplier is not required to support SSB authentication, the system shall implement local role-based access controls which support the allocation of access rights in line with the nationally-defined Job Roles/Areas of Work and Activities. Those local RBAC mechanisms must:

— Restrict users' use of the system to specific functions, assigned by the system manager(s) and only by the system manager(s);

— Not allow any user access to their allocated functions until they have entered their user identity and password

Access controls must include the ability to segregate access to the following functions:

— Viewing the audit trail

— Accessing inactive staff details

— Accessing the records of patients that are not normally accessible to system users (for example in the case of GP systems, to the records of patients that are not currently registered at the practice).

UK IG Requirement 3.3.9

a) The system must verify that the organization of the role-profile selected is that of the system the user is attempting to log into and only allow users to log in if either:

— The organization within the selected role-profile matches the organization code within the system, or

— In a community pharmacy setting, the role and area-of-work of the selected role-profile matches that for community pharmacist users, and the organization within the selected role-profile is that of the special notional organization (organization code FFFFF) set up to support EPS R2. The system shall only support the use of a role-profile of the FFFFF organization if there is no appropriate organization-specific role-profile associated with the user.

b) Within a role-profile selection screen, the system should display only those role profiles that are applicable to the system the user is attempting to log into. In addition any role-profile with the FFFFF organization will only be visible when there is no organization-specific role-profile for that organization. The system must make it clear to the user which role-profile is being used by the system: it will commonly be the case that there is only a single role-profile that is most appropriate, in which case the user should not have to explicitly select it from a list that includes any other nonappropriate (non-matching organization) or less-appropriate (FFFFF organization) role-profiles.

UK IG Requirement 3.3.10

Suppliers must provide details of the mapping of their local system functions to activities from the National RBAC Database, using the template provided. This is to support the RA process (to ensure that Ras have information to enable them to allocate users the appropriate job roles, areas of work and any additional activities) and also to support the compliance process.

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 5.11

The system shall provide the ability to assign restrictions or privileges to users/groups according to an access matrix.

B.7.2 Reporting access privileges

Canada

Canada Health Infoway Security Requirement 63a: Reporting the Access Privileges of a User

The EHRi must – and POS systems connected to the EHRi should – provide functionality that can report, for a given user:

a) which records the user can access;

b) which portions of the record the user can access;

c) which privileges (viewing, modification, etc.) the user has in respect to each of these records.

Rationale: Past experience with popular operating system software has shown how difficult it can be to determine whether a given user can access a given record or exercise a given privilege unless there is an explicit facility within the system to answer such questions. The lack of such a facility can make it extremely difficult to detect and correct errors in the assignment of user access privileges.

UK

UK IG Requirement 3.1.12

The application shall make it possible for Users to validate the role and organization relevant to the access they are being granted so as not to be able to claim ignorance of that role or organization, or otherwise justify a lack of awareness of the significance of their actions.

B.7.3 Restrictions on access privilege

USA

CCHIT SC 01.01: Access Control

The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor), or processes acting on behalf of users, for the performance of specified tasks.

ISO/IEC 27002:2005, 9.1.1.2.*b;*

HIPAA: 164.312(a) (1); 164.308(a) (3) (1)

HITSP/TP20

NIST SP 800-53: AC-6 LEAST PRIVILEGE;

AC-5 SEPARATION OF DUTIES

Canada

Canada Health Infoway Security Requirement 59: Selecting A Single Role Per Session

All POS systems connected to the EHRi must ensure that each user will access applications and services of the EHRi in a single role (i.e. users who have been registered with more than one non-overlapping role must designate a single role during each EHRi session).

Rationale: Users who wear many disparate hats need to wear them one at a time. For example, a general practitioner who works in the Emergency Department of a rural hospital one day a week (and who has emergency override privileges while on duty) must clearly indicate to the POS system when she is acting in this capacity and must do so prior to accessing a patient/person's EHR via the EHRi.

Another example would be an EHRi user accessing EHRi records as a clinician and also sometimes as a researcher.

A hierarchical organization of roles, accommodating users who frequently switch between dual roles that are both related to clinical care, would greatly reduce user frustration from needlessly having to switch between one role and the other.

See also: ISO/IEC 27001:2005, A.11.2.2

UK

UK IG Requirement 3.3.4

A system which integrates with the NHS CRS RBAC framework shall allow the user to select which of the Role Profiles allocated to the user is to be applied to that user's session with the application. If no selection is made, the system shall apply the Role Profile selected at the initial login to NHS CRS.

UK IG Requirement 3.3.5

A system which integrates with the NHS CRS RBAC framework shall allow the user to select which of the Role Profiles allocated to the user is to be applied to that user's session with the application. If no selection is made, the system shall apply the Role Profile selected at the initial login to NHS CRS.

B.7.4 Delegation of access privileges

Brazil

NGS1.04.07: Delegating power

The delegator is the individual in charge of authorizing delegation of power and the delegatee is that who receives the delegation of power. Accordingly:

— The delegator must have prior permission to grant such permissions;

— The delegation of power must be recorded in the system;

— The delegation of power must inform the following:

— The delegator;

— The delegatee;

— The reason;

— The date and time granted;

— The period of time the permission is granted.

NOTE An example of delegation of power is a physician who delegates the power to enter information about a patient into the EHR to a nurse.

Canada

Canada Health Infoway Security Requirement 63 Granting Access by Association

The EHRi and all POS systems connected to the EHRi:

a) must be capable of associating users (healthcare providers) with the records of patients/persons and allowing future access based on this association; i.e. they must be capable of granting discretionary access to records based on a registered user with legitimate and pre-existing access to a patient's record(s) granting access rights for that (those) record(s) to another registered user; and

b) must not allow users to grant other users access to a record if the granting users themselves do not possess such access with respect to the record.

Note that granting other users access to a record does not over-ride the role based access control restrictions of those other users.

B.7.5 Removing access privileges

USA

CCHIT SC 01.04: Access Control

The system shall support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.

HIPAA: 164.308(a) (4) (ii) (C); 164.308(a) (3) (i) (C);

HITSP/TP20

Canada

Canada Health Infoway Security Requirement 62: Timely Revocation of Access Privileges

The EHRi and all POS systems connected to the EHRi must support the revocation of user access privileges in a timely manner; i.e. to immediately prevent the user from logging on, after access privileges have been revoked.

Rationale: This requirement ensures that user access privileges to the EHRi can be immediately and systematically suspended if there are grounds to do so.

B.8 Acceptable use

B.8.1 Notifications to users

USA

CCHIT SC 06.07: Technical Services

The system, prior to access to any PHI, shall display a configurable warning or login banner (e.g. "The system shall only be accessed by authorized users").

In the event that a system does not support pre-login capabilities, the system shall display the banner immediately following authorization.

CC 2.1 L.4 TOE access banners (FTA_TAB); CC 3.0 FIA_TIN.1 Advisory warning message;

NIST SP 800-53 AC-8 System Use Notification

HIPAA 164.308(a)(5)(i); 164.308(a)(5)(ii)

UK

UK IG Requirement 3.1.11

The application shall prominently display the following message upon application start-up to remind users of their responsibilities and the legal constraints on the use of the system: "Computer Misuse Act 1990 – Unauthorized access to this system is an offence." Note that this wording may be updated from time-to-time.

B.9 Session security

B.9.1 User session timeout

Brazil

NGS1.03.01: Closing an inactive session

The user's session can be terminated after an adjustable inactive period, invalidating the session control parameter, using, for example, a cookie.

ABNT NBR ISO/IEC 27001:2005, A.11.5.5

USA

IFR.03

Terminate an electronic session after a predetermined time of inactivity.

SC 03.03: Authentication

The system upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user re-establishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.

Canadian: Alberta 7.3.14 (Security)

Canadian Ontario 5.6.12.a (Workstation Security);

ISO/IEC 15408, *CC SFR: FTA_SSL, FMT_SAE;*

NIST SP 800-53: AC-7 UNSUCCESSFUL LOGIN ATTEMPTS; AC-11 SESSION LOCK; AC-12 SESSION TERMINATION

HIPAA: 164.312(a) (1); 164.312(a) (2) (iii)

Canada

Canada Health Infoway Security Requirement 72: Restricting Access to Unattended Workstations

All POS systems connected to the EHRi must protect unattended workstations against an unauthorized person taking the opportunity to use the workstation while the POS is active, either with automatic timeout after a period of inactivity or by placing the workstations in a physically secure area.

Rationale: Most systems already implementing this requirement, at least at a rudimentary level (e.g.: automatic timeout after a period of inactivity). Some workstations are positioned in physically secure areas (e.g.: behind the prescriptions dispensing counter in a pharmacy). Proper positioning of workstations also plays a role in ensuring that the patients/persons cannot see the details of other people's records.

UK

UK IG Requirement 3.8.1

The system shall provide controls to protect unattended workstations from being accessed by unauthorized person(s), with automatic timeout after a period of user inactivity; this may be achieved by application of a screen-saver or application locking, requiring a legitimate user to re-authenticate. Automatic timeout will be preceded by a warning that timeout is about to take place (this warning to be a configurable period before timeout, default being 60 s).

UK IG Requirement 3.8.2

The system shall provide a facility for the user to lock the system with a single action, this action hiding any patient-identifiable data from view and ensuring that reauthentication is required for the application to be resumed.

UK IG Requirement 3.8.3

When access is denied due to the requirements in this clause, the same user can return to their session by re-authenticating, or any other user can log off the previous session (without returning to it) in order to be able to proceed with a new session.

UK IG Requirement 3.1.5: (UK specific)

The system shall integrate with Spine Security Broker mechanisms for notification of:

— Session Timeout

— Inactivity Timeout

— Smartcard Removal

— Where notified of one of these events, the system shall ensure that a user is challenged to re-authenticate as described above in requirement 3.1.4 before being allowed to continue using the NHS CRS system.

— The system shall do this by registering a Token Listener (See External Interface Specification and 3.1.6 in this Technical Specification for further information).

— Note that the session and inactivity timeout values are set by the Authority and may be changed from time to time.

UK IG Requirement 3.1.6: (UK case specific requirement)

SSO Token Listener To detect when a User's session ends, as described above in 3.1.5, the system must 'listen' for SSO Token events.

NOTE The User's Spine session is autonomous to the User's Accredited Service session(s).

The Spine Security Broker (SSB) SSOTokenListener interface provides a mechanism for applications that need notification when an SSO token expires. The token will expire if it reaches its maximum session time, or maximum idle time, or if an administrator terminates the session.

The system shall invoke the addSSOTokenListener method using the SSOToken interface; this method implements the SSOTokenListener interface. A call-back object will be invoked when the SSO token expires. Using the SSOTokenEvent (provided through the call-back), the system can determine the time, and the cause of the SSO token expiry.

In the destruction of the Session Token, the SSB invokes the registered call-back. The call-back is a HTTP POST request that transmits XML data to a servlet in the system; the system receives the HTTP Post and uses the information contained therein to take action as appropriate.

More detail is provided in the External Interface Specification.

UK IG Requirement 3.1.7: (UK case specific requirement)

The system shall keep a user session alive while that user is actively using the system. This shall be achieved by using appropriate token refresh functions with the SSO API available as part of the SSB service.

Such refreshes, which reset the inactivity timer on the Spine, can either be triggered every time a user users a function which interacts with the Spine (e.g. PDS retrieval) or by using a local idle timeout timer which causes a refresh before the Spine idle timeout is invoked

B.9.2 Connection timeout

Canada

Canada Health Infoway Security Requirement 70: Restricting Connection Times to EHRi Applications

Where appropriate, the EHRi should restrict connection duration to EHRi application services to provide additional security for access to those applications.

Rationale: This requirement 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). Given the messaging framework defined in the EHRS Blueprint, connections to an EHRi would typically not last more than a few minutes.

B.9.3 Session security

Brazil

NGS1.03.02: Security against user session theft

The communication session shall have security controls to prevent the user's session from being stolen.

NOTE 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.

ABNT NBR ISO/IEC 27001:2005, A.10.8

B.10 Maintaining data availability

B.10.1 Data backup and recovery

Brazil

NGS1.05.01: Backup/Recovery

The EHR shall allow making security copies that meet the following requirements:

Export the security attributes together with the data;

Ensure that when restoring from a security copy and files that the security attributes and their associations are automatically restored without administrator intervention;

Ensure that only users with the role of backup operator can export and restore a security copy, making sure that this user does not have direct access to the information.

ABNT NBR ISO/IEC 27001:2005, A.10.5

NGS1.05.02: Check integrity in data restoration

There shall be a control that ensures that information integrity is checked both when generating and restoring a security copy.

ABNT NBR ISO/IEC 27001:2005, A.10.5

USA

CCHIT SC 05.02: Technical Services

The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).

ISO/IEC 15408, *CC SFR: FPT_RCV;*

HIPAA 164.312(c) (1)

CCHIT SC 08.01: Backup/Recovery

The system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.

Canadian: Alberta 7.3.16 (Security);

ISO/IEC 15408, *CC SFR: FDP_ROL, FPT_RCV;*

HIPAA: 164.310(d)(1)

CCHIT SC 08.02: Backup/Recovery

The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.

Canadian: Alberta 7.3.18.9 (Security);

ISO/IEC 15408, *CC SFR: FAU_GEN;*

NIST SP 800-53: AU-2 AUDITABLE EVENTS;

HIPAA: 164.310(d) (1)

CCHIT SC 08.03: Backup/Recovery

If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.

Canadian: Alberta 7.4.2.5 (Technica+D1l);

ISO/IEC 15408, *CC SFR: FDP_ROL;*

HIPAA: 164.310(d) (1)

Canada

Canada Health Infoway Security Requirement.30: Securely Backing Up Data

All organizations hosting components of the EHRi must

a) back up PHI and security critical system data in a manner that ensures the confidentiality, integrity, and availability of the data; and

b) store the backed-up data in a physically secure environment off-site.

Rationale: Several technologies are available to ensure the confidentiality of data during storage, such as encryption or the use of de-identified data.

Jurisdictions must determine the level of protection required based on risk, technical and operational aspects.

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

The system shall back up personal data to removable storage.

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.2 (optional)

There are to be at least two copies of security subsystem software.

There are to be tools for recovering at least two copies of security subsystem software.

Integrity of security subsystem software shall be checked during each operating system restart.

B.11 Protecting data during transmission

B.11.1 Encrypting data during transmission

Brazil

NGS1.06.01: Communication security between client and server

The communication session between the client component (user side) and the server component must feature the following security services: server authentication, data integrity, and data confidentiality.

NOTE Examples of this are protocols such as HTTPS (HTTP + SSL/TLS), and IPSEC.

ABNT NBR ISO/IEC 27001:2005, A.10.9.2 *and A 10.6*

NGS1.06.03: Restriction of transmitted data

In a remote-access EHR, the data transmitted to the client component (user side) shall be only those presented to the user. This means that any and all processing associated with the selection of data shall be performed by the server side.

ABNT NBR ISO/IEC 27001:2005, A.10.9.2

NGS1.06.04: Communication security between components

In an EHR consisting of several distributed components (i.e. located in different computers), the communication between those components (e.g. a database) shall offer the following security components: partner authentication (client and server), data integrity, and data confidentiality.

ABNT NBR ISO/IEC 27001:2005, A.10.9.2

USA

CCHIT SC 06.01: Technical Services

The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.

Canadian: Alberta 7.4.6.2 and 8.4.6.2 (Technical);

ISO/IEC 15408, *CC SFR: FCS_COP; FIPS 140-2;*

NIST SP 800-53: SC-13 CRYPTOGRAPHIC OPERATIONS;

HIPAA: 164.312(e) (1); 164.312(a) (2) (iv)

HITSP T17,

FIPS PUB 140-2

CCHIT SC 06.03: Technical Services

For systems that provide access to PHI through a web browser interface (i.e. HTML over HTTP) shall include the capability to encrypt the data communicated over the network via SSL (HTML over HTTPS).

NOTE Web browser interfaces are often used beyond the perimeter of the protected enterprise network

ISO/IEC 15408, *CC SFR: AGD_ADM; HITSP/TP17;*

HIPAA: 164.312(e)(1); 164.312(a)(2)(iv)

CCHIT IFR.07

Verify that electronic health information has not been altered in transit and detect the alteration and deletion of electronic health information and audit logs in accordance with the standard specified in Table 2B row 4.

Table 2B row 4: Verification that Electronic Health Information has not been Altered in Transit: A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA- 1 or higher (e.g. Federal Information Processing Standards (FIPS) Publication (PUB) Secure Hash Standard (SHS) FIPS PUB 180-3).

CCHIT SC 06.04: Technical Services

The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 or SHA 256 hashing or their successors and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.

ISO/IEC 15408, *CC SFR: FPT_RCV; FIPS 140-2; SP800-53: SC-13 CRYPTOGRAPHIC OPERATIONS;*

HIPAA: 164.312(e) (1); HITSP T17

Canada

Canada Health Infoway Security Requirement 31: Encrypting PHI During Transmission

The EHRi and POS systems connected to the EHRi must apply industry standard cryptographic algorithms and protocols during transmission of PHI to maintain the confidentiality and integrity of this data whenever it is transmitted outside the physical security perimeter that protects information processing facilities supporting EHRi servers, applications or data.

Rationale: Interception of confidential information is a serious risk and its alteration in transit has severe consequences. Providing for the confidentiality and integrity of PHI transmitted by the EHRi is a minimum requirement.

Health information legislation does not contain specific directions regarding protection of information during transmission, but there are some general requirements. For example, Ontario's health information legislation requires custodians to "transfer" PHI in a secure manner. Manitoba's health information legislation requires a trustee who uses electronic means to request disclosure and to respond to requests for disclosure to implement procedures to prevent the interception of information by unauthorized persons.

Canada Health Infoway Security Requirement 32: Protecting Source and Destination Integrity During Transmission of PHI

The EHRi must protect the source and destination of the message against masquerade during data transmission of PHI to maintain its confidentiality and integrity.

Rationale: This is a minimum requirement to protect against the threat of masquerade. This requirement facilitates trusted end-to-end information flow and would require that a technology such as digital signatures, dedicated lines, or virtual private networks be implemented to protect source and destination.

UK

UK IG Requirement 3.10.3

To protect the confidentiality and integrity of information in transit the system shall employ cryptographic techniques which conform to NHS cryptographic standards (as issued by the Authority from time to time and available by email request to esp.ig@nhs.net). The use of clear text protocols as a remote support tool will be restricted to technical or system software support and not for accessing Personal or Sensitive Personal Data.

UK IG Requirement 3.11.18

Where a service offered by the Supplier requires the transmission of patient identifiable data by electronic means, the data shall be transmitted in an encrypted to the level required by the Approved Cryptographic Standards. This encrypted data can be transmitted via a secure email service such as NHS Mail or over an approved network such as N3.

UK IG Requirement 3.10.2

The system shall protect the confidentiality and integrity of Personal Data and Sensitive Personal Data about a patient in transit across untrusted networks, including (but not limited to):

— between data centres,

— between data centres and deployment site LANs,

— between N3 customers and remote access devices, and

— between data centres and remote access devices.

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.1

The system shall protect all personal data delivered over the Internet or other known open networks via cryptographic techniques. Any trans-border exchanges of personal data shall be protected via cryptographic techniques.

B.11.2 Confirmation of data delivery

Brazil

NGS1.07.08: Proof of delivery

Data exchanges between EHR shall have controls to confirm the delivery/reception of the data.

NOTE An example of this is TISS.

ABNT NBR ISO/IEC 27001:2005, *A 10.6*

Canada

Canada Health Infoway Security Requirement 33: Acknowledging Receipt of Transmitted PHI

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

Rationale: Message acknowledgement via handshaking or other methods is a minimum requirement to ensure complete receipt of information at its destination.

B.12 Protecting data in storage

B.12.1 Protecting data in data repositories

Brazil

NGS1.04.01: Preventing access by unauthorized entities

Forbid access to the EHR-S and DBMS by non-authenticated and unauthorized entities.

HL7 ERH-S FM IN1.2 ABNT NBR ISO/IEC 27001:2005, A.11.6.1

NGS1.04.02: EHR access control mechanism

Ensure that access to the EHR is possible only through an access control mechanism.

HL7 ERH-S FM IN1.2

NGS1.07.05: Using SGBD

The EHR shall be stored and protected by a Database Managing System (SGBD)

NGS1.07.06: Preventing direct access to the SGDB

EHR users shall not have direct access to the SGBD. User access to the EHR shall be allowed only using the EHR' access control and authentication component, never directly to the SGBD, except when making security copies.

NGS1.07.07: Encrypted patient identification data

Any data identifying patients shall be encrypted to prevent rebuilding their EHR through unauthorized access to the EHR database or security copy (produced to safeguard data).

ABNT NBR ISO/IEC 27001:2005*A 10.7.3*

USA

CCHIT IFR.05

Encrypt and decrypt electronic health information according to user-defined preferences (e.g. backups, removable media, at log-on/off) in accordance with the standard specified in Table 2B row 1.

Table 2B row 1 General Encryption and Decryption of Electronic Health Information: A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (e.g. FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).

Canada

Canada Health Infoway Security Requirement 36: Protecting Data Storage

All organizations hosting components of the EHRi must protect electronic media containing PHI or security critical system data, including user registration data, by one or more of the following means:

a) physically protecting the media in accordance with Security Requirement 18;

b) securely de-identifying the PHI it contains; or

c) encrypting the data it contains.

Rationale: Protection of the PHI is essential if use and disclosure of this information is to be controlled. In this sense, this requirement follows from the privacy requirements of 4.5. Encryption of data stores is still uncommon in healthcare and healthcare organizations have been slow to make use of contemporary technology for encrypting databases. Attempts to de-identify data stored in databases are frequently inadequate and sometimes easy to subvert.

Protection of user registration data are essential to maintaining its integrity (and hence the integrity of the user authentication process). Protecting its confidentiality is essential to maintaining the trust of healthcare providers (who, for example, do not want to be sent marketing materials from spammers gaining access to a poorly secured list of contact details for users).

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

UK

UK IG Requirement 3.11.2

The system shall ensure that NHS CRS data, including personal and sensitive personal data about a patient, and audit logs, is protected from unauthorized access and modification when stored within databases and/or files

B.12.2 Protecting data on portable media

[See also ISO/IEC 27001:2005 A.10.8.3]

USA

CCHIT SC 06.06: Technical Services

The system, when storing PHI on any device intended to be portable/removable (e.g. thumb-drives, CD-ROM, PDA, Notebook), shall support use of a standards based encrypted format using triple-DES (3DES), or the Advanced Encryption Standard (AES), or their successors.

FIPS 140-2, ISO/IEC 15408, *CC SFR: FCS_COP, OMB M-06-16, SP800-53: AC-19, HITSP T33;*

HIPAA: 164.312(e) (2) (ii)

FIPS PUB 140-2

Canada

Canada Health Infoway Security Requirement 34: Protecting PHI on Portable Media

All organizations hosting components of the EHRi must – and organizations

connecting to the EHRi should – ensure that PHI and other security critical data stored on removable media are:

a) encrypted while the media are in transit to protect the data's confidentiality and integrity; and

b) protected from theft, where appropriate, while the media are in transit to protect the data's availability.

Rationale: This requirement protects information stored on removable media. Mobile devices are covered in Security Requirement 73 (Acceptable Use of Mobile Devices).

UK

UK IG Requirement 3.11.8

Where devices or services offered by the Supplier result in the transfer of any patient identifiable data on any portable media, encryption shall be used. The level of encryption used shall conform to the Approved Cryptographic Standards as described in 3.10.3.

UK IG Requirement 3.11.9

The encryption, decryption, transport, storage and destruction of data which is transferred shall be auditable with the media logged and tracked to ensure all instances are accounted for.

UK IG Requirement 3.11.11

The Supplier shall ensure that the encryption product used is accredited to FIPS 140-2 and should have received CCTM accreditation (see http://www.cesg.gov.uk/servicecatalogue/CCTM/Pages/CCTM.aspx).

UK IG Requirement 3.11.12

The supplier shall ensure that the encryption key for each archive is of an appropriate strength and complexity as detailed in the Approved Cryptographic Standards.

UK IG Requirement 3.11.13

Where encryption keys are generated by the system automatically for transfer of data by portable media, the system shall provide the encryption key to the Data Controller for each encryption operation. In such circumstances, cryptographic keys must not be generated by the use of an algorithm or other shared secret that solely combines known or accessible environmental or other context-specific information, without the inclusion of unique, context specific secret information as provided by the user or supplier. Context specific, secret information should be controlled and managed in line with key management good practice principles.

UK IG Requirement 3.11.14

The Supplier shall ensure that any encryption keys generated by the system are stored securely to enable data recovery in the event of key loss or corruption by the Data Controller.

UK IG Requirement 3.11.15

The supplier shall ensure that the encryption key for each archive is unique to that data archive.

UK IG Requirement 3.11.16

Where the Supplier system provides a mechanism for sending encryption keys to a recipient, either electronic or manually, there must be processes in place to ensure that the encryption keys are sent following a separate communication mechanism to the encrypted data or posted separately from the encrypted media.

UK IG Requirement 3.11.17

Where a service offered by the Supplier requires the transfer of patient identifiable data by portable media the media shall be encrypted to the level required by the Approved Cryptographic Standards and transported in a secure manner. The transfer of Patient Identifiable Data shall be conducted using Secure Courier services following Department of Health Encryption Guidance guidelines.

See also UK IG Requirement 3.11.7 above.

Russian Federation

Russian Ministry of Healthcare recommendation 2009-12-23 req. 6.1

The system shall protect all personal data delivered over the Internet or other known open networks via cryptographic techniques. Any connection to the Internet or other known open networks shall be protected using firewalls.

Russian Ministry of Healthcare recommend. 2009-12-23 req. 6.2 (optional)

Any portable/removable device used for storing personal data shall be marked and registered in Audit Logs.

B.13 Data integrity

B.13.1 Data integrity checking

Brazil

NGS1.07.04: Checking data integrity

There shall be controls to check the integrity of EHR data in order to prevent user actions or system failures from causing data inconsistencies.

B.13.2 Importing data

Brazil

NGS1.07.01: Importing data

Data imported from another EHR via portable device shall be associated with a patient and a physician in charge, location, date and time of import, and user who imported the data.

HL7 EHR-S FM IN1.6

B.13.3 Data integrity during data import

Brazil

NGS1.07.02: Restricting transmission and exporting of EHR.

EHR shall be transmitted and exported only in the following situations:

— For transmission to another system;

— Backup;

— To the patient, at the request of the patient, in electronic or printed format;

— In processes requiring printing all or part of the EHR;

— To comply with legal requirements that demand printed paper documents.

All EHR transmission and exportation activities shall be recorded.

USA

SC 06.13: Technical Services

Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in Table 2B row 6.

Table 2B row 6. Record Treatment, Payment, and Health Care Operations Disclosures: The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.

B.13.4 Output data validation

Canada

Canada Health Infoway Security Requirement 78: Validating Printed Data

All POS systems connected to the EHRi should ensure it is possible to check that hardcopy print-outs are complete (e.g.: "page 3 of 5").

Rationale: This is a minimum requirement to promote data integrity. It prevents covert selective presentation of data.

See also ISO/IEC 27001:2005, A.12.2.4.

UK

UK IG Requirement 3.17.5

The Supplier shall ensure that the system provides a means for users to check that hardcopy print-outs are complete (e.g. "page 3 of 5" annotations).

B.14 Record retention

Canada

Canada Health Infoway Privacy Requirement 21: Retaining Records

The EHRi, POS systems connected to the EHRi, organizations connecting to the EHRi, and organizations hosting components of the EHRi:

a) must retain PHI in accordance with record-keeping requirements outlined in legislation; and

b) should develop guidelines and implement procedures with respect to the retention of PHI, including minimum and maximum retention periods.

Rationale: This is perceived to be a heavy burden in legacy or paper based systems; the electronic health record environment should be designed to implement such rules systematically. At the same time, patients/persons need to recognize the need of the healthcare system to hold certain core information about them on a more permanent basis.

UK

UK IG Requirement 3.11.6

The system shall ensure all data are stored for periods as defined by DH policy and described in the NHS Records Management Code of Practice Parts 1 and 2.

