14.2.9 System acceptance testing

Control

ISO/IEC 27002:2013, 14.2.9, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall establish acceptance criteria for planned new information systems, upgrades and new versions. They shall carry out suitable tests of the system prior to acceptance.

Clinical users should be involved in the testing of clinically relevant system features.

Implementation guidance

ISO/IEC 27002:2013, 14.2.9, applies.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

Control

ISO/IEC 27002:2013, 14.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.3.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should not use actual personal health information as test data.

Other information

ISO/IEC 27002:2013, 14.3.1, applies.

Other health-specific information

ISO/TS 14441 contains detailed guidance on conformance testing of EHR systems, including use of test data.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

ISO/IEC 27002:2013, 15.1.1, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing health information shall assess the risks associated with access by external parties to these systems or the data they contain, and then implement security controls that are appropriate to the identified level of risk and to the technologies employed.

Implementation guidance

ISO/IEC 27002:2013, 15.1.1, applies.

Other health-specific information

Risk assessment is essential for effective management of third-party access to systems containing health information, especially personal health information. The rights of subjects of care should be protected, even when an external party with potential access to personal health information is located in a jurisdiction different than the one governing the subject of care or health organization.

Other information

ISO/IEC 27002:2013, 15.1.1, applies.

15.1.2 Addressing security within supplier agreements

Control

ISO/IEC 27002:2013, 15.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.1.2, applies.

Health-specific implementation guidance

Third-party service delivery management is greatly simplified when a formal agreement is adopted which specifies the minimum set of controls to be implemented.

Other information

ISO/IEC 27002:2013, 15.1.2, applies.

15.1.3 Information and communication technology supply chain

Control

ISO/IEC 27002:2013, 15.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 15.1.3, applies.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Control

ISO/IEC 27002:2013, 15.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health. See also health-specific implementation guidance in 15.1.2.

15.2.2 Managing changes to supplier services

Control

ISO/IEC 27002:2013, 15.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health. See also health-specific implementation guidance in 15.1.2.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Control

ISO/IEC 27002:2013, 16.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.1, applies.

Other information

ISO/IEC 27002:2013, 16.1.1, applies.

16.1.2 Reporting information security events

Control

ISO/IEC 27002:2013, 16.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.2, applies.

Health-specific controls

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should establish security incident management responsibilities and procedures in order:

a) to ensure effective and timely response to security incidents;

b) to ensure that there is an effective and prioritized escalation path for incidents, such that crisis management and business continuity management plans can be invoked in the right circumstances and at the right time;

c) to collect and preserve incident-related audit logs and other relevant evidence.

Information security incidents include corruption or unintentional disclosure of personal health information or the loss of availability of health information systems, where such a loss adversely affects patient care or contributes to adverse clinical events.

Organizations should inform the subject of care whenever personal health information has been unintentionally disclosed.

Organizations should inform the subject of care whenever lack of availability of health information systems may have adversely affected their care.

Health-specific implementation guidance

There is a tendency in health organizations to artificially separate information security incidents from other types of incident, both in handling and in reporting. In recognition of the fact that a break-in could have led to theft of IT hardware (leading to a confidentiality breach), or that a fire could have been set to disguise misuse of IT equipment, or that an identified misuse or erroneous use of the system could have had clinical consequences, an information security assessment should be made either on all such incidents or on a representative incident, to further evaluate the efficacy of established controls and of the risk assessment that lead to their implementation.

Other information

ISO/IEC 27002:2013, 16.1.2, applies.

Other health-specific information

In many jurisdictions, data breaches involving personally identifiable information shall, by law, be reported to the data subjects whose personal information was breached. Even in those jurisdictions where no such law exists for personally identifiable information in general, there may be laws requiring notification of patients where their personal health information is breached (e.g. four Canadian provinces have laws requiring notification of breaches of personal health information, despite having no similar breach notification law for other personally identifiable data).

Information security events may include patient safety incidents where data processing or data transfer played a role.

In some jurisdictions, patients have a right to be informed of any breach of their personal health information.

16.1.3 Reporting information security weaknesses

Control

ISO/IEC 27002:2013, 16.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 16.1.3, applies.

16.1.4 Assessment of and decision on information security events

Control

ISO/IEC 27002:2013, 16.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.4, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should assess whether the information security event involved personal health information.

16.1.5 Response to information security incidents

Control

ISO/IEC 27002:2013, 16.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 16.1.5, applies.

16.1.6 Learning from information security incidents

Control

ISO/IEC 27002:2013, 16.1.6, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.6, applies.

Other information

ISO/IEC 27002:2013, 16.1.6, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

16.1.7 Collection of evidence

Control

ISO/IEC 27002:2013, 16.1.7, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.7, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information may need to consider the implications of collecting evidence for purposes of establishing medical malpractice and may also need to consider inter-jurisdictional requirements when health information systems are accessible across jurisdictional boundaries.

Other information

ISO/IEC 27002:2013, 16.1.7, applies.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control

ISO/IEC 27002:2013, 17.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, the following considerations are important in healthcare environments. Business continuity management, which includes disaster recovery, is increasingly recognised as a requirement for health organizations and the priority it is accorded continues to grow. Reflecting the rigorous availability requirements in healthcare, a major effort ought to be invested in resilience and redundancy arrangements, not just for the technology itself, and but also for the cross-training of health personnel.

Business continuity planning in healthcare is especially challenging for the information security professional, as any plans will need to be suitably integrated with the organization's plans for handling power failures, implementing infection control and dealing with other clinical emergencies. Indeed, the invocation of any of these is likely to lead directly to the invocation of the business continuity management plan, if only to provide support additional to that normally available. However, recent incidents such as the SARS outbreak have shown that major incidents may cause a staff shortage, which may then severely limit the ability to successfully operate business continuity management plans.

Health organizations should ensure that their business continuity management planning includes health crisis management planning. Patient lives may depend upon access to patient data and it is essential that this be taken into account during planning. Catastrophes and force majeure crises that would disable IT systems in other industrial sectors are the very events that may precipitate a health crisis in which timely access to health information is crucial.

Health organizations also need to ensure that the plans that they develop are regularly tested on a "programmatic" basis. The tests included in that programme should build upon one another, proceeding from desktop testing to modular testing to synthesis of likely recovery times and then finally to full rehearsals. Such a programme is thus low risk and delivers real improvement in the general level of awareness in its user population.

Finally, health organizations should remain cognizant of the role that health information systems play in patient continuity of care. Such organizations should be prepared if/when IT systems fail.

Other information

ISO/IEC 27002:2013, 17.1.1, applies.

17.1.2 Implementing information security continuity

Control

ISO/IEC 27002:2013, 17.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.2, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, organizations processing personal health information should identify processes, systems and other relevant equipment that are vital in health care delivery.

Fall-back procedures should be considered as necessary in order to counter failure in processes, systems and relevant equipment that are vital in health care delivery.

Other information

ISO/IEC 27002:2013, 17.1.2, applies.

17.1.3 Verify, review and evaluate information security continuity

Control

ISO/IEC 27002:2013, 17.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 17.1.3, applies.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control

ISO/IEC 27002:2013, 17.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 17.2.1, applies.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

Control

ISO/IEC 27002:2013, 18.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations should put a compliance auditing programme in place that addresses the full life cycle of operations, not just of those processes that identify issues, but also of those that review outcomes and that decide on updates to the ISMS.

Health organizations' audit programmes should be formally structured to cover all elements of this International Standard, all areas of risk and all implemented controls, within a 12 month to 18 month cycle.

In the highly regulated and audited environment of many health organizations, the ISMF ought to set itself the objective of establishing a graduated compliance auditing framework, whose bottom layer is self-audit by the process operators and managers. Thereafter, the auditing of the ISMS, on behalf of the ISMF, internal auditing, controls assurance assessments and external audits, ought to be defined in a manner that allows each layer to draw confidence from all of the layers below it.

18.1.2 Intellectual property rights

Control

ISO/IEC 27002:2013, 18.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.1.2, applies.

18.1.3 Protection of records

Control

ISO/IEC 27002:2013, 18.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.1.3, applies.

18.1.4 Privacy and protection of personally identifiable information

Control

ISO/IEC 27002:2013, 18.1.4, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should manage informational consent of subjects of care.

Where possible, informational consent of subjects of care should be obtained before personal health information is e-mailed, faxed, communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.

Implementation guidance

ISO/IEC 27002:2013, 18.1.4, applies.

Health-specific implementation guidance

An example of legislation or regulation requiring informational consent from subjects of care is the Council of Europe Recommendation, R (97)5 On the Protection of Medical Data, Council of Europe, Strasbourg, 12 February 1997:

Before a genetic analysis is carried out, the data subject should be informed about the objectives of the analysis and the possibility of unexpected findings.

They should be informed of unexpected findings if:

a) not prohibited by domestic law

b) the person himself has asked for this information

c) the information is not likely to cause serious harm:

    1) to his/her health

    2) to his/her consanguine or uterine kin, to a member of his/her social family, or to a person who has a direct link with his/her genetic line

d) this information is of direct importance to him/her for treatment or prevention.

An example of a professional ethical guideline requiring patient consent is the World Health Association's Declaration of Helsinki regarding medical research on human subjects.

Other information

ISO/IEC 27002:2013, 18.1.4, applies.

Other health-specific information

Further information on the management of information consent in healthcare can be found in ISO/TS 17975.

18.1.5 Regulation of cryptographic controls

Control

ISO/IEC 27002:2013, 18.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 Independent review of information security

Control

ISO/IEC 27002:2013, 18.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.2.1, applies.

18.2.2 Compliance with security policies and standards

Control

ISO/IEC 27002:2013, 18.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.2.2, applies.

18.2.3 Technical compliance review

Control

ISO/IEC 27002:2013, 18.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.3, applies.

Health-specific implementation guidance

Special attention is drawn to compliance for the purpose of technical interoperability, as large-scale health information systems typically consist of many interoperating systems.

Other information

ISO/IEC 27002:2013, 18.2.3, applies.