INTERNATIONAL STANDARD

ISO 27799

Second edition
2016-07-01

Health informatics — Information security management in health using ISO/IEC 27002

Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002

Reference number
ISO 27799:2016(E)

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

Contents

Page

Foreword

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

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 27799:2008), which has been technically revised.

Introduction

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information. It is based upon and extends the general guidance provided by ISO/IEC 27002:2013 and addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information is to be protected to ensure patient safety, and an important component of that protection is ensuring that the information's entire life cycle be fully auditable. The availability of health information is also critical to effective healthcare delivery. Health informatics systems is to meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. Protecting the confidentiality, integrity and availability of health information therefore requires health sector specific expertise.

Regardless of size, location and model of service delivery, all healthcare organizations need to have stringent controls in place to protect the health information entrusted to them. Yet many health professionals work as solo health providers or in small clinics that lack the dedicated IT resources to manage information security. Healthcare organizations therefore need clear, concise, and health-care-specific guidance on the selection and implementation of such controls. This International Standard is to be adaptable to the wide range of sizes, locations, and models of service delivery found in healthcare. Finally, with increasing electronic exchange of personal health information between health professionals (including use of wireless and Internet services), there is a clear benefit in adopting a common reference for information security management in healthcare.

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa, the United Kingdom and elsewhere. ISO 27799 draws upon the experience gained in these national endeavours in dealing with the security of personal health information and is intended as a companion document to ISO/IEC 27002. It is not intended to supplant the ISO/IEC 27000-series of standards. Rather, it is a complement to these more generic standards.

ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, but some controls require additional explanation in regard to how they can best be used to protect the confidentiality, integrity and availability of health information. There are also additional health sector specific requirements. This International Standard provides additional guidance in a format that persons responsible for health information security can readily understand and adopt.

In the health domain, it is possible for an organization (a hospital, say) to be certified using ISO/IEC 27001 without requiring certification against or even acknowledgement of ISO 27799. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with ISO 27799 as a stricter standard for healthcare will also become widespread.

Objectives

Maintaining information confidentiality, availability, and integrity (including authenticity, accountability and auditability) are the overarching goals of information security. In healthcare, privacy of subjects of care depends upon maintaining the confidentiality of personal health information. To maintain

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific control

Organizations processing health information, including personal health information, shall have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.

Implementation guidance

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific implementation guidance

In addition to following the guidance, given by ISO/IEC 27002 on what an information security policy should contain, this policy should contain statements on:

a) the need for health information security;

b) the goals of health information security;

c) compliance scope, as described in Clause 18;

d) legislative, regulatory, and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information;

e) arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination;

f) the identification of processes and systems that are vital in health care (i.e. failure may lead to adverse patient effects).

Ideally, revision of the policy's contents will be driven by the findings of the organization's risk assessment, although the policy itself need only set direction, state principles and point to other International Standards, where the (more frequently changing) specifics are to be found.

In creating their information security policy document, health organizations will need to specifically consider the following factors, which are unique to the health sector:

a) the breadth of health information;

b) the rights and ethical responsibilities of staff, as agreed in law, and as accepted by members of professional bodies;

c) the rights of subjects of care, where applicable, to privacy and to access to their records;

d) the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information;

e) the legitimate needs of clinicians and health organizations to be able to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain subjects of care to express their preferences, necessitate such overrides, also the procedures to be employed to achieve this;

f) the obligations of the respective health organizations, and of subjects of care, where healthcare is delivered on a "shared care" or "extended care" basis;

g) the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials;

h) the arrangements for, and authority limits of, temporary staff, such as locums, students and "on-call" staff;

i) the arrangements and limitations placed upon access to personal health information by volunteers and support staff, such as clergy and charity personnel;

j) the implications of security measures on patient safety;

k) the implications of information security measures on the performance of health information systems.

Many health organizations have found it advantageous to make the policy document available to staff electronically via an information security area on the health organization's Intranet.

Where the health organization obtains support from third-party organizations or collaborates with third parties, and especially where it receives services from other jurisdictions, the policy framework should include documented policy, controls and procedures that cover such interactions and that specify the responsibilities of all parties. In cases where personal data is crossing national or jurisdictional boundaries, the provisions of ISO 22857 should be applied.

Other information

ISO/IEC 27002:2013, 5.1.1, applies.

5.1.2 Review of the policies for information security

Control

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific control

The health organization's information security policy should be subject to ongoing, staged review, such that the totality of the policy is addressed at least annually. The policy should be reviewed after the occurrence of a serious security incident.

Implementation guidance

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, such review should address:

a) the changing nature of the health organization's operations and the concomitant changes to risk profile and risk management needs;

b) the changes made to the IT infrastructure of the organization, and the concomitant changes these bring to the organization's risk profile;

c) the changes identified in the external environment that similarly impact the organization's risk profile;

d) the latest controls, compliance and assurance requirements and arrangements mandated by jurisdictional health bodies or by new legislation or regulation;

e) the latest guidance and recommendations from health professional associations and from information privacy commissioners regarding the protection of personal health information;

f) the results of legal cases tested in the courts, which have established or negated precedents or established practices;

g) the challenges and issues regarding the policy, as expressed to the organization by its staff, subjects of care and their partners and care givers, researchers and governments (e.g. privacy commissioners);

h) reports on patient safety incidents in order to devise mitigations in those cases where the patient safety incident is the result of failures of information security measures.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific control

Organizations processing personal health information shall:

a) clearly define and assign information security responsibilities;

b) have an information security management forum (ISMF) in place to ensure that there is clear direction and visible management support for security initiatives involving the security of health information, as described in B.3 and B.4.

At a minimum, at least one individual shall be responsible for health information security within the organization.

The health information security forum shall meet regularly, on a monthly or near-to-monthly basis. (Typically, it is most effective to meet at the mid-point between the meetings of the governance body into which the forum reports. This allows emergency matters to be taken to a suitable meeting within a short period.)

A formal scope statement shall be produced that defines the boundary of compliance activity in terms of people, processes, places, platforms and applications.

Implementation guidance

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the essential nature of management responsibility in organizations that are custodians of personal health information, as described in B.2. Accountability and coordination can only be maintained over the long term, if the organization has an explicit information security management infrastructure.

Whatever organizational structure is adopted, it is of critical importance that it be designed and structured to facilitate access by subjects of care (e.g. to make requests to obtain personal health information), to facilitate reporting within the organizational structure and to ensure timely delivery of information.

As noted in B.4.3, the organization's (virtual or actual) information security officer should, among other duties, report to the forum and provide it with secretariat services. The officer should be responsible for collating, publishing and commenting on the reports received by forum members.

Health organizations should publicise the scope statement widely within the organization, then review it and ensure it is adopted by the organization's information, clinical and corporate governance groups.

Other information

ISO/IEC 27002:2013, 6.1.1, applies.

6.1.2 Segregation of duties

Control

ISO/IEC 27002:2013, 6.1.2, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information should, where feasible, segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of personal health information.

Implementation guidance

ISO/IEC 27002:2013, 6.1.2, applies.

Other information

ISO/IEC 27002:2013, 6.1.2, applies.

6.1.3 Contact with authorities

Control

ISO/IEC 27002:2013, 6.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 6.1.3, applies.

6.1.4 Contact with special interest groups

Control

ISO/IEC 27002:2013, 6.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.4, applies.

In addition to the guidance given by ISO/IEC 27002, it is important to understand that the task of identifying and registering users of health information systems includes all of the following:

a) the accurate capture of a user's identity (e.g. Joan Smith, born March 26th 1982, currently resident at a specific address);

b) the accurate capture, after verification, of a user's enduring professional credentials (e.g. Dr. Joan Smith, cardiologist) and/or job title (e.g. Susan Jones, Medical Receptionist);

c) the assignment of an unambiguous user identifier.

Note that subjects of care are not typically system users, although those who are able to access all or part of their personal data online (e.g. through an online portal) would indeed be system users (though ones who are granted limited access). Note also that there are health applications where a user may seek general health advice and information. While this request for information may be recorded, the accessing user remains anonymous. Many Web sites offering information on pregnancy, AIDS, or other public health topics operate in this fashion. Users of such general information sites do not typically require registration and are therefore excluded from consideration in the discussion that follows. See also 7.2.1.

Other information

ISO/IEC 27002:2013, 9.2.1, applies.

9.2.2 User access provisioning

Control

ISO/IEC 27002:2013, 9.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.2, applies.

Health-specific implementation guidance

User access provisioning procedures should clearly determine whether users will or will not have access to personal health information.

Other information

ISO/IEC 27002:2013, 9.2.2, applies.

9.2.3 Management of privileged access rights

Control

ISO/IEC 27002:2013, 9.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.3, applies.

Health-specific implementation guidance

In the discussion that follows, several access control strategies are specified that can help significantly to ensure the confidentiality and integrity of personal health information. These are:

a) role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles;

b) workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access;

c) discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).

In addition to following the guidance given by ISO/IEC 27002, health information systems containing personal health information should support role-based access control capable of mapping each user to one or more roles and each role to one or more system functions.

A user of a health information system containing personal health information shall access its services in a single role (i.e. users who have been registered with more than one role shall designate a single role during each health information system access session).

Health information systems should associate users (including health professionals, supporting staff and others) with the records of subjects of care and allow future access based on this association.

Additional guidance on privilege management in health can be found in ISO 22600-1 and in ISO 22600-2.

Other information

ISO/IEC 27002:2013, 9.2.3, applies.

9.2.4 Management of secret authentication information of users

Control

ISO/IEC 27002:2013, 9.2.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.4, applies.

Health-specific implementation guidance

No additional guidance for information security management in health, although it should be noted that time pressures found in health delivery situations can make effective use of passwords difficult to employ. Many health organizations have considered the adoption of alternative authentication technologies to address this problem.

Other information

ISO/IEC 27002:2013, 9.2.4, applies.

9.2.5 Review of user access rights

Control

ISO/IEC 27002:2013, 9.2.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.5, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to personal health information in emergency situations, where a subject of care may be unable to communicate consent.

Other information

ISO/IEC 27002:2013, 9.2.5, applies.

9.2.6 Removal or adjustment of access rights

Control

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific control

All organizations that process personal health information shall, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting, or volunteer activities.

Implementation guidance

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the many examples in healthcare of students, interns and locums who have retained their access privileges after cessation of their internship, locum, etc. Especially in large hospitals, large numbers of temporary staff will typically have short-term access to personal health information. The termination of the access rights of such staff needs to be carefully managed. At the same time, in healthcare, many transactions take place well after the time of care (e.g. the sign-off of medical transcriptions). This can significantly complicate the process of removing access rights in a timely fashion and these transactions should be taken into account when designing and implementing procedures on the removal of access rights.

Health organizations should seriously consider immediate termination of access rights following the supply of a resignation notice, notice of dismissal, etc. wherever an increased risk is perceived from the continuation of such access.

Other information

ISO/IEC 27002:2013, 9.2.6, applies.

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Control

ISO/IEC 27002:2013, 9.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.3.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing health information should, when determining user responsibilities, respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies.

Other information

ISO/IEC 27002:2013, 9.3.1, applies.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Control

ISO/IEC 27002:2013, 9.4.1, applies.

Health-specific control

Health information systems processing personal health information shall authenticate users and should do so by means of authentication involving at least two factors.

Access to information and application system functions related to the processing personal health information should be isolated from (and separate to) access to information processing infrastructure that is unrelated to the processing of personal health information.

Implementation guidance

ISO/IEC 27002:2013, 9.4.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, special consideration should be given to the technical measures by which a subject of care is securely authenticated when accessing all or part of his/her own information (in those health information systems that permit such access). Similar emphasis should also be given to the ease of use of such measures, especially for handicapped subjects of care, and to provisions for access by substitute decision makers.

9.4.2 Secure log-on procedures

Control

ISO/IEC 27002:2013, 9.4.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 9.4.2, applies.

9.4.3 Password management system

Control

ISO/IEC 27002:2013, 9.4.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

ISO/IEC 27002:2013, 12.4.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.4.3, applies.

Other information

ISO/IEC 27002:2013, 12.4.3, applies.

12.4.4 Clock synchronisation

Control

ISO/IEC 27002:2013, 12.4.4, applies.

Health-specific control

Health information systems supporting time-critical-shared care activities shall provide time synchronization services to support tracing and reconstitution of activity timelines where required.

Implementation guidance

ISO/IEC 27002:2013, 12.4.4, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that the timing of events as electronically recorded in personal health information and in audit records can play an essential role in processes, such as coroners' inquests, investigations into medical malpractice and other judicial or quasi-judicial proceedings where it is essential to accurately determine a clinical sequence of events.

Other information

ISO/IEC 27002:2013, 12.4.4, applies.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

ISO/IEC 27002:2013, 12.5.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.5.1, applies.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control

ISO/IEC 27002:2013, 12.6.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.6.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 12.6.1, applies.

12.6.2 Restrictions on software installation

Control

ISO/IEC 27002:2013, 12.6.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.6.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 12.6.2, applies.

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Control

ISO/IEC 27002:2013, 12.7.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.7.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

Control

ISO/IEC 27002:2013, 13.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.1.1, applies.

13.1.2 Security of network services

Control

ISO/IEC 27002:2013, 13.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should carefully consider what impact the loss of network service availability will have upon clinical practice. See also Clause 17.

Other information

ISO/IEC 27002:2013, 13.1.2, applies.

13.1.3 Segregation in networks

Control

ISO/IEC 27002:2013, 13.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.1.3, applies.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

ISO/IEC 27002:2013, 13.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.1, applies.

Health-specific implementation guidance

Organizations shall ensure that the security of such exchanges of information is the subject of policy development and compliance audit (see Clause 18).

The security of information exchanges can be greatly assisted by the use of information exchange agreements that specify the minimum set of controls to be implemented.

Special attention should be given to the usability of cryptographic tools. If such tools are too complex, healthcare users might abstain from using them.

See also health-specific implementation guidance in 8.2.1.

Other information

ISO/IEC 27002:2013, 13.2.1, applies.

Other health-specific information

Specific guidance on health information exchange policies can be found in ISO 22857. Though that International Standard explicitly references trans-border flow of personal health information (where borders in this context represent health jurisdictions, not necessarily national boundaries), much of its advice can be adapted, where necessary, to deal with exchange of data from one organization to another.

13.2.2 Agreements on information transfer

Control

ISO/IEC 27002:2013, 13.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.2.2, applies.

Other health-specific information

As noted in 13.2.1, specific guidance on health information exchange policies can be found in ISO 22857. Though that International Standard explicitly references trans-border flow of personal health information (where borders in this context represent health jurisdictions, not necessarily national boundaries), much of its advice can be adapted, where necessary, to deal with exchange of data from one organization to another.

13.2.3 Electronic messaging

Control

ISO/IEC 27002:2013, 13.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other health-specific information

ISO/TS 14441 contains a detailed set of functional privacy and security requirements for EHR systems.

14.1.1.1 Uniquely identifying subjects of care

Health-specific control

Health information systems processing personal health information:

a) shall ensure that each subject of care can be uniquely identified within the system;

b) shall be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Health-specific implementation guidance

The provision of emergency care and other situations in which adequate identification of subjects of care may not have been possible will inevitably create instances of multiple records for the same patient. Some capacity shall exist within every health information system to merge multiple instances of patient records into a single record. Such merging requires the greatest care and will therefore not only necessitate personnel trained in such merging, but may also require technical tools to better facilitate the integration of information from the original records into a unified whole.

Organizations processing personal health information should ensure that data from which personal identification can be derived is only retained where it is necessary to do so and that deletion, anonymization and pseudonymization techniques are appropriately used to the full extent possible to minimize the risk of unintentional disclosures of personal information.

14.1.1.2 Output data validation

Health-specific control

Health information systems processing personal health information shall provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the subject of care under treatment.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, some additional important factors need to be considered. Before relying on personal health information provided by a health information system, health professionals need to be shown sufficient information to ensure that the subject of care they are treating matches the information retrieved. Matching a subject of care under treatment to an existing record can be a non-trivial task. Some systems enhance security by including photographic ID with each subject of care's record. Such enhancements may themselves create privacy problems, as they potentially permit the implicit capture of facial characteristics, such as race that are not included as fields of data. The requirements for identification of subjects of care and the availability of data used to support it may also vary from jurisdiction to jurisdiction. Great care needs to be exercised in the design of health information systems to ensure that health professionals can trust the system to provide the information needed to confirm that each record retrieved matches the individual under treatment.

Health information systems should make it possible to check that hardcopy print-outs are complete (e.g. page 3 of 5).

Other information

ISO/IEC 27002:2013, 14.1.1, applies.

14.1.2 Securing application services on public networks

Control

ISO/IEC 27002:2013, 14.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.1.2, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the care that shall be taken in determining whether data involved in electronic commerce and online transactions contain personal health information. If they do, this information needs to be appropriately protected. Of special concern in healthcare are data related to billing, medical claims, invoice lines, requisitions, and other e-commerce data from which personal health information can be derived.

Other information

ISO/IEC 27002:2013, 14.1.2, applies.

14.1.3 Protecting application services transactions

Control

ISO/IEC 27002:2013, 14.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.1.3, applies.

Health-specific implementation guidance

See Health-specific implementation guidance in 14.1.2.

Other information

ISO/IEC 27002:2013, 14.1.3, applies.

14.1.3.1 Publicly available health information

Health-specific controls

Publicly available health information (as distinct from personal health information) should be archived.

The integrity of publicly available health information should be protected to prevent unauthorized modification.

The source (authorship) of publicly available health information should be stated and its integrity should be protected.

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Control

ISO/IEC 27002:2013, 14.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.1, applies.

14.2.2 System change control procedures

Control

ISO/IEC 27002:2013, 14.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.2, applies.

14.2.3 Technical review of applications after operating platform changes

Control

ISO/IEC 27002:2013, 14.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.3, applies.

14.2.4 Restrictions on changes to software packages

Control

ISO/IEC 27002:2013, 14.2.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.4, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

14.2.5 Secure system engineering principles

Control

ISO/IEC 27002:2013, 14.2.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.5, applies.

14.2.6 Secure development environment

Control

ISO/IEC 27002:2013, 14.2.6, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.6, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

14.2.7 Outsourced development

Control

ISO/IEC 27002:2013, 14.2.7, applies.

Implementation guidance:

ISO/IEC 27002:2013, 14.2.7, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.7, applies.

14.2.8 System security testing

Control

ISO/IEC 27002:2013, 14.2.8, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.8, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

The tasks and related documents for maintaining and improving the ISMS are summarized in Figure B.7.

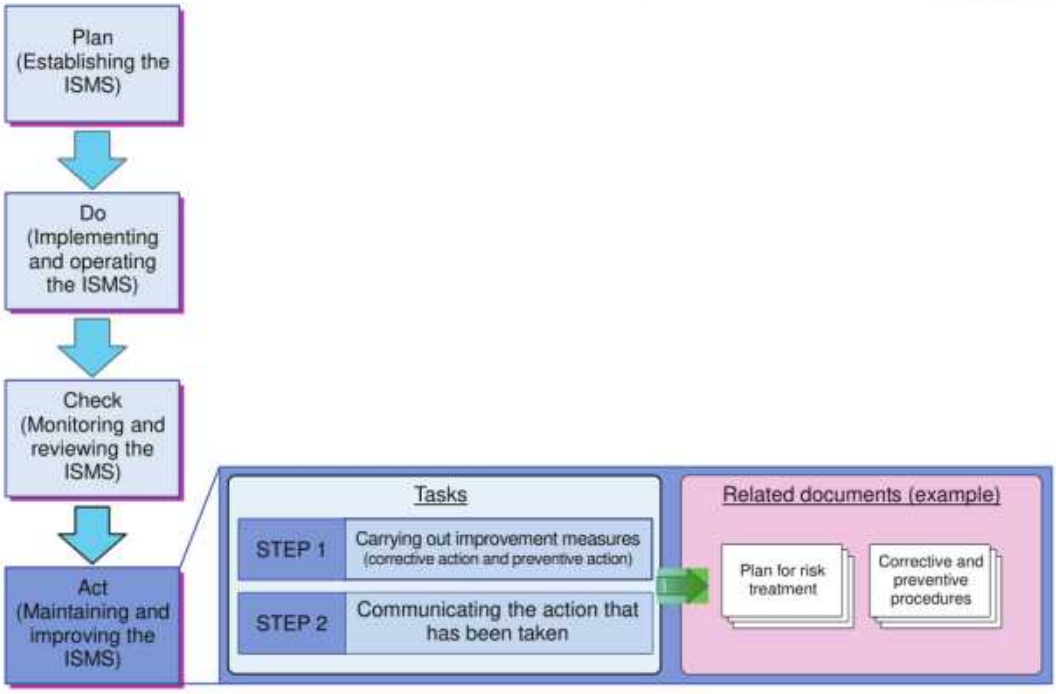

Figure B.7 — Tasks and related documents for monitoring, reviewing, maintaining and improving the ISMS

Annex C
(informative)

Checklist for conformance to ISO 27799

C.1 Instructions for completing the checklist

The checklist in Table C.1 is intended to help organizations processing personal health information determine whether they conform to this International Standard. It lists the controls from this International Standard and contains columns to check where conformance to the controls has been achieved. What follows is an explanation of the columns.

a) Clause: the numbers in the leftmost column corresponds to the clause numbers in the International Standard.

b) Implemented: whether the control is implemented

   1) Yes: the control is implemented and operational.

   2) No: the control is not implemented and operational. The work might be initiated but cannot be said to be fully implemented and in operation within the organization on an ongoing basis.

   Alternatively, the present overall compliance can be presented in percentage figures.

c) Priority: the priority that the organization intends to give the implementation of the control. Recommended to be on a scale of numbers 1, 2, 3, etc., where 1 is the highest priority.

d) Reference document, decision, or diary number: reference to supporting organizational documentation, where applicable.

e) Budgeted: whether implementation of the control has been budgeted (where applicable).

f) Responsible: where the control has not been implemented and operationalized, the name of the person or organizational entity who is nominated by the organization to be responsible for the work of implementing/operationalizing the control.

g) Note: any relevant comments on the control, where applicable.

h) Follow-up: note of what follow-up is planned or performed, where applicable.

The checklist can be used during all types of internal and external auditing and assessment of information security-related work of any organization processing personal health information. The list is designed to give a good overview over the information security situation and also easily be a support for follow-ups.

Table C.1 — Information security controls — Check list for ISO 27799

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
5.1	Management direction for information security								
5.1.1	Policies for information security								
1	Is there a written information security policy?							(Would or should demand?)	
2	Is the written information security policy approved by management?							(Would or should demand?)	

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
3	Is the written information security policy published, and the communicated to all employees and relevant external parties? (how, where, when?)							(Would or should demand?)	
4	Does the information security policy express:								
A	— the need for health information security?								
B	— the goals of health information security?								
C	— compliance scope, as described in 0.0.0.0?								
D	— legislative, regulatory, and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information?								
E	— arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination?								
F	— the identification of processes and systems that are vital in health care (i.e. failure may lead to adverse patient effects)								
G	— the breadth of health information?								
H	— the rights and ethical responsibilities of staff, as agreed in law, and as accepted by members of professional bodies?								
I	— the rights of subjects of care, where applicable, to privacy and to access to their records?								
J	— the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information?								
K	— the legitimate needs of clinicians and health organizations to be able to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain subjects of care to express their preferences, necessitate such overrides; also the procedures to be employed to achieve this?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
L	— the obligations of the respective health organizations, and of subjects of care, where healthcare is delivered on a "shared care" or "extended care" basis?								
M	— the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials?								
N	— the arrangements for, and authority limits of, temporary staff, such as locums, students and "on-call" staff?								
O	— the arrangements for, and limitations placed upon, access to personal health information by volunteers and support staff such as clergy and charity personnel?								
P	— the implications of security measures on patient safety?								
Q	q) the implications of information security measures on the performance of health information systems?								
5.1.2	Review of the policies for information security								
1	Is there an ongoing staged review that addresses the totality of the policy annually?								
2	Is the policy reviewed after the occurrence of a serious security incident?								
	In addition to following the guidance given by ISO/IEC 27002, does the review address:								
A	— the changing nature of the health organization's operations and the concomitant changes to risk profile and risk management needs?								
B	— the changes made to the IT infrastructure of the organization, and the concomitant changes these bring to the organization's risk profile?								
C	— the changes identified in the external environment that similarly impact the organization's risk profile?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
12.1.3	Capacity management								
	No additional guidance								
12.1.4	Separation of development, testing and operational environments								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization separate (physically or virtually) development and testing environments for health information systems processing such information from operational environments hosting those health information systems?								
2	Are rules defined and documented for the migration of software from development to operational status by the organization hosting the affected application(s)?								
12.2	Protection from malware								
12.2.1	Controls against malware								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization implement appropriate prevention, detection and response controls to protect against malicious software?								
2	Does the organization implement appropriate user awareness training to protect against malicious software?								
12.3	Backup								
12.3.1	Information backup								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization back up all personal health information and store it in a physically secure environment to ensure its future availability?								
2	Does the organization, in order to protect confidentiality, back up personal health information in an encrypted format?								
12.4	Logging and monitoring								
12.4.1	Event logging								
1	Do the health information systems processing personal health information, create a secure audit record each time a user accesses, creates, updates or archives personal health information via the system?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Does the audit log uniquely identify the user, uniquely identify the data subject (i.e. the subject of care), identify the function performed by the user (record creation, access, update, etc.), and note the time and date at which the function was performed?								
3	When personal health information is updated, is a record of the former content of the data and the associated audit record (i.e. who entered the data on what date) retained?								
4	When messaging systems are used to transmit messages containing personal health information:								
A	Is there a log of such message transmissions?								
B	Does that log contain the time, date, origin and destination of the message, but not its content?								
5	Is there a carefully assessed and determined retention period for these audit logs, with particular reference to clinical professional standards and legal obligations, in order to enable investigations to be carried out when necessary and to provide evidence of misuse where necessary?								
6	Is the health information system's audit logging facility operational at all times while the health information system being audited is available for use?								
7	Are health information systems containing personal health information provided with facilities for analysing logs and audit trails that:								
A	Allow the identification of all system users who have accessed or modified a given subject of care's record(s) over a given period of time?								
B	Allow the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time?								
12.4.2	Protection of log information								
1	Are audit records secure and tamper-proof?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Is access to system audit tools and audit trails safeguarded to prevent misuse or compromise?								
	[There are many Health-specific implementation guidances in relation to protection of log information that are not included in this document], applies								
12.4.3	Administrator and operator logs								
	No additional guidance								
12.4.4	Clock synchronisation								
1	Do health information systems supporting time-critical-shared care activities provide time synchronization services to support tracing and reconstitution of activity timelines where required?								
12.5	Control of operational software								
12.5.1	Installation of software on operational systems								
	No additional guidance								
12.6	Technical vulnerability management								
12.6.1	Management of technical vulnerabilities								
	No additional guidance								
12.6.2	Restrictions on software installation								
1	Are rules governing the installation of software by users established and implemented?								
12.7	Information systems audit considerations								
12.7.1	Information systems audit controls								
	No additional guidance								
13.1	Network security management								
13.1.1	Network controls								
	No additional guidance								
13.1.2	Security of network services								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization carefully consider what impact the loss of network service availability will have upon clinical practice?								
13.1.3	Segregation in networks								
	No additional guidance								
13.2	Information transfer								
13.2.1	Information transfer policies and procedures								
1	Does the organization ensure that the security of such information exchange is the subject of policy development and compliance audit?								
13.2.2	Agreements on information transfer								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
	No additional guidance								
13.2.3	Electronic messaging								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization, when transmitting personal health information by electronic messaging, ensure its confidentiality and integrity?								
2	Are e-mail between health professionals that contain personal health information encrypted in transit?								
13.2.4	Confidentiality or non-disclosure agreements								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization have a confidentiality agreement in place that specifies the confidential nature of this information?								
2	Is the agreement applicable to all personnel accessing health information?								
3	Does the agreement above include reference to the penalties that are possible when a breach in the information security policy is identified?								
14.1	Security requirements of information systems								
14.1.1	Information security requirements analysis and specification								
14.1.1.1	Uniquely identifying subjects of care								
1	Do the health information systems processing personal health information ensure that each subject of care can be uniquely identified within the system?								
2	Are health information systems processing personal health information capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency?								
3	Does the organization ensure that data from which personal identification can be derived is only retained where it is necessary to do so, and that deletion, anonymization and pseudonymization techniques are appropriately used to the full extent possible to minimize the risk of unintentional disclosures of personal information?								

9.6 Preparatory steps

Thaw permanent cultures in a water bath at 37 °C. Add 0,5 ml of a thawed culture to a 25 cm^2 flask which already contains 5 ml of MEM (including 10 % FCS). Incubate cultures at 37 °C, using an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity, to reach a confluency (contact inhibition) of 50 % to maximally 100 % (about 2 d to 4 d). To remove dead cells, replace the medium about 30 h after culture initiation. Use the remaining cells for experiments. (They may also be used for further subculturing.) Discard cells which have undergone more than 15 passages because they cannot be used for further experiments.

9.7 Preparation of test cultures

9.7.1 General

Wash the cells once with 5 ml HBBS (without Ca^{2+} and Mg^{2+}) for about 5 min and then remove the medium by suction.

Trypsinize the cells for about 5 min using about 1,0 ml of trypsin (0,25 %) and approximately 1,0 ml of HBBS (without Ca^{2+} and Mg^{2+}) to separate the cells from the bottom of the culture flask.

Stop this reaction by adding approximately 3 ml of MEM including 10 % FCS.

Pipette this mixture several times to separate cells from the flask and to obtain homogenous, single cell suspensions.

Count the number of cells in a 10 µl sample in a hemocytometer [4].

Dilute the suspension to the required cell density (30 000 to 80 000 per 5 ml culture) using MEM including 10 % FCS.

9.7.2 Seeding

Add 5 ml of cell suspension to each chamber of a culture dish (7.3), of which each chamber contains a slide. Each chamber represents one culture.

Incubate the dishes for 6 h at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity.

Prior to treatment, check the dishes visually for cell attachment. (See Annex B.)

9.7.3 Preparation of S9 mix

Prepare the S9 mix according to 6.5.2.

9.8 Treatment of test cultures

9.8.1 Treatment without S9 mix

Remove the medium from the culture chambers approximately 6 h after seeding. Add 4 ml of fresh medium (with FCS). Thereafter, add the test sample, then either the positive control or the dilution water for the negative control in a volume of 1 ml (final volume of 5 ml). Incubate the cultures for 24 h at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 volume fraction and at least 90 % humidity. Higher concentrations of test sample can be applied as long as the validity and cytotoxicity criteria (3.14, 9.8.5, 10.2) are met. If higher amounts of sample are used, the concentration of the medium has to be adjusted.

---

4) Alternatively, an automatic cell or particle counter device may be used.

9.8.2 Treatment with S9 mix

Remove the medium from the chambers approximately 6 h after seeding. Add to each chamber 1 ml of the S9 mix and 3 ml of fresh medium (without FCS). Thereafter, add the test sample, then either the positive control or the dilution water for the negative control in a volume of 1 ml per culture, resulting in a final volume of 5 ml. Incubate cultures for 4 h at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity. Higher concentrations of test sample can be applied as long as the validity and cytotoxicity criteria (3.14, 9.8.5, 10.2) are met. If higher amounts of sample are used, the concentration of the medium has to be adjusted.

After 4 h, remove the medium and wash the cultures twice with 5 ml HBSS. Add 5 ml of MEM (incl. 10 % FCS) and incubate for further 20 h at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity.

9.8.3 Processing of cell cultures

Prepare cells as follows [13]:

— remove the culture medium completely;

— treat each culture for 3 min with 5 ml of sodium citrate-solution (6.2.17) at a temperature of 37 °C (hypotonic treatment);

— remove the sodium citrate-solution and replace it by approximately 5 ml of fixation solution (6.2.18) at a temperature of about 4 °C for about 5 min; remove and replace the fixation solution by the same amount of fresh fixation solution (4 °C) for about 5 min;

— remove the slides from the culture chambers. Allow the fixation solution to drip off and dry the slides at ambient temperature.

9.8.4 Staining

— After the slides have dried, stain for 3 min in May-Grünwald-solution, modified (6.2.12);

— rinse the slides with WEISE-buffer (6.2.19) and place the slides for approximately 20 min in a Giemsa-solution (6.2.20);

— rinse twice with WEISE-buffer and remove surplus of staining material in xylene. Thereafter, cover the slides with coverslips and examine the slides as in 10.3.

9.8.5 Treatment for determination of the survival index

Seed approximately 250 000 cells into 25 cm^2 flasks already containing 5 ml of MEM (including 10 % FCS) per negative control or test sample concentration. Cultivate the cells for 30 h at 37 °C in an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity (9.6). Thereafter, treat the cells with dilution water or test sample concentrations (9.8).

At the end of the respective treatment period, harvest the cells of all cultures as follows:

— remove the medium and wash once with 5 ml of HBBS (without Ca^{2+} and Mg^{2+});

— trypsinize with about 1,0 ml of trypsin (0,25 %) and about 1,0 ml of HBBS (without Ca^{2+} and Mg^{2+}) to remove cells from bottom of flasks;

— stop the process by adding 3 ml of MEM (including 10 % FCS);

— pipette this mixture several times to separate cells from the flask and to obtain homogeneous single cell suspensions;

— dilute the cells to an appropriate amount in negative controls. Dilute all other cultures as cell suspensions of the negative controls were diluted. The same amount is taken from each culture and counted using a haemocytometer [5] to determine cell survival.

10 Evaluation and assessment

10.1 Cell morphology

At the end of the treatment, check all the cultures by an inverse microscope for changes in cell morphology and attachment of cells at a magnification of about 200-fold with the exception of positive controls. (See Annex B.)

10.2 Selection of concentrations to be analysed

For non-toxic samples, read only the highest tested concentration. For toxic samples, the lowest concentration which induces more than 50 % cytotoxicity in at least one of the indices (10.4, 10.5, 10.6) shall be chosen for reading of slides. Independently, no relevant changes should be induced in cell morphology (10.1) or attachment of cells. If those effects are observed for this concentration, the concentration for reading shall be reduced to the highest concentration which does not induce changes in cell morphology or cell attachment. For toxic samples, the next two lower dilutions of the test sample shall also be read. If a relevant increase in micronucleated cells is observed, lower concentrations are read until the first concentration without clastogenic effect is reached.

Prior to reading slides, check them for their quality. Use only slides of good quality for reading to avoid interference of slide quality with the assessment.

10.3 Reading of slides

Read 1 000 cells per culture and note the number of micronucleated cells amongst them.

Take into account the following criteria:

— the maximum size of a micronucleus is about 30 % of the size of a normal nucleus;

— concerning their staining micronucleus and nucleus shall have the same appearance;

— micronuclei shall be clearly separated from the nucleus;

— only cells with good cytoplasmic outlines are used for reading.

In addition to micronucleated cells, record fragmentations (cells with fragmented nuclei, cells with several nuclei of the same size, and cells with more than six micronuclei) amongst the evaluated 1 000 cells.

10.4 Mitotic index

Determine the mitotic index (3.7) for all cultures microscopically on the slides. The number of mitotic cells among a total of 1 000 cells per culture is determined. All cells which were not in interphase are defined as mitotic.

5) Alternatively, an automatic cell or particle counter device may be used.

10.5 Survival index

Determine the survival index (3.14 and 9.8.5) for all cultures except for positive controls. The number of cells observed for negative controls is set to 100 %. On this basis, the number of living cells in the test sample-treated cultures is converted to a percentage.

10.6 Proliferation index

Determine the proliferation index (3.9) for all cultures except for positive controls.

Evaluate 1 000 cells (counting all cells of each clone) per culture, separated into different clone sizes (1, 2, 4 or 8 cells). Calculate the proliferation index following Equation (1):

$$I_P = \frac{(n_{CL1} \times 1) + (n_{CL2} \times 2) + (n_{CL4} \times 3) + (n_{CL8} \times 4)}{n_{CL}} \quad (1)$$

where

I_P is the proliferation index;

n_{CL} is the number of clones counted;

n_{CL1} is the number of clones with 1 cell;

n_{CL2} is the number of clones with 2 cells;

n_{CL4} is the number of clones with 3 or 4 cells;

n_{CL8} is the number of clones with 5, 6, 7 or 8 cells.

Due to clone disintegration in experiments with the S9 mix, this index is most frequently smaller if compared to experiments without the S9 mix.

10.7 Validity criteria

The mean of the ratio of micronucleated cells in negative control cultures shall not exceed 3 %.

Positive controls shall have induced statistically significant increases in the ratio of micronucleated cells.

10.8 Assessment criteria

The following criteria shall be met for a positive result:

— a significant increase according to an appropriate statistical test (chi-squared test corrected for continuity according to Yates) [15] in micronucleated cells in treated cultures as compared to the respective negative controls;

— the number of micronucleated cells exceed the range of the historical negative control data.

If neither criteria is met, the test sample shall be evaluated as non-genotoxic according to this part of ISO 21427. If only one criterion is met, the test shall be repeated as the result is ambiguous.

10.9 Determination of the decisive D value

The "decisive D value" means the lowest D value (3.4) at which no detectable genotoxic effects are found for cultures treated with the test sample or dilutions thereof according to the criteria given in 10.8.

11 Precision

Results of an interlaboratory trial are given in Annex D.

12 Test report

This clause specifies which information is to be included in the test report. The clause shall require information to be given on at least the following aspects of the test:

— a reference to this part of ISO 21427 (ISO 21427-2);

— identity of the test sample (origin and date of sampling, pH value);

— result, according to Clause 10;

— if appropriate, any deviation from this procedure or circumstances that may have affected the result.

The documentation will include the following information:

a) positive controls (chemical name, source, batch number or comparable data (if available);

b) storage of sample and preparation of test sample (storage conditions (if not tested directly), adjustment of pH value, centrifugation (including g and time), filtration (including filter material and diameter of pores) and other manipulations);

c) cell line (cell line, source, date of arrival, storage conditions, check for karyotype stability, plating efficiency and mycoplasma contamination);

d) metabolizing system (preparation and origin of the S9 fraction, protein content, date of preparation, storage conditions);

e) test environment (address of performing laboratory, date of test);

f) results:

   1) survival index, mitotic index, proliferation index, number of cells analysed, micronculei per culture including means, criteria for considering results positive, negative or equivocal, signs of toxicity, dose-response relationship, and

   2) where possible, statistical analysis and method applied, concurrent and historical negative-control data, concurrent and historical positive-control data, conclusions, D values, other observations (e.g. precipitation).

Annex A
(informative)

Bromodeoxyuridine (BrdU) method

A.1 General

Incubate cells in a surplus of bromodeoxyuridine (BrdU) for about 14 h. Bromodeoxyuridine (BrdU) is incorporated into DNA as replacement for thymidine and results in an altered chromosome staining of affected chromatid parts. Using a special staining procedure, it is possible to differentiate between metaphases, which have undergone 1st, 2nd or 3rd mitosis since co-culturing with BrdU.

A.2 BrdU treatment

Perform subculturing in culture dishes by seeding approximately 80 000 cells of a single cell suspension per culture. Use four harvest times and four cultures per harvest time. Dissolve the BrdU freshly prior to use under light protection at a concentration of 5 µg of BrdU per millilitre in culture medium (including 10 % FCS) and store it under light protection at 4 °C until use.

24 h after passaging, remove the medium from the cultures and replace it under light protection by the "BrdU-medium". Incubate the cultures for 14 h at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 and at least 90 % humidity.

Thereafter, remove the medium under light protection and rinse twice with 5 ml HBSS. Add 5 ml of MEM (including 10 % FCS) per culture and incubate at 37 °C, in an atmosphere containing a volume fraction of 5 % CO_2 and a humidity of at least 90 % until harvest. Harvest the cultures 16 h, 18 h, 20 h and 22 h after the addition of BrdU.

A.3 Preparation of slides

Remove the culture medium completely.

Treat each culture for approximately 20 min with approximately 5 ml of a potassium chloride solution (6.2.29) at a temperature of approximately 37 °C (hypotonic treatment).

Add approximately 5 ml fixation solution (4 °C) (6.2.18) for about 15 min. Remove and replace the fixation solution by the same amount of fresh fixation solution (4 °C) for about 10 min. Remove and replace the fixation solution by the same amount of fresh fixation solution (4 °C) for about 5 min.

Remove the slides from the culture chambers. Allow the fixation solution to drip off and move the slide for a short period through the blue part of the flame of a Bunsen burner.

A.4 Staining of slides

A.4.1 Preparation of Soerensen-buffer

Dissolve 45,36 g KH_2PO_4 in 1 000 ml water (solution A) and dissolve 64,33 g Na_2HPO_4 in 1 000 ml water (solution B). Mix one part A, one part B and 8 parts of deionized water. This results in a solution with a pH of 6.8.

A.4.2 Staining

After storage for 2 d to 4 d in the dark, transfer the slides with the coated side up into dishes and cover with 1 cm of Soerensen-buffer. Thereafter, irradiate with UV-light (wavelength 254 nm) for 10 min from a distance of about 15 cm.

Transfer the slides into holders and immerse them in cuvettes which have previously been filled with "SSC twice" (a solution containing 0,3 mol/l NaCl and 0,03 mol/l of sodium citrate in deionized water). Incubate the slides in "SSC twice" for about 30 min at about 60 °C.

Thereafter, remove the slides and allow them to cool. Afterwards, place them for 10 min in their holders into cuvettes which had already been filled with a Giemsa solution, prepared by adding 15 ml of Giemsa to 185 ml Soerensen-buffer (pH 6.8).

Remove from staining and allow to dry. Remove the surplus of staining material in xylene and cover the slides. Protect slides against light.

A.5 Evaluation

Evaluate 200 metaphases per harvest time and note the numbers of the 1st, 2nd and 3rd metaphases.

The following criteria shall be met:

— in the 1st metaphases, both chromatids of all chromosomes are stained blue-violet;

— in the 2nd metaphases, one chromatid of all chromosomes is stained blue-violet, whereas the corresponding part of its sister chromatid is stained light-violet;

— in the 3rd metaphases, chromatids are stained predominantly light-violet.

A.6 Calculation of cell cycle length

Calculate the cell cycle length, l_{CC}, of the respective cell line according to Equation (A.1):

$$l_{CC} = \frac{t_h}{(1 \times n_1) + (2 \times n_2) + (3 \times n_3)} \times 100 \qquad \text{(A.1)}$$

where

t_h is the harvest time in hours, h;

n_1 is the number of 1st mitosis in percent, %;

n_2 is the number of 2nd mitosis in percent, %;

n_3 is the number of 3rd mitosis in percent, %.

The mean of all four harvest times is used as mean cell cycle length for the respective cell line.

Annex B
(informative)

Evaluation schemes

B.1 Evaluation scheme for cell attachment and cell morphology

1 = good attachment and fibroblast-like cells
2 = slightly reduced attachment and some rounded cells
3 = reduced attachment and cells partly rounded and/or non-attached
4 = no attached cells, all cells rounded

B.2 Evaluation scheme for acceptance of preparations

A = acceptable
- 1 sufficient assessable cells of good quality
- 2 reduced amount of assessable cells
- 3 reduced amount of assessable cells, partly multi-fragmented nuclei

B = limited acceptable
- 1 severe reduction of assessable cells
- 2 severe reduction of assessable cells, partly multi-fragmented nuclei
- 3 interference of precipitate limiting slide reading

N = not acceptable
- 1 no or only few assessable cells
- 2 severe interference of precipitate, no slide reading possible

Annex C
(normative)

S9 fraction

C.1 Induction of liver enzymes

For enzyme induction, at least six male rats (e.g. Sprague-Dawley rats), each with about 200 g to 300 g of body mass, receive a single intraperitoneal injection of a polychlorinated biphenyl (e.g. Aroclor 1254) dissolved in an appropriate vehicle at a dose of 500 mg/kg body mass five days prior to termination. In the case of phenobarbital / β-naphthoflavone induction, the rats simultaneously receive 80 mg/kg body mass phenobarbital intraperitoneally and 80 mg/kg body mass β-naphthoflavone orally on three consecutive days in an appropriate vehicle. The livers are prepared 24 h after the last treatment.

Animals should be kept in special adequately marked cages which will be used only for this purpose. Animal husbandry should be standardized, with 12 h of electrical lighting daily, 20 °C to 23 °C room temperature, and about 60 % mean relative humidity, on a bedding of softwood granules. The air should be changed about ten times per hour. The animals should receive an appropriate standard diet and water of drinking quality ad libitum.

C.2 Preparation of the S9 fraction

Livers shall be removed under sterile conditions immediately after termination and kept at 4 °C ± 1 °C until all the animals have been prepared. All the remaining steps should be carried out under sterile conditions at 4 °C ± 1 °C.

Wash the livers with cold (4 °C ± 1 °C), 0,15 mol/l KCl solution (approximately 1 ml KCl per 1 g liver). Homogenize the livers in fresh, cold (4 °C ± 1 °C), 0,15 mol/l KCl (approximately 3 ml KCl per 1 g liver). Centrifuge the homogenate in a cooling centrifuge at 4 °C ± 1 °C and 9 000 g for 10 min. Store the supernatant (the S9 fraction) below –70 °C in small portions.

Annex D
(informative)

Precision data

The precision data given in Table D.1 were determined in an interlaboratory trial, organized by Germany in November 2005.

Table D.1 — Precision data

Sample No.	Sample	S9-Mix	*l*	Validity criteria		LID	Sample
				NC *o* %	PC *o* %		*o* %
1	Waste water No. 1 spiked with 1 µg/ml Mitomycin C	–	10	0	0	160	0
		+	10	10	0	20	0
2	Waste water No. 2	–	10	0	0	5	0
		+	10	0	10	5	10
3	Waste water No. 3 spiked with 4 µg/ml Cyclophosphamide	–	10	0	10	5	0
		+	9	0	0	20	20
4	Waste water No. 4	–	10	0	10	5	0
		+	10	0	0	5	0

Explanation

l	is the number of laboratories;
o	is the number of outliers;
NC	is the number of negative controls;
PC	is the number of positive controls;
LID	is the lowest ineffective dilution (median).

Bibliography

[1] ISO 5667-1, *Water quality — Sampling — Part 1: Guidance on the design of sampling programmes and sampling techniques*

[2] ISO 5667-2, *Water quality — Sampling — Part 2: Guidance on sampling techniques*

[3] ISO 5667-3, *Water quality — Sampling — Part 3: Guidance on the preservation and handling of water samples*

[4] ISO 5667-10, *Water quality — Sampling — Part 10: Guidance on sampling of waste waters*

[5] ISO 5667-14, *Water quality — Sampling — Part 14: Guidance on quality assurance of environmental water sampling and handling*

[6] ISO 13829, *Water quality — Determination of the genotoxicity of water and waste water using the umu-test*

[7] ISO 16240, *Water quality — Determination of the genotoxicity of water and waste water — Salmonella/microsome test (Ames test)*

[8] ISO/TS 20281, *Water quality — Guidance on statistical interpretation of ecotoxicity data*

[9] AMES, B.N., MCCANN, J. and YAMASAKI, E. Methods for detecting carcinogens and mutagens with the Salmonella/mammalian-microsome mutagenicity test. *Mutation Res.*, **31**, 1975, pp. 347-364

[10] ARMSTRONG, M.J., BEAN, C.L. and GALLOWAY, S.M. A quantitative assessment of the cytotoxicity associated with chromosomal aberration induction in Chinese hamster ovary cells. *Mutation Res.*, **265**, 1992, pp. 45-60

[11] BRADLEY, M.O., BHUYAN, B., FRANCIS, M.C., LANGENBACH, R., PETERSON, A. and HUBERMAN, E. Mutagenesis by chemical agents in V79 Chinese hamster cells: A review and analysis in literature. A report of the Gene-Tox Program. *Mutation Res.*, **87**, 1981, pp. 81-142

[12] DEMARINI, D.M., DALLAS, M.M. and LEWTAS, J. Cytotoxicity and effect on mutagenicity of buffers in a microsuspension assay. *Ter. Carc. Mut.*, **9**, 1989, pp. 287-295

[13] KALWEIT, S., UTESCH, D., VON DER HUDE, U. and MADLE, S. Chemically induced micronucleus formation in V79 cells — comparison of three different test approaches. *Mutation Res.*, **439**, 1999, pp. 183-190

[14] MILLER, B., PUJADAS, E. and GOCKE, E. Evaluation of the micronucleus test *in vitro* using Chinese hamster cells: Results of 4 chemicals weakly positive in the *in vivo* micronucleus test. *Environ. Mol. Mutagen.*, **26**, 1995, pp. 240-247

[15] RICHARDSON, C., WILLIAMS, D.A., ALLEN, J.A., AMPHLETT, G., CHANTER, D.O. and PHILLIPS, B. Analysis of data from in vitro cytogenetic assays. In: *Statistical Evaluation of Mutagenicity Test Data* (ed. D.J. Kirkland), Cambridge University Press, Cambridge, 1989, pp. 141-154

[16] SCOTT, D., GALLOWAY, S.M., MARSHALL, R.R., ISHIDATE, JR. M., BRUSICK, D., ASHBY, J. and MYHR, B.C. Genotoxicity under extreme culture conditions. A report from ICPEMC Task Group 9. *Mutation Res.*, **257**, 1991, pp. 147-204

[17] SPEIT, G., HAUPTER, S. and VOGEL, W. Characterization of mitosis with sister chromatid differentiation (SCD) and consequences for the analysis of proliferation kinetics and sister chromatid exchanges in asynchronously growing cells. *Hum. Genet.*, **71**, 1985, pp. 358-360