

DIN EN ISO 27799

ICS 35.240.80

Einsprüche bis 2014-11-19
Vorgesehen als Ersatz für
DIN EN ISO 27799:2008-10

Entwurf

**Medizinische Informatik –
Informationsmanagement im Gesundheitswesen bei Verwendung der
ISO/IEC 27002 (ISO/DIS 27799:2014);
Englische Fassung prEN ISO 27799:2014**

Health informatics –
Information management in health using ISO/IEC 27002 (ISO/DIS 27799:2014);
English version prEN ISO 27799:2014

Informatique de santé –
Gestion de l'information relative à la santé en utilisant l'ISO/CEI 27002
(ISO/DIS 27799:2014);
Version anglaise prEN ISO 27799:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-09-19 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an named@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Medizin (NAMED), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 131 Seiten

DIN-Normenausschuss Medizin (NAMED)

Nationales Vorwort

Dieses Dokument (prEN ISO 27799:2014) wurde von der WG 4 „Security“ des Technischen Komitees ISO/TC 215 „Health Informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ (Sekretariat: NEN, Niederlande) erarbeitet. Der Arbeitsausschuss NA 063-07-04 AA „Sicherheit“ des Fachbereichs 7 „Medizinische Informatik“ des Normenausschusses Medizin (NAMED) im DIN hat an der Erarbeitung mitgewirkt.

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung von prEN ISO 27799:2014 und ISO/DIS 27799:2014.

Für die im Abschnitt 2 zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO 27000 siehe DIN ISO/IEC 27000

ISO 27002 siehe DIN ISO/IEC 27002

Zusammenfassung

Diese Internationale Norm enthält Richtlinien für die Entwicklung von organisationsbezogenen Informationssicherheitsnormen und Methoden zum Management der Informationssicherheit, einschließlich der Auswahl, Umsetzung und Verwaltung von Maßnahmen, die die Risikoumgebung(en) der Informationssicherheit der Organisation berücksichtigen.

Diese Norm gibt Richtlinien vor, um die Interpretation und Umsetzung der ISO/IEC 27002 (Information Technology — Security techniques — Code of practice for information security controls) in der medizinischen Informatik zu unterstützen und ist ein begleitendes Dokument zu jener Norm.

Die vorliegende Norm unterstützt die Umsetzung der in ISO/IEC 27002 beschriebenen Maßnahmen und ergänzt diese an geeigneter Stelle, damit sie zum Management der Sicherheit von Gesundheitsinformationen effektiv eingesetzt werden können. Mit der Umsetzung dieser Norm ist es Organisationen der Gesundheitsversorgung und anderen Verwahrern von Gesundheitsinformationen möglich, ein minimal erforderliches Sicherheitsniveau sicherzustellen, das den Randbedingungen der Organisationen angemessen ist und das die Vertraulichkeit, Integrität und Verfügbarkeit von persönlichen Gesundheitsinformationen in der Versorgung aufrechterhält.

Diese Norm gilt für Gesundheitsinformationen in all ihren Aspekten; denn, in welcher Form auch immer die Informationen vorliegen (Worte und Zahlen, Tonaufzeichnungen, Abbildungen, Videomaterial und medizinische Bilder), welche Mittel auch immer zur Speicherung genutzt werden (auf Papier drucken oder schreiben oder elektronisches Speichern) und welche Mittel auch immer zur Übertragung genutzt werden (manuell, per Fax, über Computernetzwerke oder per Post), die Informationen müssen immer angemessen geschützt werden.

Diese Norm definiert gemeinsam mit ISO/IEC 27002, was in Bezug auf die Informationssicherheit in der Gesundheitsversorgung erforderlich ist; sie definieren nicht, wie diese Anforderungen zu erfüllen sind. Somit ist diese Norm — soweit es irgendwie möglich ist — technologieneutral. Neutralität im Hinblick auf die Umsetzung von Technologien ist ein wesentliches Kennzeichen. Sicherheitstechnologien unterliegen immer noch einer schnellen Entwicklung und die Geschwindigkeit dieser Änderungen wird derzeit in Monaten und nicht in Jahren gemessen. Im Gegensatz dazu wird von Normen erwartet, auch wenn sie einer periodischen Überarbeitung unterliegen, dass sie im Großen und Ganzen für Jahre gültig bleiben. Ebenso wichtig ist, dass Technologieneutralität es Anbietern und Dienstleistern überlässt, neue oder sich entwickelnde Technologien anzubieten, die die in dieser Norm beschriebenen notwendigen Anforderungen erfüllen.

Wie in der Einleitung bereits festgehalten, ist die Kenntnis der ISO/IEC 27002 für das Verständnis dieser Norm unverzichtbar.

Die folgenden Gebiete der Informationssicherheit liegen außerhalb des Anwendungsbereiches dieser Norm:

- a) Methoden und statistische Tests zur effektiven Anonymisierung persönlicher Gesundheitsinformationen;
- b) Methoden zur Pseudonymisierung persönlicher Gesundheitsinformationen (siehe Anhang D für eine kurze Beschreibung einer Technischen ISO-Spezifikation, die sich speziell mit diesem Thema befasst);
- c) Dienstgüte des Netzwerks und Methoden, um die Verfügbarkeit von Netzwerken, die für die medizinische Informatik genutzt werden, zu messen; und
- d) Datenqualität (soweit nicht identisch mit Datenintegrität).

Änderungen

Gegenüber DIN EN ISO 27799:2008-10 sind folgende Änderungen vorgesehen:

- a) Änderung des Titels von „Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“ in „Informationsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“;
- b) Anpassung des gesamten Dokuments an die aktuelle Ausgabe der ISO/IEC 27002.

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe ist identisch mit der Benummerung in der Englischen Fassung.

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

medizinische Informatik

wissenschaftliche Fachrichtung, die sich mit den kognitiven, informationsverarbeitenden und kommunikativen Aufgabenstellungen der Praxis, Ausbildung und Forschung in der Gesundheitsversorgung befasst, einschließlich der Informationswissenschaft und -technologie, um diese Aufgabenstellungen zu unterstützen

[ISO 18307]

3.2

Gesundheitsinformationssystem

Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen, in einer von Computern zu verarbeitenden Form, sicher gespeichert und übermittelt sowie zugänglich für mehrere autorisierte Nutzer

[ISO/TR 20514]

3.3

Gesundheitsversorgung

jegliche Art von Dienstleistungen mit Auswirkungen auf den Status der Gesundheit, die von Heilberuflern oder Hilfskräften erbracht wird

[Europäisches Parlament, 1998, wie von der WHO zitiert]

3.4

Organisation der Gesundheitsversorgung

allgemeiner Ausdruck, um viele Arten von Organisationen zu beschreiben, die Dienstleistungen der Gesundheitsversorgung erbringen

[ISO 18307]

3.5

Heilberufler

Person, die von einer anerkannten Stelle autorisiert ist, zur Erbringung gewisser medizinischer Dienstleistungen qualifiziert zu sein

[ISO 17090-1]

3.6

Erbringer von Gesundheitsversorgung

jegliche Person oder Organisation, die in die Erbringung von Gesundheitsversorgung für einen Klienten eingebunden ist oder dazu gehört, oder die sich um das Wohlbefinden eines Klienten kümmert

[ISO 27527]

3.7

identifizierbare Person

jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifizierungsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind

[ISO 22587]

3.8

Patient

behandelte Person (siehe 3.1.9)

3.9

persönliche Gesundheitsinformationen

Informationen über eine identifizierbare Person, die sich auf den körperlichen oder geistigen Gesundheitszustand der betreffenden Person oder auf die Erbringung von Gesundheitsdienstleistungen für die betreffende Person beziehen, und zu denen folgende Informationen gehören können:

- a) Informationen über die Vormerkung der betreffenden Person zur Erbringung von Gesundheitsdienstleistungen;
- b) Informationen über Zahlungen oder Berechtigungen zum Empfang medizinischer Dienstleistungen bezüglich der betreffenden Person;
- c) eine Nummer, ein Symbol oder ein Kennzeichen, die/das einer bestimmten Person zugeteilt wurde, um diese für medizinische Zwecke eindeutig zu identifizieren;
- d) jegliche Informationen über die bestimmte Person, die im Rahmen der Erbringung von medizinischen Dienstleistungen erhoben wurden;
- e) Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz abgeleitet wurden; und
- f) Identifizierung einer Person (z. B. eines Heilberufers) als Erbringer von Gesundheitsversorgung für die bestimmte Person.

ANMERKUNG Persönliche Gesundheitsinformationen schließen keine Informationen ein, die, entweder allein für sich oder in Kombination mit anderen Informationen, die für den Halter frei erhältlich sind, anonymisiert sind, d. h. die Identität der betroffenen Person, die Gegenstand der Informationen ist, kann aus den Informationen nicht abgeleitet werden.

3.10

behandelte Person

eine oder mehrere Personen, die terminlich eingeplant sind, eine Leistung des Gesundheitswesens zu erhalten, diese gerade erhalten oder diese bereits erhalten haben

[ISO/TS 18308:2004]

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-
Managementsysteme — Überblick und Terminologie*

DIN ISO/IEC 27002, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das
Informationssicherheits-Management*

Contents

Page

1	Scope	1
1.1	General	1
1.2	Scope exclusions	1
2	Normative references	2
3	Terms and definitions	2
4	Structure of this standard.....	4
5	Information security policies	5
5.1	Management direction for information security.....	5
5.1.1	Policies for information security	5
5.1.2	Review of the policies for information security	7
6	Organization of information security	8
6.1	Internal organization	8
6.1.1	Information security roles and responsibilities	8
6.1.2	Segregation of duties.....	10
6.1.3	Contact with authorities.....	10
6.1.4	Contact with special interest groups	10
6.1.5	Information security in project management	11
6.2	Mobile devices and teleworking	11
6.2.1	Mobile device policy.....	11
6.2.2	Teleworking.....	13
7	Human resource security	14
7.1	Prior to employment.....	14
7.1.1	Screening	14
7.1.2	Terms and conditions of employment	15
7.2	During employment.....	16
7.2.1	Management responsibilities	16
7.2.2	Information security awareness, education and training.....	17
7.2.3	Disciplinary process	18
7.3	Termination and change of employment	19
7.3.1	Termination or change of employment responsibilities	19
8	Asset management.....	19
8.1	Responsibility for assets	19
8.1.1	Inventory of assets	19
8.1.2	Ownership of assets	20
8.1.3	Acceptable use of assets.....	21
8.1.4	Return of assets	21
8.2	Information classification	21
8.2.1	Classification of information.....	21
8.2.2	Labelling of information.....	23
8.2.3	Handling of assets.....	23
8.3	Media handling	24
8.3.1	Management of removable media.....	24
8.3.2	Disposal of media.....	25
8.3.3	Physical media transfer	25
9	Access control	26
9.1	Business requirements of access control	26
9.1.1	Access control policy	26
9.1.2	Access to networks and network services	28
9.2	User access management	28
9.2.1	User registration and de-registration	28

9.2.2	User access provisioning	29
9.2.3	Management of privileged access rights	30
9.2.4	Management of secret authentication information of users	31
9.2.5	Review of user access rights	32
9.2.6	Removal or adjustment of access rights	32
9.3	User responsibilities	33
9.3.1	Use of secret authentication information.....	33
9.4	System and application access control	34
9.4.1	Information access restriction	34
9.4.2	Secure log-on procedures	35
9.4.3	Password management system	35
9.4.4	Use of privileged utility programs.....	36
9.4.5	Access control to program source code.....	37
10	Cryptography	37
10.1	Cryptographic controls	37
10.1.1	Policy on the use of cryptographic controls	37
10.1.2	Key management	38
11	Physical and environmental security	39
11.1	Secure areas.....	39
11.1.1	Physical security perimeter	40
11.1.2	Physical entry controls	41
11.1.3	Securing offices, rooms and facilities	41
11.1.4	Protecting against external and environmental threats	42
11.1.5	Working in secure areas	42
11.1.6	Delivery and loading areas	42
11.2	Equipment	43
11.2.1	Equipment siting and protection.....	43
11.2.2	Supporting utilities	44
11.2.3	Cabling security	44
11.2.4	Equipment maintenance	45
11.2.5	Removal of assets	45
11.2.6	Security of equipment and assets off-premises.....	46
11.2.7	Secure disposal or re-use of equipment	46
11.2.8	Unattended user equipment	47
11.2.9	Clear desk and clear screen policy	47
12	Operations security	48
12.1	Operational procedures and responsibilities	48
12.1.1	Documented operating procedures	48
12.1.2	Change management	49
12.1.3	Capacity management.....	49
12.1.4	Separation of development, testing and operational environments	50
12.2	Protection from malware.....	51
12.2.1	Controls against malware	51
12.3	Backup	52
12.3.1	Information backup.....	52
12.4	Logging and monitoring	53
12.4.1	Event logging	53
12.4.2	Protection of log information	54
12.4.3	Administrator and operator logs	56
12.4.4	Clock synchronisation	56
12.5	Control of operational software	57
12.5.1	Installation of software on operational systems	57
12.6	Technical vulnerability management.....	58
12.6.1	Management of technical vulnerabilities	58
12.6.2	Restrictions on software installation.....	59
12.7	Information systems audit considerations	59
12.7.1	Information systems audit controls.....	59
13	Communications security	60

13.1	Network security management	60
13.1.1	Network controls	60
13.1.2	Security of network services	60
13.1.3	Segregation in networks	61
13.2	Information transfer	61
13.2.1	Information transfer policies and procedures	61
13.2.2	Agreements on information transfer	63
13.2.3	Electronic messaging	63
13.2.4	Confidentiality or non-disclosure agreements	64
14	System acquisition, development and maintenance	65
14.1	Security requirements of information systems	65
14.1.1	Information security requirements analysis and specification	65
14.1.2	Securing application services on public networks	67
14.1.3	Protecting application services transactions	68
14.2	Security in development and support processes	69
14.2.1	Secure development policy	69
14.2.2	System change control procedures	69
14.2.3	Technical review of applications after operating platform changes	70
14.2.4	Restrictions on changes to software packages	71
14.2.5	Secure system engineering principles	71
14.2.6	Secure development environment	72
14.2.7	Outsourced development	72
14.2.8	System security testing	73
14.2.9	System acceptance testing	73
14.3	Test data	74
14.3.1	Protection of test data	74
15	Supplier relationships	74
15.1	Information security in supplier relationships	74
15.2	Test data	74
15.2.1	Information security policy for supplier relationships	74
15.2.2	Addressing security within supplier agreements	76
15.2.3	Information and communication technology supply chain	77
15.3	Supplier service delivery management	78
15.3.1	Monitoring and review of supplier services	78
15.3.2	Managing changes to supplier services	78
16	Information security incident management	79
16.1	Management of information security incidents and improvements	79
16.1.1	Responsibilities and procedures	79
16.1.2	Reporting information security events	80
16.1.3	Reporting information security weaknesses	81
16.1.4	Assessment of and decision on information security events	82
16.1.5	Response to information security incidents	82
16.1.6	Learning from information security incidents	83
16.1.7	Collection of evidence	83
17	Information security aspects of business continuity management	84
17.1	Information security continuity	84
17.1.1	Planning information security continuity	84
17.1.2	Implementing information security continuity	85
17.1.3	Verify, review and evaluate information security continuity	85
17.2	Redundancies	86
17.2.1	Availability of information processing facilities	86
18	Compliance	86
18.1	Compliance with legal and contractual requirements	86
18.1.1	Identification of applicable legislation and contractual requirements	86
18.1.2	Intellectual property rights	87
18.1.3	Protection of records	88
18.1.4	Privacy and protection of personally identifiable information	88

18.1.5	Regulation of cryptographic controls.....	90
18.2	Information security reviews	90
18.2.1	Independent review of information security	90
18.2.2	Compliance with security policies and standards	90
18.2.3	Technical compliance review	91
Annex A Threats to health information security (informative)		92
Annex B Practical action plan for implementing ISO/IEC 27002 in healthcare (informative)		96
B.1	Taxonomy of the 27001 and 27002 standards	96
B.2	Management commitment to implementing ISO/IEC 27002	96
B.3	Establishing, operating, maintaining and improving the ISMS	97
B.4	Planning: establishing the ISMS	97
B.4.1	Selecting and defining a compliance scope	97
B.4.2	Gap analysis.....	99
B.4.3	Establishing or enhancing a health information security forum	99
B.4.4	Assessing risks to health information.....	99
B.4.5	Risk management	101
B.4.6	Security improvement planning	102
B.4.7	Statement of applicability	102
B.4.8	ISMS document set.....	102
B.4.9	Potential for facilitation by the use of tools	103
B.4.10	Summary.....	104
B.5	Doing: implementing and operating the ISMS.....	104
B.6	Checking: monitoring and reviewing the ISMS	106
B.6.1	Need for on-going assurance	106
B.6.2	Compliance assessment.....	106
B.6.3	Summary.....	107
B.7	Acting: maintaining and improving the ISMS	107
Annex C Checklist for 27799 (informative)		109
C.1	Instructions for completing the checklist	109
Bibliography.....		112
Related standards in health information security		112
Other information security standards		113
Other standards		114

Foreword

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

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

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

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

ISO 27799 was prepared by Technical Committee ISO/TC 215, *Health informatics*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (ISO 27799:2008), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] 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 *Information technology — Security techniques — Code of practice for information security controls*¹ 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 must 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 must 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 guidance must 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. The present international standard (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.

¹ This guideline is consistent with the revised version of ISO/IEC 27002:2013.

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 confidentiality, measures must also be taken to maintain the integrity of data, if for no other reason than that it is possible to corrupt the integrity of access control data, audit trails, and other system data in ways that allow breaches in confidentiality to take place or to go unnoticed. In addition, patient safety depends upon maintaining the integrity of personal health information; failure to do this can also result in illness, injury or even death. Likewise, a high level of availability is an especially important attribute of health systems, where treatment is often time-critical. Indeed, disasters that could lead to outages in other, non-health related, IT systems may be the very times when the information contained in health systems is most critically needed. Moreover, denial of service attacks against networked systems are increasingly common.

The controls discussed in this standard are those identified as appropriate in healthcare to protect confidentiality, integrity and availability of personal health information and to ensure that access to such information can be audited and accounted for. These controls help to prevent errors in medical practice that might ensue from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained.

There are additional considerations that shape the goals of health information security. They include:

- a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care's right to privacy²;
- b) maintaining established privacy and security best practices in health informatics;
- c) maintaining individual and organizational accountability among health organizations and health professionals;
- d) supporting the implementation of systematic risk management within health organizations;
- e) meeting the security needs identified in common healthcare situations;
- f) reducing operating costs by facilitating the increased use of technology in a safe, secure, and well managed manner that supports – but does not constrain – current health activities;
- g) maintaining public trust in health organizations and the information systems these organizations rely upon;
- h) maintaining professional standards and ethics as established by health-related professional organizations (insofar as information security maintains the confidentiality and integrity of health information);
- i) operating electronic health information systems in an environment appropriately secured against threats; and
- j) facilitating interoperability among health systems, since health information increasingly flows among organizations and across jurisdictional boundaries (especially as such interoperability enhances the proper handling of health information to ensure its continued confidentiality, integrity and availability).

Relation to information governance,³ corporate governance and clinical governance

While health organizations may differ in their positions on clinical governance and corporate governance, the importance of integrating and attending to information governance ought to be beyond debate as a vital

² In addition to legal obligations, a wealth of information is available on ethical obligations relating to health information; e.g., the code of ethics of the World Health Organization. These ethical obligations may also, in certain circumstances, impact health information security policy.

³ Note that in some countries, information governance is referred to as information assurance.

support to both. As health organizations have become ever more critically dependent on information systems to support care delivery (e.g. by exploiting decision support technologies and trends towards 'evidence based' rather than 'experience based' healthcare), it has become evident that events in which losses of integrity, availability and confidentiality occur may have a significant clinical impact and that problems arising from such impacts will be seen to represent failures in the ethical and legal obligations inherent in a 'duty of care'.

All countries and jurisdictions will undoubtedly have case studies where such breaches have led to misdiagnoses, deaths, or protracted recoveries. Clinical governance frameworks need therefore to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other 'core' clinical management matters. This standard will assist those responsible for clinical governance in understanding the contribution made by effective information security strategies.

Health information to be protected

There are several types of information whose confidentiality, integrity and availability⁴ need to be protected:

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

The extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data (item 3 above) may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data (item 7 above) might not require high availability (frequent archiving with a retrieval time measured in hours rather than seconds might suffice in a given application) but its content might be highly confidential. Risk assessment can properly determine the level of effort needed to protect confidentiality, integrity and availability (see section ***). The results of regular risk assessment need to be fitted to the priorities and resources of the implementing organization.

Threats and vulnerabilities in health information security

Types of information security threats and vulnerabilities vary widely, as do their descriptions. While none are truly unique to healthcare, what *is* unique in healthcare is the array of factors to be considered when assessing threats and vulnerabilities.

By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded. In large health organizations, the sheer volume of people moving through operational areas is significant. These factors increase the vulnerability of systems to physical threats. The

⁴ Level of availability depends upon the uses to which the data will be put.

likelihood that such threats will occur may increase when emotional or mentally ill subjects of care or relatives are present.

The critical importance of correctly identifying subjects of care and correctly matching them to their health records leads health organizations to collect detailed identifying information. Regional or jurisdictional patient registries (i.e., registries of subjects of care) are sometimes the most comprehensive and up-to-date repositories of identifying information available in a jurisdiction. This identifying information is of great potential value to those who would use it to commit identity theft and so must be rigorously protected.

Many health organizations are chronically under-funded and their staff members are sometimes obliged to work under significant stress and with systems kept in service long after they ought to have been retired. These factors can increase the potential for certain types of threat and can exacerbate vulnerabilities. On the other hand, clinical care involves a range of professional, technical, administrative, ancillary and voluntary staff, many of whom see their work as a vocation. Their dedication and diversity of experience can often usefully reduce exposure to vulnerabilities. The high level of professional training received by many health professionals also sets healthcare apart from many other industrial sectors in reducing the incidence of insider threats.

The health environment, with its unique threats and vulnerabilities, should therefore be considered with special care. Annex A contains an informative list of the types of threat that need to be considered by health organizations when they assess risks to the confidentiality, integrity and availability of health information and to the integrity and availability of related information systems.

Who should read this standard?

This standard is intended for those responsible for overseeing health information security and for healthcare organizations and other custodians of health information seeking guidance on this topic, together with their security advisors, consultants, auditors, vendors and third-party service providers.

This standard's authors do not intend to write a primer on computer security, nor to restate what has already been written in ISO/IEC 27002 or in ISO/IEC 27001. There are many security requirements that are common to all computer-related systems, whether used in financial services, manufacturing, industrial control, or indeed in any other organized endeavour. A concerted effort has been made to focus on security requirements necessitated by the unique challenges of delivering electronic health information that supports the provision of care.

Benefits of using this standard

ISO/IEC 27002 is a broad and complex standard and its advice is not tailored specifically to healthcare. This standard (ISO/IEC 27799) allows for the implementation of 27002 within health environments in a consistent fashion and with particular attention to the unique challenges that the health sector poses. By following it, healthcare organizations help to ensure that the confidentiality and integrity of data in their care is maintained; that critical health information systems remain available; and that accountability for health information is upheld.

The adoption of this guidance by healthcare organizations both within and among jurisdictions will assist interoperability and enable the safe adoption of new collaborative technologies in the delivery of healthcare. Secure and privacy-protective information sharing can significantly improve healthcare outcomes.

As a result of implementing this guidance, healthcare organizations can expect to see the number and severity of their security incidents reduced, allowing resources to be redeployed to productive activities. IT security will thereby allow health resources to be deployed in a cost effective and productive manner. Indeed, research by the respected Information Security Forum and by market analysts has shown that good all-round security can have as much as a 2% positive effect upon organizations' results.

Finally, a consistent approach to IT security, understandable by all involved in healthcare, will improve staff morale and increase the trust of the public in the systems that maintain personal health information.

How to use this standard

Readers not already familiar with ISO/IEC 27002 are urged to read the introductory sections of that standard before continuing. Implementers of the present standard (27799) must first thoroughly read ISO/IEC 27002, as the text below will frequently refer the reader to the relevant sections of that standard. The present document cannot be fully understood without access to the full text of ISO/IEC 27002.

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in Annex B. No mandatory requirements are contained in this section. Instead, general advice and guidance are given on how best to proceed with implementation of 27002 in healthcare. The section is organized around a cycle of activities (plan/do/check/act) that are described in ISO/IEC 27001 and that, when followed, will lead to a robust implementation of an information security management system.

Readers seeking specific advice on the security control security control categories and clauses described in ISO/IEC 27002 will find it in the sections of the document with the same section number and title as is found in ISO/IEC 27002. This section leads the reader through each of the eleven security control clauses of the 27002 standard. Minimum requirements are stated where appropriate and, in some cases, normative guidelines are set out on the proper application of certain 27002 security controls to the protection of health information.

Once the 27002 standard has been put into place, effective ongoing management is considered essential if the benefits of the standard are to be maintained. Section 0 discusses compliance assessment and the requirements for ongoing information security management.

This standard concludes with four informative appendices. The first describes the general threats to health information. The second briefly describes other standards that can be applied to specific aspects of health information security. The third discusses the advantages of support tools as an aid to implementation. The fourth appendix lists related standards in health information security.

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

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

1.1 General

This standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 (Information Technology — Security techniques — Code of practice for information security controls) and is a companion to that standard.⁵

The present standard provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary so that they can be effectively used for managing health information security. By implementing this standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

This standard applies to health information in all its aspects; whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, via fax, over computer networks, or by post), as the information must always be appropriately protected.

This standard and ISO/IEC 27002 taken together define *what* is required in terms of information security in healthcare; they do not define *how* these requirements are to be met. That is to say, to the fullest extent possible, this standard is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that this standard describes.

As noted in the introduction, familiarity with ISO/IEC 27002 is indispensable to an understanding of this standard.

1.2 Scope exclusions

The following areas of information security are outside the scope of this standard:

- a) methodologies and statistical tests for effective anonymisation of personal health information;
- b) methodologies for pseudonymisation of personal health information (see Annex D for a brief description of an ISO technical specification that deals specifically with this topic);
- c) network quality of service and methods for measuring availability of networks used for health informatics; and
- d) data quality (as distinct from data integrity).

⁵ This guideline is consistent with the revised version of ISO/IEC 27002:2013.

2 Normative references

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

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, security terms and definitions given in ISO/IEC 27000 apply.

For the purposes of this document, health-informatics terms and definitions are as follows:

3.1

health informatics

scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks

[ISO 18307]

3.2

health information system

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

[ISO TR 20514]

3.3

healthcare

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

[European Parliament, 1998, as cited by WHO]

3.4

healthcare organization

generic term used to describe many types of organizations that provide healthcare services

[ISO 18307]

3.5

health professional

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

[ISO 17090-1]

3.6

healthcare provider

any person or organization who is involved in or associated with the delivery of health care to a client, or caring for client wellbeing

[ISO 27527]

3.7

identifiable person

one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[ISO 22587]

3.8

patient

subject of care (see below, section 3.1.9).

3.9

personal health information

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

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

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

3.10

subject of care

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

[ISO/TS 18308:2004]

4 Structure of this standard

This standard provides guidance on the 14 security control clauses, 35 main security categories, and 114 controls specified in ISO/IEC 27002. As with that standard, each clause defining security controls contains one or more main security categories. The order of the clauses and categories does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important – healthcare organizations applying this standard should identify controls applicable to their environment and business processes.

Each main security control category of ISO/IEC 27002 contains a control objective stating what is to be achieved and one or more controls that can be applied to achieve the control objective.

Readers of this standard are presumed to have access to the text of ISO/IEC 27002. Control descriptions in this standard are structured as follows:

Health-specific control

Defines the health-specific control statement, as stated in ISO/IEC 27002, to satisfy the control objective.

Health specific Implementation guidance

Provides more detailed information to support the implementation of the control in a healthcare delivery environment to meet the control objective when protecting the confidentiality, integrity and availability of personal health information. If there is no health-specific guidance provided, the text states “No additional guidance for information security management in health.”

Other health-specific information

Provides further health-specific information that may need to be considered, for example references to other standards. If there is no other information to be provided, this part is not shown.

NOTE TO READERS AND REVIEWERS:

In the following sections, the text in blue is taken verbatim for ISO/IEC 27002 and is included for your convenience during balloting, review and comment.

Some or most of this text in blue WILL BE REMOVED IN THE FINAL VERSION OF THIS STANDARD!

ISO copyright does not permit us to reproduce almost the entirety of 27002 within the body of this document. Please suggest text if there are any places where important points from the original text of 27002 need to be referred to explicitly in this document.

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

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

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

At the highest level, organizations should define an “information security policy” which is approved by management and which sets out the organization’s approach to managing its information security objectives.

Information security policies should address requirements created by:

- a) business strategy;
- b) regulations, legislation and contracts;
- c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

- a) definition of information security, objectives and principles to guide all activities relating to information security;
- b) assignment of general and specific responsibilities for information security management to defined roles;
- c) processes for handling deviations and exceptions.

At a lower level, the information security policy should be supported by topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics.

Examples of such policy topics include:

- a) access control (see Clause 9);

- b) information classification (and handling) (see 8.2);
- c) physical and environmental security (see Clause 11);
- d) end user oriented topics such as:
 - 1) acceptable use of assets (see 8.1.3);
 - 2) clear desk and clear screen (see 11.2.9);
 - 3) information transfer (see 13.2.1);
 - 4) mobile devices and teleworking (see 6.2);
 - 5) restrictions on software installations and use (see 12.6.2);
- e) backup (see 12.3);
- f) information transfer (see 13.2);
- g) protection from malware (see 12.2);
- h) management of technical vulnerabilities (see 12.6.1);
- i) cryptographic controls (see Clause 10);
- j) communications security (see Clause 13);
- k) privacy and protection of personally identifiable information (see 18.1.4);
- l) supplier relationships (see Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an “information security awareness, education and training programme” (see 7.2.2).

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 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).

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 documents 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:

- 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;
- 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.

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

The need for internal policies for information security varies across organizations. Internal policies are especially useful in larger and more complex organizations where those defining and approving the expected levels of control are segregated from those implementing the controls or in situations where a policy applies to many different people or functions in the organization. Policies for information security can be issued in a single “information security policy” document or as a set of individual but related documents.

If any of the information security policies are distributed outside the organization, care should be taken not to disclose confidential information.

Some organizations use other terms for these policy documents, such as “Standards”, “Directives” or “Rules”.

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

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

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The review of policies for information security should take the results of management reviews into account.

Management approval for a revised policy should be obtained.

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 determine the effectiveness of information security..*

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

All information security responsibilities should be defined and allocated.

Health-specific control

[from 27799:2008, 7.3.2.1]:

Organizations processing personal health information **shall**:

- a) clearly define and assign information security responsibilities;
- b) have an 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 0.

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

Allocation of information security responsibilities should be done in accordance with the information security policies (see 5.1.1). Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and in particular for acceptance of residual risks should be defined. These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes should be defined.

Individuals with allocated information security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be stated. In particular the following should take place:

- a) the assets and information security processes should be identified and defined;
- b) the entity responsible for each asset or information security process should be assigned and the details of this responsibility should be documented (see 8.1.2);
- c) authorization levels should be defined and documented;
- d) to be able to fulfil responsibilities in the information security area the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments;
- e) coordination and oversight of information security aspects of supplier relationships should be identified and documented.

Health-specific implementation guidance

[from 27799:2008, 7.3.2.1]

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 **0**. 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 **0**, 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

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

6.1.2 Segregation of duties

Control

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information **should** ensure that the IT systems employed contain application functionalities that enforce the approval of clinical processes by different role holders, where this is required.

Implementation guidance

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Other information

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner (e.g. if it is suspected that laws may have been broken).

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

Organizations under attack from the Internet may need authorities to take action against the attack source.

Maintaining such contacts may be a requirement to support information security incident management (see Clause 16) or the business continuity and contingency planning process (see Clause 17). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be implemented by the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment).

6.1.4 Contact with special interest groups

Control

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance

Membership in special interest groups or forums should be considered as a means to:

- a) improve knowledge about best practices and stay up to date with relevant security information;
- b) ensure the understanding of the information security environment is current and complete;
- c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
- d) gain access to specialist information security advice;
- e) share and exchange information about new technologies, products, threats or vulnerabilities;

- f) provide suitable liaison points when dealing with information security incidents (see Clause 16).

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of confidential information.

6.1.5 Information security in project management

NEW Control

Information security should be addressed in project management, regardless of the type of the project.

Implementation guidance

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g. a project for a core business process, IT, facility management and other supporting processes. The project management methods in use should require that:

- a) information security objectives are included in project objectives;
- b) an information security risk assessment is conducted at an early stage of the project to identify necessary controls;
- c) information security is part of all phases of the applied project methodology.

Information security implications should be addressed and reviewed regularly in all projects. Responsibilities for information security should be defined and allocated to specified roles defined in the project management methods.

Health-specific control

Healthcare project management should consider patient safety as a project risk in any project involving the processing of personal health information.

Health-specific implementation guidance

Patient safety is a critical component of any project risk assessment in a project involving the processing of personal health information. Risks to patient safety need to be carefully analysed and explicitly addressed.

Other health-specific information.

ISO/TR 17791:2013 *Health informatics -- Guidance on standards for enabling safety in health software* provides a review of relevant patient safety related standards.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;

- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see Clause 10) and enforcing use of secret authentication information (see 9.2.4).

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

- a) separation of private and business use of the devices, including using software to support such separation and protect business data on a private device;
- b) providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information **should**:

- i) specifically assess the risks involved in healthcare mobile computing;
- j) prepare policy on the precautions to be taken when using mobile computing devices, including wireless devices;
- k) require their mobile users to follow this policy.

As noted in ISO/IEC 27002, mobile network wireless connections, while similar to those of wired networks, have some important differences from an information security point of view. Some wireless encryption protocols such as Wired Equivalent Privacy (WEP) are still in use despite known weaknesses that render them largely ineffective. Moreover, information stored on mobile devices may not always be backed up (e.g. because of limited network bandwidth or because the devices are not connected at the times when backups are scheduled).

Other information

Mobile device wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are:

- a) some wireless security protocols are immature and have known weaknesses;
- b) information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.

Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organization's premises.

6.2.2 Teleworking

Control

A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.

Implementation guidance

Organizations allowing teleworking activities should issue a policy that defines the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

- a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;
- b) the proposed physical teleworking environment;
- c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system;
- d) the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment;
- e) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;
- f) the use of home networks and requirements or restrictions on the configuration of wireless network services;
- g) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
- h) access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation;
- i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;
- j) malware protection and firewall requirements.

The guidelines and arrangements to be considered should include:

- a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;
- b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;
- c) the provision of suitable communication equipment, including methods for securing remote access;
- d) physical security;
- e) rules and guidance on family and visitor access to equipment and information;

- f) the provision of hardware and software support and maintenance;
- g) the provision of insurance;
- h) the procedures for backup and business continuity;
- i) audit and security monitoring;
- j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information **should**:

- l) prepare policy on the precautions to be taken when teleworking;
- m) ensure that teleworking users of health information systems abide by this policy.

Some national jurisdictions (e.g. in Germany) have already placed restrictions on teleworking by health professionals.

It is important to consider that in healthcare, teleworking can cross jurisdictional borders and can even take place on board planes and ships situated beyond any national jurisdiction. Physicians already routinely e-mail medical images, etc. across boundaries to obtain specialist opinions. International teams involved in disaster relief may, in future, rely upon health information systems in jurisdictions other than their home jurisdiction. The legal and ethical considerations of doing this need to be taken into account in the design and deployment of health information systems (especially national systems) that may be used in this manner.

Other information

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible workplace”, “remote work” and “virtual work” environments.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Health-specific controls

All organizations whose staff, contractors or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job application.

Background verification checks on all candidates for employment should include a verification of applicable health professional qualifications where such qualifications are professionally accredited (e.g., physicians, nurses, etc.)

When an individual is hired for a specific information security role, organizations should make sure the candidate:

- a) has the necessary competence to perform the security role;

b) can be trusted to take the role, especially if the role is critical for the organization

Implementation guidance

Verification should take into account all relevant privacy, protection of personally identifiable information and employment based legislation, and should, where permitted, include the following:

- a) availability of satisfactory character references, e.g. one business and one personal;
- b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;
- c) confirmation of claimed academic and professional qualifications;
- d) independent identity verification (passport or similar document);
- e) more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organizations should make sure the candidate:

- f) has the necessary competence to perform the security role;
- g) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and, in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organization and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, all organizations whose staff, contractors or volunteers process (or are expected to process) personal health information **should, as a minimum**, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.

7.1.2 Terms and conditions of employment

Control

As part of their contractual obligation, employees should agree and sign the terms and conditions.

Health-specific control

[from 27799:2008, 7.5.1.1]

In addition to the control given by ISO/IEC 27002, all organizations whose staff members are involved in processing personal health information **should** document such involvement in relevant job descriptions. Security roles and responsibilities, as laid down in the organization's information security policy, **should** also be documented in relevant job descriptions.

Special attention needs to be placed upon the roles and responsibilities of temporary or short-term staff such as locums, students, interns, etc.

Implementation guidance

The contractual obligations for employees or contractors should reflect the organization's policies for information security in addition to clarifying and stating:

- a) that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities (see 13.2.4);

- b) the employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see 18.1.2 and 18.1.4);
- c) responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by the employee or contractor (see Clause 8);
- d) responsibilities of the employee or contractor for the handling of information received from other companies or external parties;
- e) actions to be taken if the employee or contractor disregards the organization's security requirements (see 7.2.3).

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organization should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 7.3).

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information **should** ensure that employees or contractors have a duty to report breaches of health information security or patient privacy.

It is important to know how and where to contact health professional staff, although, as some medical staff move on a regular basis, address details may have a limited value. Health organizations should therefore give consideration to the collection of a reasonable number of references and to undertaking other forms of check, e.g. by professional bodies and academic institutions.

Wherever possible, criminal background checks **should** be undertaken. See also 9.1.1.

Other information

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. An external party, with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

Control

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

Implementation guidance

Management responsibilities should include ensuring that employees and contractors:

- a) are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;
- b) are provided with guidelines to state information security expectations of their role within the organization;
- c) are motivated to fulfil the information security policies of the organization;

- d) achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see 7.2.2);
- e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;
- f) continue to have the appropriate skills and qualifications and are educated on a regular basis;
- g) are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the special emphasis that needs to be placed on the concerns of subjects of care who do not wish their personal health information to be accessed by health workers who are neighbours, colleagues or relatives. Such concerns often make up a large percentage of complaints from those with fears about the confidentiality of their personal health information. Likewise, staff members often do not wish to be placed unnecessarily in the position of reviewing information about friends, relatives or neighbours. Effective management of health information systems needs to address these concerns.

Other information

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organization. For example, poor management can lead to information security being neglected or potential misuse of the organization's assets.

7.2.2 Information security awareness, education and training

Control

All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, all organizations processing personal health information **shall** ensure that information security education and training are provided on induction and, that regular updates in organizational security policies and procedures are provided to all employees and, where relevant, third-party contractors, researchers, students and volunteers who process personal health information.

Disciplinary processes with respect to breaches of information security should follow procedures that are reflected in policy and thus known to the subject(s) of the disciplinary process. In addition to complying with applicable laws, such processes should comply with the agreements reached between health professionals and health professional bodies.

Implementation guidance

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged.

An information security awareness programme should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programme should be planned taking into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new

employees and contractors. The awareness programme should also be updated regularly so it stays in line with organizational policies and procedures, and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects such as:

- a) stating management's commitment to information security throughout the organization;
- b) the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements;
- c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties;
- d) basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks);
- e) contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organization should develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The programme should consider different forms of education and training, e.g. lectures or self-studies.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organization of their own behaviour.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

7.2.3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred (see 16.1.7).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organization's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations' disciplinary processes with respect to breaches of information security **should** follow procedures that are reflected in policy and thus

known to the subject(s) of the disciplinary process. In addition to complying with applicable laws, such processes **should** comply with the agreements reached between health professionals and health professional bodies.

Other information

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.
--

7.3.1 Termination or change of employment responsibilities

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.

Implementation guidance

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 13.2.4) and the terms and conditions of employment (see 7.1.2) continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment (see 7.1.2).

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Health-specific implementation guidance

It is important to note that in healthcare, many types of staff, e.g. doctors and nurses, commonly progress through training programmes and other "rotations" where their access rights can change fundamentally. To ensure the termination of previous rights that are no longer required for their role, such changes of employment should be initially processed in the same way as for individuals who are leaving the organization's employ.

Other information

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.
--

8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

Health-specific control

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information **should**:

- n) account for health information assets (i.e. maintain an inventory of such assets);
- o) have a designated custodian of these health information assets (see 8.1.2);

- p) have rules for acceptable use of these assets that are identified, documented, and implemented (see 8.1.3).

Implementation guidance

An organization should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset should be assigned (see 8.1.2) and the classification should be identified (see 8.2).

Health-specific implementation guidance

Organizations processing health information **should** have rules for maintaining the currency of information assets (e.g. the currency of a drug database) and the integrity of these assets (e.g. the functional integrity of medical devices that record or report data).

Medical devices that record or report data may require special security considerations in relation to the environment in which they operate and to the electromagnetic emissions that occur during their operation. Such devices **should** be uniquely identified.

Other information

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005^[11] provides examples of assets that might need to be considered by the organization when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005^[11]).

8.1.2 Ownership of assets

Control

Assets maintained in the inventory should be owned.

Implementation guidance

Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

- a) ensure that assets are inventoried;
- b) ensure that assets are appropriately classified and protected;
- c) define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;
- d) ensure proper handling when the asset is deleted or destroyed.

Health-specific implementation guidance

It is important to note that while many information assets can be owned by in the conventional sense used in 27002, the notion of ownership of personal health information is fraught with legal, ethical and policy-based issues. In many jurisdictions, individuals may have rights with respect to their own personal health information that limit or transcend any straightforward notion of "ownership" of this information by a healthcare organization or a health professional. Rather, healthcare organizations and health professionals are often viewed in relation to personal health information as custodians or trustees.

Other information

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

8.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

Implementation guidance

Employees and external party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

Health-specific implementation guidance

No additional guidance for information security management in health.

8.1.4 Return of assets

Control

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, all employees and contractors **shall** return all personal health information in their possession upon termination of employment.

Implementation guidance

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see 11.2.7).

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period of termination, the organization should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information **should** uniformly classify such data as confidential.

Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, as well as legal requirements. Assets other than information can also be classified in conformance with classification of information which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information assets should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered. The scheme should be aligned to the access control policy (see 9.1.1).

Each level should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection.

Classification should be included in the organization's processes, and be consistent and coherent across the organization. Results of classification should indicate value of assets depending on their sensitivity and criticality to the organization, e.g. in terms of confidentiality, integrity and availability. Results of classification should be updated in accordance with changes of their value, sensitivity and criticality through their life-cycle.

Health-specific implementation guidance

Determining levels of protection for information assets in healthcare is complex and comparisons with government or military data classifications can be misleading. The following are important characteristics of information assets within healthcare.

- a) The confidentiality of personal health information is often largely subjective, rather than objective. In other words, ultimately, only the data subject (i.e. the subject of care) can make a proper determination of the relative confidentiality of various fields or groupings of data. For example, a person escaping from an abusive relationship may consider his or her new address and phone number to be much more confidential than clinical data about setting his or her broken arm.
- q) The confidentiality of personal health information is context-dependent. For example, the name and address of a subject of care in a list of admissions to a hospital's emergency department may not be considered especially confidential by that individual, yet the same name and address in a list of admissions to a clinic treating sexual impotence may be considered highly confidential by the individual.
- r) The confidentiality of personal health information can shift over the lifetime of an individual's health record. For example, changing societal attitudes over the last 20 years have resulted in many subjects of care no longer considering their sexual orientation to be confidential. Conversely, attitudes toward drug and alcohol dependency have caused some subjects of care to consider addiction counselling data to be, if anything, even more confidential today than such data would have been considered 20 years ago.

Because one cannot predict the sensitivity of a given element of personal health information through all its uses and all the phases of its life cycle, all personal health information **should** be subject to suitably careful protection at all times. Note that while all personal health information should be uniformly classified as confidential, practical considerations may necessitate identifying the records of subjects of care, who may be at elevated risk of access by those who do not have a need to know. Such individuals include employees of the organization itself (especially if their condition is one eliciting emotional behaviours), heads of government, celebrities, politicians, newsmakers and members of groups facing especially high risks (e.g. those with sexually transmitted diseases, or those whose personal health information contains information about genetic predisposition to serious illness). The records of such individuals may need to be specially tagged so that access can be closely monitored. However, great care must be exercised in implementing such schemes as this tagging can exacerbate the very problem it is designed to avoid, i.e. it can draw attention to the particular data items tagged. It is also important to emphasise that while certain subjects of care may be at elevated risk, their personal health information is not innately more confidential than that of other subjects of care. *All* personal health information is confidential and should be treated accordingly. See also the discussion in 7.2.1.

Identifying and (where appropriate) protectively labelling information assets as confidential can be an important tool in staff training and in policy compliance. This works best when the classification acts as an indicator of required information handling practices. The classification may also be an important component of data protection agreements among jurisdictions and with third-party organizations and their staff. The identification and labelling of information assets is also an essential component of ISO/IEC 27002.

In addition to the traditional classification of data on the basis of its sensitivity to disclosure, the criticality of information also needs to be classified, i.e. the extent to which the availability and integrity of the information are essential for the ongoing provision of healthcare. Time factors involved in clinical processes often play a crucial role in determining the availability requirements for personal health information. Classification in respect of availability, integrity, and criticality also needs to be applied to processes, IT devices, software, locations and personnel. Criticality **should** be identified through a risk assessment.

Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or on the contrary under-classification can endanger the achievement of business objectives.

An example of an information confidentiality classification scheme could be based on four levels as follows:

- a) disclosure causes no harm;
- b) disclosure causes minor embarrassment or minor operational inconvenience;
- c) disclosure has a significant short term impact on operations or tactical objectives;
- d) disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk.

8.2.2 Labelling of information

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Health-specific control

All health information systems processing personal health information **should** inform users of the confidentiality of personal health information accessible from the system (e.g. at start-up or log-in) and **should** label hardcopy output as confidential when it contains personal health information.

"Implementation guidance"

Procedures for information labelling need to cover information and its related assets in physical and electronic formats. The labelling should reflect the classification scheme established in 8.2.1. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of media. The procedures can define cases where labelling is omitted, e.g. labelling of non-confidential information to reduce workloads. Employees and contractors should be made aware of labelling procedures.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Health-specific implementation guidance

Not all health information is confidential and not all health information systems provide users with access to personal health information. Users of health information systems need to know when the data they are accessing contains personal health information.

Other information

Labelling of classified information is a key requirement for information sharing arrangements. Physical labels and metadata are a common form of labelling.

Labelling of information and its related assets can sometimes have negative effects. Classified assets are easier to identify and accordingly to steal by insiders or external attackers.

8.2.3 Handling of assets

NEW Control