INTERNATIONAL STANDARD

ISO 27799

Second edition
2016-07-01

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

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

Reference number
ISO 27799:2016(E)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

Foreword

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

Objectives

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

confidentiality, measures is 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 International 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. These includes the following:

a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care is right to privacy;[1)]

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;

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,[2)] 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 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

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

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

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 International 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 availability[3)] needs to be protected by

a) personal health information,

b) pseudonymized data derived from personal health information through some methodology for pseudonymous identification,

c) statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data,

d) clinical/medical knowledge not related to any specific 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 c) above] may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data [item g) 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 B.4.4). 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 likelihood that such threats will occur may increase when emotional or mentally ill subjects of care or relatives are present.

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

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 should 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 International Standard?

This International 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 International Standards 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 International Standard

ISO/IEC 27002 is a broad and complex International Standard and its advice is not tailored specifically to healthcare. ISO 27799 allows for the implementation of ISO/IEC 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 International Standard by healthcare organizations both within and among jurisdictions will assist interoperation 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 International Standard, 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 International Standard

Readers not already familiar with ISO/IEC 27002 are urged to read the introductory clauses of that standard before continuing. The implementers of ISO 27799 is to read first thoroughly ISO/IEC 27002, as the text below will frequently refer the reader to the relevant clauses of that standard. The present International Standard 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 clause. Instead, general advice and guidance are given on how best to proceed with implementation of ISO/IEC 27002 in healthcare. The clause 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 clauses of this International Standard with the same clause number and title as is found in ISO/IEC 27002. This clause leads the reader through each of the eleven security control clauses of the ISO/IEC 27002. Minimum requirements are stated where appropriate and, in some cases, normative guidelines are set out on the proper application of certain ISO/IEC 27002 security controls to the protection of health information.

Once ISO/IEC 27002 has been put into place, the ongoing management is considered essential if the benefits of the International Standard are to be maintained. Clause 18 discusses compliance assessment and the requirements for ongoing information security management. Annex C contains a self-assessment matrix with regard to compliance.

This International Standard concludes with four informative appendices.

Annex A describes the general threats to health information. Annex B briefly describes a practical action plan for implementing complementary information security related International Standards. Annex C provides a checklist for compliance to ISO 27799. Clause 2 lists the standards that are cited in a normative way; the Bibliography lists other related standards in health information security.

Health informatics — Information security 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).

This International Standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.[4)]

This International 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 International 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 International 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, through fax, over computer networks, or by post), as the information is always be appropriately protected.

This International 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 International 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, International 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 International Standard describes.

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

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

a) methodologies and statistical tests for effective anonymization of personal health information;

b) methodologies for pseudonymization of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic);

c) network quality of service and methods for measuring availability of networks used for health informatics;

d) data quality (as distinct from data integrity).

4) This International Standard is consistent with the revised version of ISO/IEC 27002.

国际标准

ISO 27799

第二版 2016 年
7 月 1 日

健康信息学-采用ISO/IEC 27002标准的健康信息安全管理

健康信息安全——运用 ISO/IEC 27002 进行健康信息安全的管理

Reference number ISO 27799:2016(E)

国际标准化组织

目录

前言

国际标准化组织（ISO）是由各国标准化机构（ISO 成员机构）组成的世界性联合组织。国际标准的制定工作通常由 ISO 技术委员会负责。凡对已设立技术委员会的某一主题感兴趣的成员机构均有权在该委员会中派代表。与 ISO 保持联络的国际组织（政府组织和非政府组织）也参与其工作。ISO 与国际电工委员会（IEC）在所有电工标准化事务上密切合作。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有详细说明。尤其应注意不同类型的 ISO 文件所需的不同批准标准。本文件是依据 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives）。

请注意，本文件中的某些内容可能受专利权保护。国际标准化组织（ISO）不承担识别任何此类专利权的责任。在文件编制过程中所识别出的任何专利权详情将在引言部分和/或国际标准化组织收到的专利声明清单中列出（见 www.iso.org/patents）。

本文件中使用的任何商标名称均为方便用户而提供，不构成任何背书。

有关符合性评定中 ISO 专用术语和表达的含义的解释，以及 ISO 在技术性贸易壁垒（TBT）方面遵循世贸组织原则的信息，请访问以下网址：前言 补充信息

负责本文件的委员会是国际标准化组织/技术委员会 215，即健康信息学技术委员会。

本第二版废止并取代了第一版（ISO 27799:2008），并对其技术内容进行了修订。

引言

本国际标准为医疗保健组织及其他个人健康信息保管者提供了如何最佳保护此类信息的保密性、完整性和可用性的指导。它基于并扩展了 ISO/IEC 27002:2013 中的一般性指导，针对医疗行业的特殊信息安全管理需求及其独特的运营环境进行了阐述。虽然个人信息的保护和安全对所有个人、企业、机构和政府都很重要，但医疗行业有其特殊要求，必须满足这些要求以确保个人健康信息的保密性、完整性、可审计性和可用性。许多人认为这类信息是所有个人信息中最保密的。保护这种保密性对于维护患者隐私至关重要。健康信息的完整性必须得到保护，以确保患者安全，而保护的一个重要组成部分是确保信息的整个生命周期都可完全审计。健康信息的可用性对于有效的医疗保健服务也至关重要。健康信息学系统必须能够满足独特的需求，以在自然灾害、系统故障和拒绝服务攻击面前保持正常运行。因此，保护健康信息的保密性、完整性和可用性需要具备卫生部门的专业知识。

无论规模大小、所处位置以及服务提供模式如何，所有医疗保健机构都需要采取严格的控制措施来保护委托给它们的健康信息。然而，许多医疗专业人员作为独立的医疗服务提供者或在小型诊所工作，这些诊所缺乏专门的信息技术资源来管理信息安全。因此，医疗保健机构需要有关此类控制措施的选择和实施的清晰、简洁且针对医疗保健行业的指导。本国际标准应适用于医疗保健领域中各种规模、位置和服务提供模式。最后，随着医疗专业人员之间个人健康信息的电子交换日益增多（包括无线和互联网服务的使用），在医疗保健领域采用通用的信息安全管理参考标准显然具有明显的好处。

ISO/IEC 27002 已在澳大利亚、加拿大、法国、荷兰、新西兰、南非、英国等国家和地区通过国家或地区指南广泛用于卫生信息学 IT 安全管理。ISO 27799 借鉴了这些国家在处理个人健康信息安全方面的经验，旨在作为 ISO/IEC 27002 的配套文件。它并非要取代 ISO/IEC 27000 系列标准，而是对这些更通用的标准的补充。

ISO 27799 将 ISO/IEC 27002 标准应用于医疗保健领域，同时谨慎考虑了为保护个人健康信息而适当应用安全控制措施的相关事宜。在某些情况下，这些考虑使得作者得出结论，认为若要充分保护个人健康信息，应用 ISO/IEC 27002 中的某些控制目标是必不可少的。因此，ISO 27799 对 ISO/IEC 27002 中规定的某些安全控制措施的应用施加了限制。

ISO/IEC 27002 中描述的所有安全控制目标都适用于卫生信息学，但其中一些控制措施需要进一步解释，说明如何才能最好地用于保护卫生信息的保密性、完整性和可用性。此外，还有卫生部门特有的其他要求。本国际标准以负责卫生信息安全的人员能够轻松理解并采用的格式提供了额外的指导。

在医疗保健领域，一个组织（比如一家医院）有可能通过 ISO/IEC 27001 认证，而无需通过或甚至无需承认 ISO 27799 认证。然而，人们希望随着医疗保健机构努力提高个人健康信息的安全性，作为医疗保健领域更严格标准的 ISO 27799 的符合性也能得到广泛采用。

目标

保持信息的保密性、可用性和完整性（包括真实性、可问责性和可审计性）是信息安全的总体目标。在医疗保健领域，患者隐私取决于个人健康信息的保密性。为了保持

保密性方面，还应采取措施来维护数据的完整性，原因在于访问控制数据、审计追踪以及其他系统数据的完整性有可能遭到破坏，从而导致保密性被侵犯或这种侵犯未被察觉。此外，患者安全取决于个人健康信息的完整性，若不能保证这一点，可能会导致疾病、受伤甚至死亡。同样，高可用性是医疗系统的一个特别重要的属性，因为医疗救治往往时间紧迫。实际上，在可能导致其他非医疗相关 IT 系统中断的灾难期间，医疗系统中所包含的信息可能最为关键。此外，针对联网系统的拒绝服务攻击也日益常见。

本国际标准中所讨论的控制措施是那些在医疗保健领域被认为适当的措施，旨在保护个人健康信息的保密性、完整性和可用性，并确保对这些信息的访问能够被审计和记录。这些控制措施有助于防止因未能保持健康信息的完整性而导致的医疗实践中的错误。此外，它们还有助于确保医疗服务的连续性。

还有其他一些因素影响着健康信息安全的目标。这些因素包括以下几点：

a) 遵守适用的数据保护法律法规中规定的立法义务，保护受照护者享有隐私权；

b) 在卫生信息学领域保持既定的隐私和安全最佳实践；

C 在卫生组织和卫生专业人员中保持个人和组织的责任制；

d) 支持在卫生组织内部实施系统性风险管理；

e) 满足常见医疗保健场景中所确定的安全需求；

f)通过以安全、可靠且管理良好的方式促进技术的更多使用，从而降低运营成本，同时支持但不阻碍当前的卫生活动

g) 维护公众对卫生组织及其所依赖的信息系统的信任；

h) 遵守由卫生相关专业组织所确立的专业标准和道德规范（在信息安全维护健康信息的保密性和完整性方面）；

在适当防范威胁的环境中操作电子健康信息系统；

鉴于健康信息在各组织之间以及跨越司法管辖区的流动日益频繁（尤其是这种互操作性有助于妥善处理健康信息，以确保其持续的保密性、完整性和可用性），促进卫生系统之间的互操作性至关重要。

与信息治理、2）公司治理和临床治理的关系

尽管各卫生组织在临床治理和公司治理方面的立场可能有所不同，但信息治理的重要性应当毋庸置疑，它是对这两者的有力支撑。随着卫生组织越来越依赖信息系统来支持医疗服务的提供（例如通过利用决策支持技术以及从“经验驱动”向“证据驱动”的医疗保健转变），这一点已变得显而易见。

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

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

发生完整性、可用性和保密性受损的事件可能会产生重大的临床影响，由此产生的问题将被视为未能履行“注意义务”所固有的伦理和法律义务。

所有国家和地区无疑都有这样的案例研究，即此类违规行为导致了误诊、死亡或长期康复。因此，临床治理框架需要将有效的信息安全风险管理与护理治疗计划、感染管理策略和其他“核心”临床管理事项同等看待。本国际标准将有助于负责临床治理的人员了解有效的信息安全策略所做出的贡献。

需要保护的健康信息

有几种类型的信息，其保密性、完整性和可用性需要受到保护。

a) 个人健康信息

b) 通过某种假名识别方法从个人健康信息中得出的假名化数据，

C　统计和研究数据，包括通过去除个人身份识别信息从个人健康信息中得出的匿名数据，

d) 与任何特定护理主题无关的临床/医学知识，包括临床决策支持数据（例如药物不良反应数据）

e) 关于卫生专业人员、员工和志愿者的数据，

f)与公共卫生监测相关的信息

g)由健康信息系统生成的包含个人健康信息或从个人健康信息派生的假名数据，或包含有关用户对个人健康信息操作的数据的审计追踪数据，以及

h) 包括访问控制数据和其他与安全相关的系统配置数据在内的卫生信息系统安全数据。

需要保护的保密性、完整性和可用性的程度取决于信息的性质、其用途以及所面临的风险。例如，上述 c) 项中的统计数据可能并不需要保密，但保护其完整性可能非常重要。同样，审计追踪数据（上述 g) 项）可能不需要很高的可用性（在特定的应用中，定期存档且检索时间以小时而非秒来衡量可能就足够了），但其内容可能高度机密。风险评估能够恰当地确定保护保密性、完整性和可用性所需的努力程度（见 B.4.4）。定期风险评估的结果需要与实施组织的优先事项和资源相适应。

卫生信息安全中的威胁与漏洞

信息安全威胁和漏洞的类型多种多样，其描述方式也各不相同。虽然没有哪一种威胁或漏洞是医疗保健行业独有的，但在评估威胁和漏洞时，医疗保健行业所要考虑的因素却是独一无二的。

就其本质而言，卫生机构的运作环境决定了不可能完全将访客和公众隔绝在外。在大型卫生机构中，通过运营区域的人员数量相当庞大。这些因素增加了系统遭受物理威胁的脆弱性。当存在情绪不稳定或精神失常的患者或其亲属时，此类威胁发生的可能性可能会增加。

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

正确识别护理对象并将其与健康记录正确匹配至关重要，这促使医疗机构收集详细的识别信息。在某些地区或司法管辖区，患者登记处（即护理对象登记处）有时是该地区最全面、最及时的识别信息库。这些识别信息对于那些企图利用其实施身份盗窃的人来说具有极大的潜在价值，因此必须严格加以保护。

许多卫生组织长期资金不足，其工作人员有时不得不在巨大压力下工作，而且一些系统在早就应该淘汰的情况下仍被继续使用。这些因素可能会增加某些类型威胁的可能性，并加剧脆弱性。另一方面，临床护理涉及专业人员、技术人员、行政人员、辅助人员和志愿者等各类人员，其中许多人将工作视为一种使命。他们的奉献精神和丰富多样的经验往往能够有效降低脆弱性。许多卫生专业人员接受的高水平专业培训也使医疗保健行业在减少内部威胁方面有别于许多其他工业部门。

因此，对于健康环境所具有的独特威胁和脆弱性，应当予以特别关注。附录 A 列出了一份详尽的清单，其中包含健康组织在评估健康信息以及相关信息系统在保密性、完整性和可用性方面所面临的风险时需要考虑的威胁类型。

谁应阅读本国际标准?

本国际标准旨在为负责监督健康信息安全的人员、寻求有关此主题指导的医疗保健组织及其他健康信息保管方、其安全顾问、咨询师、审计员、供应商和第三方服务提供商提供参考。

本国际标准的作者无意撰写计算机安全入门读物，也不打算重复 ISO/IEC 27002 或 ISO/IEC 27001 中已有的内容。所有与计算机相关的系统，无论用于金融服务、制造业、工业控制，还是其他任何有组织的活动，都存在许多共同的安全要求。本标准力求重点关注提供电子健康信息以支持医疗护理过程中所面临的独特挑战而产生的安全要求。

采用本国际标准的好处

ISO/IEC 27002 是一项广泛而复杂的国际标准，其建议并非专门针对医疗保健领域。ISO 27799 则允许在医疗环境中以一致的方式实施 ISO/IEC 27002，并特别关注医疗行业所面临的独特挑战。遵循该标准，医疗保健机构有助于确保其照管下的数据的保密性和完整性得以维持，关键的医疗信息系统保持可用，并且对医疗信息的责任得以落实。

各辖区内的医疗保健组织以及各辖区之间采用本国际标准，将有助于实现互操作性，并能够安全采用新的协作技术来提供医疗保健服务。安全且保护隐私的信息共享能够显著改善医疗保健效果。

通过实施本国际标准，医疗保健组织有望减少安全事件的数量和严重程度，从而能够将资源重新调配到生产性活动中。因此，信息技术安全将使医疗资源能够以经济高效且富有成效的方式进行部署。事实上，备受尊敬的信息安全论坛和市场分析师的研究表明，全面良好的安全措施能够使组织的业绩提高多达 2%。

最后，采取一种所有医疗保健领域相关人员都能理解的、一致的信息技术安全方法，将提升员工士气，并增强公众对维护个人健康信息系统的信任。

如何使用本国际标准

不熟悉 ISO/IEC 27002 的读者在继续阅读之前，建议先阅读该标准的引言部分。ISO 27799 的实施者应首先仔细阅读 ISO/IEC 27002，因为下文会频繁提及该标准的相关条款。若无 ISO/IEC 27002 的完整文本，无法充分理解本国际标准。

寻求有关如何在医疗保健环境中实施 ISO/IEC 27002 指南的读者将在附录 B 中找到一份实用的行动计划。本条款中不包含强制性要求。相反，它提供了有关如何在医疗保健领域最佳实施 ISO/IEC 27002 的一般性建议和指导。该条款围绕 ISO/IEC 27001 中描述的活动周期（计划/执行/检查/行动）组织，遵循这些活动将有助于建立一个稳健的信息安全管理体系。

寻求有关 ISO/IEC 27002 中所述安全控制类别和条款的具体建议的读者，可在本国际标准中找到与 ISO/IEC 27002 具有相同条款编号和标题的条款。本条款将引导读者了解 ISO/IEC 27002 中的 11 个安全控制条款。在适当情况下，会说明最低要求，并且在某些情况下，还会就某些 ISO/IEC 27002 安全控制在健康信息保护中的正确应用制定规范性指南。

一旦 ISO/IEC 27002 得以实施，持续管理就被认为是保持国际标准效益的关键所在。第 18 条讨论了合规性评估以及持续的信息安全管理要求。附录 C 包含了有关合规性的自我评估矩阵。

本国际标准附有四个资料性附录。

附录 A 描述了健康信息面临的一般威胁。附录 B 简要介绍了实施与信息安全相关的国际标准的实用行动计划。附录 C 提供了符合 ISO 27799 的检查表。第 2 条列出了以规范方式引用的标准；参考文献列出了其他与健康信息安全相关的标准。

健康信息学-采用ISO/IEC 27002标准的健康信息安全管理

1 范围

本国际标准为组织的信息安全标准和信息安全管理体系实践提供了指导方针，包括控制措施的选择、实施和管理，同时考虑了组织的信息安全风险环境。

本国际标准规定了支持在卫生信息学领域对 ISO/IEC 27002 进行解释和实施的指南，并且是该国际标准的配套标准。4)

本国际标准为 ISO/IEC 27002 中所述控制措施提供了实施指南，并在必要时对其进行补充，以便能够有效地用于管理健康信息安全。通过实施本国际标准，医疗保健组织和其他健康信息保管者将能够确保其组织情况所要求的最低必要安全水平，并保持其保管的个人健康信息的保密性、完整性和可用性。

本国际标准适用于健康信息的所有方面，无论信息采取何种形式（文字和数字、录音、绘图、视频和医学图像），无论采用何种方式存储（打印或书写在纸上或电子存储），以及无论采用何种方式传输（手工、传真、计算机网络或邮寄），因为信息始终应得到适当保护。

本国际标准与 ISO/IEC 27002 一起规定了医疗保健领域信息安全方面的要求，但并未规定如何满足这些要求。也就是说，在最大程度上，本国际标准是技术中立的。技术中立性是其一个重要特征。安全技术仍在快速发展，其变化速度如今以月而非年来衡量。相比之下，尽管国际标准会定期接受审查，但总体而言，其有效期通常为数年。同样重要的是，技术中立性使供应商和服务提供商能够自由推荐符合本国际标准所描述的必要要求的新技术或正在发展的技术。

正如引言中所指出的，熟悉 ISO/IEC 27002 对于理解本国际标准是必不可少的。

以下信息安全领域不在本国际标准的范围内:

a) 用于有效匿名化个人健康信息的方法和统计测试;

b) 个人健康信息假名化的方法（关于此主题的具体技术规范的简要说明见参考文献）;

C 网络服务质量以及用于卫生信息学的网络可用性测量方法;

d) 数据质量（与数据完整性有别）。

4 This International Standard is consistent with the revised version of ISO/IEC 27002.

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。