国际标准

ISO 27799

健康信息学——基于ISO/IEC 27002的医疗信息安全控制

医疗信息技术——基于 ISO/IEC 27002 标准的医疗领域信息安全控制

第三版 2025-12

参考编号
ISO 27799:2025（英文）

受版权保护的文档

ISO版权办公室
CP401·Ch.de Blandonnet 8
CH-1214 Vernier，日内瓦
电话：**41227490111**
电子邮件：copyright@iso.org
网站：www.iso.org 发布

于瑞士

目录

前言

国际标准化组织（ISO）是一个由各国国家标准机构（即ISO成员机构）组成的全球性联合会。国际标准的制定工作通常由ISO技术委员会负责开展。任何对特定技术领域感兴趣并已成立相应技术委员会的成员机构，均有权派代表参与该委员会的工作。各类国际组织（包括政府机构和非政府组织）也会在ISO的协调下共同参与相关工作。在电气技术标准化的所有事务中，ISO均与国际电工委员会（IEC）保持密切合作。

本文件的制定程序及其后续维护程序详见ISO/IEC指令第1部分。特别需要注意的是，**不同类型的ISO文件所需的不同批准标准**。本文件依据ISO/IEC指令第2部分的编辑规则起草（详见www.iso.org/directives）。

ISO特此提醒：本文件的实施可能涉及使用(a)一项或多项专利。ISO不对相关专利权利的证据真实性、有效性或适用性表明任何立场。截至本文件发布之日，ISO尚未收到实施本文件可能需要使用(a)任何专利的通知。但需提醒实施方，上述信息可能并非最新数据，最新信息可从www.iso.org/patents提供的专利数据库获取。ISO不对任何或全部此类专利权利的识别承担责任。

本文件中使用的任何商品名称均为为方便用户而提供的信息，不构成任何背书。

有关标准的自愿性、ISO中与合格评定相关的特定术语和表述的含义，以及ISO在技术性贸易壁垒（TBT）方面遵守世界贸易组织（WTO）原则的信息，请参阅www.iso.org/iso/foreword.html。本文件由ISO/TC 215技术委员会*健康信息学*与欧洲标准化委员会（CEN）CEN/TC 251技术委员会*健康信息学*根据ISO与CEN之间的技术合作协定（《维也纳协定》）共同制定。

第三版废止并取代了技术上已修订的ISO 27799:2016和ISO/TS 14441:2013。

主要变化如下：

—与ISO/IEC 27002:2022的新结构保持一致，并反映该标准较前一版本的其他变更；

——修订并增加针对健康领域的具体管控措施；

— 移除原本仅出现在本文件第二版中、后被纳入 ISO/IEC 27002:2022 的内容；

一 增加了提供有关医疗卫生机构网络安全补充指导的详尽附录，并基于ISO/TS14441:2013标准第5.3节，更新了医疗卫生信息系统安全与隐私要求的示例。

关于本文件的任何反馈或问题均应提交给用户所在国的国家标准机构。这些机构的完整列表可在www.iso.org/members.html查阅。

引言

0.1 概要

本文件包含一套适用于医疗机构的信息安全控制措施。该文件涵盖了ISO/IEC 27002:2022标准中的所有控制措施，并在某些情况下对这些控制措施进行了补充，或提供了其在医疗领域应用的指导原则。此外，还包含若干专为医疗行业设计的额外控制措施，这些措施并非源自ISO/IEC 27002:2022标准中的任何条款。

0.2 背景与上下文

影响医疗保健领域信息安全的因素包括以下几点：

a) 指采用数字技术作为运行基础、且专门或主要应用于医疗领域的设备。搭载健康软件的医疗器械便是典型代表。

b) 需要在临床安全性和有效性与信息安全之间取得平衡。

c) 在确保患者能够获取相关个人健康信息以用于诊断和治疗的同时，维护其隐私。

d)个人健康信息在组织内部及组织之间（可能位于不同司法管辖区）的分布式特性，导致需要各类系统、应用程序和设备之间具备高度的互操作性。

e) 使用者涵盖多种不同群体，包括医生、护士、其他临床医师、培训人员、学生、医疗助理、技术人员、行政人员及志愿者，以及受照护者及其代理人。

f) 负责医疗保健、临床研究、教学、教育及培训等领域中的一项或多项工作的各组织之间及内部存在多重相互依存关系与信息流动。

g)在正常情况下，某些医疗服务需要持续提供（每天24小时不间断）。此外，自然灾害及其他异常事件可能导致对医疗服务的需求激增。

h) 提供医疗服务的机构，以及系统、设备和器械的制造商或供应商，均须遵守一系列广泛的法律、法规、监管及合同要求，这些要求在不同司法管辖区可能存在差异。

i) 不同职业（如信息通信技术（ICT）人员与医疗器械工作人员）在确保系统、设备及装置的安全性方面，其问责制与专业责任的要求存在重叠或不完整之处。

鉴于这一总体背景，医疗保健行业具有若干特定于该行业的信息安全要求（即便这些要求并非独一无二）。然而，ISO/IEC 27002:2022中的控制措施是刻意采用通用形式的，因此才需要制定本文件。

0.3 受众与用途

本文件适用于以下类型的组织：

——因其他原因提供医疗服务或保管个人健康信息；

——提供用于处理个人健康信息的软件、系统、设备、装置或服务；

— 负责医疗保健监管、认证、检查、质量保证或类似工作。

本文件特别适用于以下人员：

— 在上述各类组织中工作的信息通信技术（ICT）及医疗设备或器械专业人员；

—信息安全专业人士（尤其是不熟悉医疗领域的人员）：这类专业人士包括顾问、渗透测试员、审计师，以及就职于提供信息安全认证、检查、保证或认可服务机构的人员。

正确实施本文件所述的各项控制措施，能够为个人（包括受照护者、其代理人及组织员工）提供保障；同时也能为各类利益相关方（包括医疗机构的管理层与治理委员会、与其他医疗机构进行信息交换或共享的机构、公共主管部门、监管机构、审计机构，以及为医疗服务提供资金支持、保险承保、资质认证或监督检查的机构）提供保障。

本文件适用于医疗保健机构，在制定和实施符合ISO/IEC 27001标准的信息安全管理体系（ISMS）控制措施时使用。

健康信息学——基于ISO/IEC 27002的医疗信息安全控制

1 范围

本文件为医疗机构提供了信息安全控制措施（包括实施指南），其制定依据为ISO/IEC 27002:2022标准。

除广泛应用于其他领域的通用信息通信技术（ICT）设备和软件外，本文件的范围还包括专为医疗保健领域设计的软件和系统，例如电子健康记录系统以及集成健康软件的医疗设备。此类医疗设备可具备可编程特性，且可包含软件、固件或两者兼有。

其他数字设备（例如用于环境与感染控制、楼宇管理及物理安全的设备）亦属于适用范围，这些设备可应用于提供医疗服务的场所。

本文件适用于信息的各个方面，无论信息以何种形式呈现（包括文本、数字、录音、图纸、图像和视频），无论其通过何种方式获取或采集，无论采用何种存储方式（如打印、书写于纸张或电子存储），亦无论通过何种方式传输或交换（口头、手递、邮寄、存储介质移动、直接链接或网络）。

本文件适用于所有类型和规模的组织，这些组织提供医疗保健服务，或出于其他原因保管个人健康信息。其负责的信息可通过多种方式和地点进行存储和处理，包括本地或云端，但均属于本文件的适用范围。

本文件适用于所有提供医疗服务的实体场所，例如医院、诊所以及专用于医疗目的的其他场所或设施（如救护车、移动影像或诊断单元）。该文件同样适用于在其他场所（如住宅设施）提供的医疗服务。除上述各类场所外，本文件还涵盖所有医疗服务提供方式，包括远程或虚拟医疗服务。

2 规范性参考文献

文中引用的下列文件，其部分或全部内容均构成本文件的要求。对于标注日期的引用，仅引用的版本有效；对于未标注日期的引用，则适用所引用文件的最新版本（包括所有修订内容）。

ISO/IEC 27002:2022 *信息安全、网络安全与隐私保护——信息安全控制*

ISO 81001-1，*医疗软件与医疗信息技术系统的安全性、有效性及安全性——第1部分：原则与概念*

3 术语、定义及缩写词

就本文件而言，应适用ISO/IEC 27002:2022、ISO 81001-1及下述标准中规定的术语和定义。

ISO和IEC维护术语数据库，用于标准化工作，具体地址如下：

—ISO在线浏览平台：网址为https://www.iso.org/obp

——IEC Electropedia：可在https://www.electropedia.org/获取

3.1 术语与定义

3.1.1
健康
全面的生理、心理和社会福祉

条目注释1：健康不仅仅是没有疾病或虚弱。

条目注释2：改编自世界卫生组织1）。

3.1.2
健康软件
专为管理、维护或改善个人健康（3.1.1）或提供医疗服务而设计的软件，或为集成到医疗器械中而开发的软件

条目注释1：健康软件完全涵盖了被视为医疗器械类软件的范畴。

[来源：ISO 81001-1:2021,3.3.9]

3.1.3
卫生保健

与个人*健康*（3.1.1）相关的护理活动、服务、管理或物资3.1.4

个人健康信息
与个人的*身体健康或心理健康*（3.1.1）**或向该个人提供健康服务**相关且可识别个人的信息

条目注释1：个人健康信息可包括以下内容：

a) 关于个人注册提供医疗服务的相关信息；

b) 关于该个人的医疗支付或医疗资格相关信息；

c) 为健康目的而分配给个人的编号、符号或特定标识，用于唯一识别该个体；

d) 在向个人提供医疗服务过程中收集的关于该个人的任何信息；

e) 通过对身体部位或体液进行检测或检查所获得的信息；

f) 将某人（例如医疗专业人员）认定为该个体的医疗服务提供者。

条目注释2：个人健康信息不包括以下信息：无论是单独存在时，还是与信息主体可获取的其他信息结合时，均已经过匿名化处理。

条目注释3：个人健康信息是个人身份信息（PII）的一个子集。来源：ISO/TS 17975:2022，第3版.21，

修订版——新增了条目注释3。

3.1.5
代表权
监护人代理书
有权代表*受照护人*作出决策的人（3.1.6）

示例1：尚未成年的儿童的父母。

示例2：学习障碍或缺乏精神能力的成年人的监护人。

条目注释1：改编自ISO 13940:2015，5.2.4.3。

1) https://www.who.int/about/governance/constitution。

3.1.6
受照管主体
寻求、正在接受或已接受医疗服务的人员（3.1.3）

条目注释1：改编自ISO 13940:2015第5.2.1节。

3.2 缩写术语

HLT 健康

ICT 信息和通信技术

ISMS 信息安全管理系统

PII 个人身份信息

4 概要

4.1 本文档的结构

本文件采用ISO/IEC 27002:2022标准的结构（第5至第8条款），并列出了该标准中的所有控制标题。基于此框架，本文件：

a) 表明ISO/IEC 27002:2022标准中哪些控制措施（包括其目的、指南及其他相关信息）在健康领域保持不变；

b) 对于ISO/IEC 27002:2022中的某些控制措施，该标准提供了关于如何在医疗健康领域实施这些控制措施的指导、其他相关信息，或两者兼有。

c)对于ISO/IEC 27002:2022中其余的控制措施，本文补充说明了每项控制措施的内容、目的及实施指南。在某些情况下，还提供了与健康相关的其他信息。

d)本规范规定了专门针对健康领域的控制措施，这些措施并非基于ISO/IEC 27002:2022中的任何现有控制措施。这些附加控制措施的结构与ISO/IEC 27002中的控制措施相同，其控制措施标题前缀为“HLT”（代表HeaLTh）。

关于ISO/IEC 27002:2022，c)和d)项中的控制措施分别是补充性和附加性的本文件包含4个附录：

—附件A是一份专门针对健康领域的控制措施参考清单，即c)和d)项下的控制措施。附件A亦是对ISO/IEC 27001:2022标准附件A的补充。

—附录B提供了一个对照表，展示了本文件中的 HLT 控制措施与ISO 27799:2016标准中控制措施的对应关系。该附录为两个版本之间的过渡提供了支持，并补充了ISO/IEC 27002:2022标准的附录B。

一附录C提供了关于医疗保健领域中信息安全方面尤为重要的信息。

—附录D提供了医疗信息技术系统开发与采购的示例要求，以及其与MDS2（医疗器械安全制造商披露声明）的对应关系。

4.2 安全

安全、健康与信息系统效能相互依存。在评估和管理风险及其风险控制措施时，始终应考虑这一相互关系。例如，系统或数据在诊疗现场无法使用的风险不仅属于安全风险；若影响诊疗决策的制定，该风险将对安全性产生重大影响。进而，这将影响卫生系统的整体效能。

安全性、保障性和有效性三者相互依存的特性导致一个结果：某些出于善意的风险控制措施，在特定情况下可能对其中一项或两项特性产生负面影响。例如，为降低未经授权访问带来的风险而实施的管控措施，可能影响系统的可用性和可用性，从而削弱系统效能；同时，这些措施还可能催生出损害安全性的系统变通方案。

在卫生领域的信息安全管理体系的所有方面，均应考虑安全性问题，包括控制措施的选择与实施。因此，在本文件中实施控制措施时，必须充分考虑其对安全性可能产生的任何影响。

4.3 选择并应用控件

4.3.1 确定控制措施

控制措施的确定取决于组织在完成风险评估后所作出的决策，且该评估必须具有明确的范围界定。针对已识别风险的相关决策，应基于风险接受标准、风险处理方案以及组织所采用的风险管理方法。在确定控制措施时，还必须充分考虑所有相关的国家及国际法律法规。此外，控制措施的确定还取决于这些措施之间如何相互配合，从而形成多层次的防御体系。

卫生组织应根据实际情况，从本文件及ISO/IEC 27002标准中选择适当的信息安全控制措施。此外，可根据实际需求设计新的信息安全控制措施以满足特定要求。

4.3.2 指导的应用

若本文件提供了针对某项控制措施的医疗保健领域具体指导且该控制措施正在实施，则应遵循该指导；若未遵循，则需记录未遵循的原因，并说明如何实现该控制措施的目的（“遵守或解释”）。

在某些控制措施的指导文件中，存在指向本文件内其他控制措施或其他标准（或两者）的交叉引用。此类交叉引用仅用于提供信息参考。

4.3.3 符合 ISO/IEC 27001:2022 标准使用

如附录A所列，这些补充性和附加性控制措施可用于在卫生机构中确定和实施符合ISO/IEC 27001标准的信息安全管理体系（ISMS）相关控制。

ISO/IEC 27001:2022标准第6.1.3节要求组织编制适用性声明。附录A中的控制措施也可用于此目的。

5 组织控制

5.1 信息安全政策

应遵循ISO/IEC 27002:2022标准第5.1节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

信息安全政策应明确信息安全的管理方法，并须获得最高管理层批准，之后至少每年进行一次审查，且在发生任何重大安全事件后也需重新审查。

健康用途（补充）

确保最高管理层对信息安全的承诺，并确保该承诺始终保持最新状态。

健康指导

信息安全政策应包含以下内容的相关声明：

a) 对健康信息安全的需求；

b)健康信息安全的目标；

c) 合规范围；

d)立法、监管及合同方面的要求，包括保护个人健康信息的相关规定，以及医疗专业人员保护此类信息所承担的法律与伦理责任；

e) 信息安全事件通报机制，包括用于提出保密相关关切的渠道，且相关人员无需担心受到责备或追究责任；

f) 及时报告实际或疑似事件（包括险些发生的事故）至关重要，这样一旦发生任何事件，便能尽早处理，避免事态恶化。

g)识别医疗保健领域中至关重要的流程与系统（即其失效可能导致护理效果不佳或患者安全降低）。

政策内容的修订应以风险评估的结果为指导。

在制定和维护信息安全政策及特定主题政策时，应考虑以下因素：

a) 健康信息的广度；

b) 员工的权利与责任，包括法律及道德要求、专业机构制定的标准以及任何当地规定；

c) 受照护对象享有隐私权，以及在适用情况下享有查阅其医疗记录的权利；

d)临床医生在获取受照护者知情同意及保护个人健康信息保密方面的义务；

e) 多个组织（这些组织可能位于不同的司法管辖区）提供医疗保健或支持服务，以及个人（包括受照护者本人及其亲属或亲密伴侣），他们可参与受照护者当前或过去的健康和社会照护的提供、确定、实施或筹资（见附件C）；

f) 为研究和临床试验目的而应用于信息共享的协议与程序；

g)相关安排及访问限制如下：

1) 参与医疗服务提供工作的人员，包括正式员工、临时或访视人员，例如代班人员、培训人员、学生以及“值班”或机构工作人员（更多信息见附件C）；

2)为直接护理提供支持的人员，包括行政及辅助人员、神职人员、慈善工作者及其他志愿者（更多信息见附件C）；

3)来自监管和检查机构、财务及其他审计机构、卫生专业人员等人员，负责调查涉及医疗服务提供的临床或其他事件；

h) 当必须从外部获取有关当事人的信息，或此类信息被当局或其他第三方要求提供时：此类情况包括有人在犯罪过程中受到伤害，或存在对儿童、妇女、老年人、学习障碍人士及其他弱势群体遭受虐待或照护不足的嫌疑；

i) 安全措施对患者安全的影响；

j) 信息安全措施对健康信息系统功能与性能的影响。

当获得第三方的支持或协作时，尤其是当机构从其他司法管辖区获取服务时，相关政策框架应包含有文件记录的政策与程序，涵盖此类互动，并明确各方的责任。

在适用的情况下，政策审查应涵盖以下方面：

a) 运营模式的不断变化，以及由此带来的风险特征和风险管理需求的相应调整；

b) 对信息通信技术（ICT）架构或基础设施（或两者）所做的修改，以及这些修改对风险状况所产生的相应影响；

c) 外部环境中已识别出的、同样会影响风险状况的变化；

d)由各司法管辖区卫生机构或新立法/法规所规定的最新控制措施、合规要求及保证机制；

e)卫生专业协会及监管机构在 PII 保护领域的最新指南与建议（另见5.34）；

f) 法院审理的法律案件结果，这些案件确立或推翻了判例，或形成了既定实践；

g)该政策面临的挑战与问题，已由其工作人员、受照护者及其伴侣与照护者、研究人员及政府机构（例如 PII 保护领域的监管机构）向该组织提出。

h) 报告患者安全事件，以便在患者安全事件由信息安全措施失效导致的情况下制定相应的缓解措施。

5.2 信息安全角色与职责

应遵循ISO/IEC 27002:2022标准第5.2节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

至少应有一名专人负责信息安全工作。

目的（补充）

为确保明确的工作方向、对涉及健康信息安全的活动提供可见的管理支持，并具备充足的技术专业知识。

健康指导

只有当组织具备明确的信息安全管理体系基础设施时，才能长期维持信息安全的问责机制与协调机制。

在信息安全相关的职责与责任中，一个关键要素是设有信息安全官或能够获得其权限——该官员负责统筹信息安全工作。最重要的是，最高管理层必须对所有与信息安全相关的事宜承担相应的责任。

许多组织，尤其是规模较大的组织（例如员工人数超过500人或客户数量超过10,000家），都应设立信息安全咨询小组。此类小组有时也被称为委员会或董事会。

该小组的宗旨是确保为保障健康信息安全提供明确的方向和可见的管理支持。小组应定期召开会议（通常每月一次），以“及时掌握情况”并保持信息更新。

除信息安全官外，该小组还应包括来自以下组织的代表：

—使用健康信息技术系统或其他信息通信技术基础设施及服务（例如：医生、护士、其他临床医师、管理人员及行政人员）；

—在组织内对系统和服务的运行承担专业责任或问责义务（例如，信息通信技术工作人员、**医疗设备及医院工程专业人员）。**

其他健康信息

有关信息安全咨询小组的更多信息，请参见附件C。

5.3 职责分离

应遵循ISO/IEC 27002:2022标准第5.3节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在规模极小的组织中，有时无法完全分离所有相互冲突的职责与责任范围。在此类情况下，应在可行范围内对职责与责任范围进行划分。此外，应对仍存在的问题性冲突采取相应措施。剩余的冲突领域应予以记录，并附上相应的补偿措施。

医疗保健领域的许多工作人员（如专业人员和研究人员）会持续转换角色。原本不存在冲突的职责或责任范围，可能在瞬间转变为相互冲突的状态。例如，一名医师可能某一时刻正在指导实习医师，下一刻便开始提供临床诊疗服务。对于职责与责任范围频繁变更的岗位，应特别重视职责与责任范围的分离管理。

5.4 管理职责

应遵循ISO/IEC 27002:2022标准第5.4节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.5 与当局取得联系

应遵循ISO/IEC 27002:2022标准第5.5节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.6 **与特殊利益集团接触**

应遵循ISO/IEC 27002:2022标准第5.6节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

隐私保护要求对信息安全具有重大影响。鉴于医疗领域特有的考量因素，应考虑与那些专注于健康信息隐私与安全的组织、论坛及 professionals ′associations 建立合作关系。

5.7 威胁情报

应遵循ISO/IEC 27002:2022标准第5.7节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在健康领域，存在多种需要予以考虑并持续保持情报掌握的威胁因素。其中尤为相关的因素包括以下几点：

a) 除通用的信息通信技术（ICT）和物联网设备外，还存在专用于医疗领域的设备，其中包括多种不同类型和型号的医疗器械。

b) 对于通用的信息通信技术设备，安全措施包括更新软件、应用补丁以及使用能防范恶意软件的软件。**出于临床安全**及其他原因，在某些配备健康软件的医疗设备上，可能无法采取此类措施。

c) 许多医疗机构使用的硬件和软件已过时、配置不当，或两者兼有。

d)在维护准确的库存数据和控制资产方面，可能会面临特定的挑战。

其他健康信息

更多信息见附件C。

5.8 信息**安全在项目管理中的应用**

应遵循ISO/IEC 27002:2022标准第5.8节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

项目管理中应充分考虑安全性和隐私保护。

其他健康信息

另请参阅5.38，其中讨论了分析与规范；另请参阅5.34，其中涉及隐私保护。

ISO 81001-1 对安全性、有效性与安保性之间的相互依存关系（包括项目管理相关问题）提供了详尽指导。该标准还提供了其他相关标准的信息，尤其针对医疗器械领域。

5.9 信息及其他相关资产的清单

应遵循ISO/IEC 27002:2022标准第5.9节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

所有信息流（包括组织内部及组织之间的信息流）及其接口（含集成平台）均应纳入清单。

健康用途（补充）

为确保信息流及其接口得到明确标识，从而保障信息安全并明确相应的所有权归属。

健康指导

除了设备、装置和软件组件等资产外，卫生组织日益依赖结构化信息流（既包括组织内部IT架构各模块之间的信息流动，也涵盖与外部各方的信息交互），以及相关的接口——尤其是集成平台。

在客户与供应商的关系中，所有权有时难以确定。此类情况下，双方之间的（合同）协议可提供帮助；该协议也有助于明确所有者的义务。

其他健康信息

有关资产所有权以及资产的不同类型和用途的更多信息，请参见附件C。

5.10 信息及其他相关资产的合理使用

应遵循ISO/IEC 27002:2022标准第5.10节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.11 资产返还

应遵循ISO/IEC 27002:2022标准第5.11节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

应制定相关政策，要求个人提供书面确认，证明其持有的所有形式资产均已妥善归还或按要求删除。

健康用途（补充）

在变更或终止雇佣关系、合同或协议的过程中，保护个人健康信息。

健康指导

该政策应包含相关措施：若在雇佣关系、合同或协议变更或终止期间或之后发现，部分资产未被妥善归还或删除，则可对相关个人采取相应措施。

保险单要求的书面确认文件应包含所有不属于个人、且存储于个人自有设备或代表个人在其他地方存储的信息（例如由云服务提供商提供的存储及其他服务，包括电子邮件）。

在归还个人或其代表持有的信息会导致不必要的重复时，该政策可允许个人安全删除该信息而无需归还。政策应明确规定确保安全删除所需遵循的技术措施。

5.12 信息分类

应遵循ISO/IEC 27002:2022标准第5.12节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

个人健康信息至少应被归类为机密信息。

健康用途（补充）

确保在所有情况下对个人健康信息进行正确分类。

健康指导

医疗领域的分类工作颇具挑战性。需综合考虑以下因素。

—医疗记录及其他个人健康信息的法律、法规、监管、合同及地方政策要求存在显著差异。在某些情况下，这些要求基于纸质记录的规定，未能充分考虑电子存储的信息。其他潜在问题还包括要求表述模糊或不一致。这种情况通常源于要求本身持续演变，且存在多个不同的法规来源。例如，作为 PII 子集的个人健康信息，既受总体性数据保护法规的约束，也需遵守其他非健康领域特有的要求。

在个人健康信息领域，通常需要采用多种分类标准。例如，关于腿部骨折的信息与性传播疾病的信息显然属于不同敏感等级。知名人士的个人健康信息与其他人的相比可能存在差异。某些敏感等级会随时间变化：部分个人数据敏感度较低（例如，十年前的精神健康发作与当前发作之间的差异），而另一些数据则可能变得更为敏感。个人信息还可通过整合其他来源的数据而改变其分类等级。此外，某些个人健康信息可能关联到其他个体：例如涉及遗传因素的家庭成员信息，或涉及施加伤害行为的信息（如儿童虐待案例）。

所有均需分类的个人健康信息，也可能来源于可穿戴技术、植入式设备及其他医疗装置。对于遗传数据和生物识别数据应给予特别关注——尤其是在相关法律、法规、监管要求、合同条款及地方政策对此类数据的要求不够详细或具体的情况下。

5.13 信息标注

应遵循ISO/IEC 27002:2022标准第5.13节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

并非所有健康信息都属于机密信息，也并非所有健康信息系统都允许用户访问个人健康信息。健康信息系统的用户需要明确：其所访问的数据是否包含或构成个人健康信息。

应考虑在用户每次启动或登录时（例如）向其提供相关信息。然而，仅在特定用户首次访问系统时提供此类信息即可满足需求。

5.14 信息传输

应遵循ISO/IEC 27002:2022标准第5.14节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

在任何转让发生之前，必须制定相应的规则、程序及协议。

健康用途（补充）

确保信息在整个生命周期内的传输安全。

健康指导

各组织应确保信息交换的安全性成为政策制定及合规审计的核心内容（参见5.36）。应恰当运用加密技术。

通过采用明确规定需实施最低限度控制措施的信息交换协议，可以显著提升信息交换的安全性。此类协议对所有参与信息交换的各方均具有约束力，而规则和程序通常仅适用于单一组织内部。

应制定相关政策，确保通过电子邮件、即时通讯或其他方式交换的个人健康信息及其他机密信息得到妥善保护。若无法实现足够的安全性，则绝不应通过这些渠道交换此类信息。

其他健康信息

关于健康信息交换政策的具体指导可参阅ISO 22857标准。尽管ISO 22857明确提及个人健康信息的跨境流动（此处的“边界”指法律管辖范围，而非必然指国家边界），但其大部分建议可根据实际需求进行调整，以适用于不同组织之间的数据交换。

5.15 访问控制

应遵循ISO/IEC 27002:2022标准第5.15节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

个人健康信息的访问权限应由适当的政策（如基于角色的访问控制）进行规范。

健康用途（补充）

确保对个人健康信息的访问权限得到妥善控制。

健康指导

个人健康信息访问权限的控制

对个人健康信息的访问权限应予以严格管控。一般而言，健康信息系统的用户仅应访问其个人健康信息：

a) 当用户属于数据主体（即其个人健康信息被访问的受照护对象）的照护团队成员时；

b)当用户代表数据主体执行某项活动时；

c) 当需要特定数据来支持此项活动时。

为防止医疗服务延迟或受到其他不利影响，可能需要制定明确的政策和流程（并附相关授权），以便在紧急情况下 override “常规”访问控制规则（有时称为“打破玻璃”）。

控制模型

该组织应采用适当的控制模型制定访问策略，以实现以下目标：

a) 满足预定义角色的需求，其相关权限应与该角色的需求相一致且仅限于满足该角色的需求；

b)体现专业性、伦理性、法律性及患者照护相关要求；

c) 支持医疗专业人员或其他授权人员执行的任务及相应的工作流程。

其他健康信息

基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）是可行的访问控制模型，有时会结合使用。

另请参阅5.34关于可能限制个人健康信息访问的其他隐私注意事项，这些注意事项应酌情纳入访问控制策略。

ISO 22600系列标准提供了关于健康信息学中访问控制的进一步信息。

5.16 身份管理

应遵循ISO/IEC 27002:2022标准第5.16节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

应对有权查阅个人健康和其他保密信息的用户实行正式登记程序。

健康用途（补充）

为确保每位用户均被分配正确的用户身份。

健康指导

注册流程应包含严格的验证环节，以确保分配给用户的身份信息经过适当的身份认证，并且其访问权限与其角色相匹配。

在适用情况下，注册流程应包含以下全部内容：

a) 核实该个人是否与其自称的身份一致；

b) 核实个人的专业资质，包括其当前资质是否有效；

c) 准确采集与个人相关的信息；

d)分配唯一且无歧义的用户身份。

对于刚加入组织的人员，其个人信息（如姓名、出生日期）应与护照等有效证件进行核对；除非此类核对已在筛选流程中完成（更多信息参见6.1）。

专业资质应通过相关注册机构、监管机构或专业组织进行核实；部分专业资质可通过数字证书进行验证。

注册流程应适用于各类用户，包括医疗专业人员、具有高级权限的信息通信技术（ICT）工作人员、患者及其照护人员。上述各类用户均需满足不同的注册要求。

其他健康信息

将身份管理与物理安全相关活动相结合具有积极作用。例如，发放用于控制房间或场所出入权限的安全通行证；另一个例子是发放身份徽章或通行证。

5.17 认证信息

应遵循ISO/IEC 27002:2022标准第5.17节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在医疗服务提供场景中，时间压力可能导致密码的有效使用变得困难。在此类情况下，医疗机构应考虑采用替代性身份验证技术以解决这一问题。

其他健康信息

另见8.5。

5.18 访问权限

应遵循ISO/IEC 27002:2022标准第5.18节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

尤其在大型医院中，通常有大量员工会短期访问个人健康信息。对此类员工访问权限的终止需要谨慎管理。此类员工包括学生、实习生、培训人员及临时工；其他还包括代理人员或同等职位人员，以及承担他人职责或轮班工作的正式员工。

另一个问题是，许多交易发生在医疗护理事件（例如医疗记录转录的确认）之后，有时甚至延迟了相当长的时间。这会显著增加及时撤销访问权限的复杂性，在设计和实施访问权限撤销流程时必须充分考虑这些交易因素。

一旦收到辞职通知、解雇通知等文件，应立即终止相关访问权限；若继续此类访问行为会带来更高的风险，则必须采取此措施。

5.19 供应商关系中的信息安全

应遵循ISO/IEC 27002:2022第5.19节中规定的控制措施、相关属性表、目的、**指导原则**及其他信息。

健康控制（补充）

应评估外部人员访问系统或其所含数据所带来的风险，并根据所评估的风险实施相应的控制措施。

健康用途（补充）

管理和保护供应商对系统及数据的外部访问权限。

健康指导

风险评估对于有效管理第三方对包含健康信息（尤其是个人健康信息）的系统的访问至关重要。

受照护者的权利应得到保护，即使拥有潜在个人健康信息访问权限的第三方位于与管理该受照护者或健康机构不同的司法管辖区。

所有可能被供应商以任何理由（包括提供云服务、数据处理、技术支持、培训或测试）访问的个人健康信息及其他机密信息，均应进行加密处理。

应制定相应的政策，并配套相应的流程和程序，以确保目标得以实现并受到有效监控。在某些情况下（例如特定医疗器械），无法对数据进行加密，此时应基于风险评估实施相应的管控措施。

其他健康信息

根据不同的系统、服务及供应商，信息可能通过多种方式被访问——例如使用运行在数据库、文件系统或网络上的应用程序、实用工具及工具包。供应商及其分包商可能拥有管理权限或其他特权，同时还具备诊断功能或特殊权限工具，这些工具可能使用户能够获取机密信息。对于供应商的客户而言，要全面了解供应商的实际能力范围几乎是不可能的。在评估与供应商合作关系的风险时，必须充分考虑这些因素。

5.20 在供应商协议中解决信息安全问题

应遵循ISO/IEC 27002:2022标准第5.20节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.21 管理信息通信技术供应链中的信息安全

应遵循ISO/IEC 27002:2022标准第5.21节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

对于配备健康软件的医疗器械，制造商应提供的信息包括医疗器械安全声明（MDS2）、配置要求、漏洞评估以及软件物料清单（SBOM）。

其他健康信息

参见附件D和ISO 81001-1。

5.22 供应商服务的监控、审查及变更管理

应遵循ISO/IEC 27002:2022标准第5.22节规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.23 云服务使用中的信息安全

应遵循ISO/IEC 27002:2022标准第5.23节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

其他健康信息

ISO/TS 23535 和 ISO/TR 21332 提供了关于医疗领域所使用的云服务在安全性和隐私保护方面的相关信息。

5.24 信息安全事件管理的规划与准备

应遵循ISO/IEC 27002:2022第5.24节中规定的控制措施、相关属性表、目的、**指南**及其他信息。

健康指导

在处理和报告信息安全事件时，不应将其与其他类型的事件割裂开来评估。所有类型的事件都应纳入信息安全事件管理流程。毕竟，黑客入侵可能导致信息通信技术（ICT）硬件被盗（进而引发保密泄露）；纵火可能旨在掩盖ICT设备的滥用行为；而已发现的系统滥用或误用行为也可能产生严重的临床后果等。

5.25 对信息安全事件的评估与决策

应遵循ISO/IEC 27002:2022标准第5.25节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

分类与优先级排序方案应考虑事件是否涉及以下一项或两项：

a) 个人健康信息；

b) 集成健康软件的医疗设备。

该方案还应评估临床活动是否（可能）受到影响。

5.26 对信息安全事件的响应

应遵循ISO/IEC 27002:2022标准第5.26节规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.27 从信息安全事件中学习

应遵循ISO/IEC 27002:2022标准第5.27节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.28 证据收集

应遵循ISO/IEC 27002:2022标准第5.28节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

卫生组织应考虑为调查临床事件而收集证据所产生的影响。

5.29 中断期间的信息安全

应遵循ISO/IEC 27002:2022标准第5.29节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.30 企业持续运营所需的ICT基础设施准备

应遵循ISO/IEC 27002:2022标准第5.30节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

医疗机构应明确在医疗保健服务提供过程中至关重要的流程、系统及其他相关设备。

应急预案应根据需要包含备用程序，以应对流程中的故障。
这些系统及其他相关设备对医疗保健服务的提供至关重要。

鉴于医疗保健领域对系统可用性的严格要求，必须特别关注技术与人员层面的弹性与冗余机制建设。

医疗保健领域的ICT连续性规划应与业务连续性规划（例如应对停电的预案、实施感染控制措施以及处理其他临床紧急情况的计划）相适当整合。

受照护对象的安全性取决于能否获取其数据，这一点应在规划阶段予以充分考虑。工业及其他领域中可能导致信息通信技术（ICT）系统瘫痪的灾难和不可抗力危机，正是可能引发健康危机的关键事件——而及时获取健康信息在这些情况下至关重要。

卫生组织还应确保其制定的计划定期按照“程序化”原则进行测试。该测试方案应循序渐进地实施：从桌面测试开始，逐步进行模块化测试、综合估算可能的恢复时间，最终开展全面演练。此类测试方案风险较低，能显著提升用户群体的整体认知水平。

医疗卫生机构应充分认识到健康信息系统在连续性医疗服务中的重要作用。此类机构需做好应对信息通信技术（ICT）系统发生故障时的准备。

根据系统故障的性质和持续时间，可能需要采用其他方式采集本应在正常情况下记录在系统中的患者护理相关信息。**备用方案可包括**使用电子表格或纸质表格等方式。应急措施应确保在故障期间采集的信息尽可能准确、完整且及时。

在系统故障期间采集的数据，通常需要在故障解除后重新运行时手动传输或录入系统。此外还需对数据的准确性、完整性及数据完整性进行额外核查。
应作为更新流程的一部分执行。

5.31 法律、法规、监管及合同要求

应遵循ISO/IEC 27002:2022标准第5.31节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.32 知识产权

应遵循ISO/IEC 27002:2022标准第5.32节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.33 记录保护

应遵循ISO/IEC 27002:2022标准第5.33节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.34 PII 隐私与保护

应遵循ISO/IEC 27002:2022标准第5.34节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

仅当用户确有必要查阅受照护者的医疗记录时，方可获取其个人健康信息。

当用户存在合法需求时，这并不必然意味着用户有权获取所有被照护者的个人健康信息，因为法律、法规、专业要求、当地政策或其他规定可能导致额外的访问限制。例如：

a)对涉及患者性健康、心理健康、避孕措施、当前妊娠状况或既往妊娠结局等个人健康信息的访问权限，可仅限于治疗该特定病症的临床医生。

b) 受照护对象有权指定其健康记录中哪些内容可被特定用户或用户群体访问，哪些不可访问。

c) 受照护对象有权查阅自己的医疗记录，但可能需要对其隐瞒某些信息；这种情况适用于某些心理健康状况，或当受照护者的健康记录中包含其他个人（例如患有相关疾病或诊断的亲属）的信息时——这些信息的隐私必须得到保护。

d)在记录诸如a)项所列的某些健康事项时，可为受照护对象使用化名或特殊标识符生成记录，并限制其获取真实身份信息；

e)某些需要重点关注的对象，其所有记录均可被赋予别名或特殊标识符，以防止他人获取其真实身份；例如，这适用于“重要人物”（VIP）、安全部队成员及犯罪受害者。

对于有权代理人的儿童或成人的记录查阅，还需考虑其他相关因素。

在照护对象或其代理人有权指定是否允许查阅特定记录的情况下，应保存相应的记录日志。这些日志应详细记录向照护对象或其代理人提供的建议及其后续作出的决定。

当拒绝查阅受照护对象部分医疗记录时，存在相应的处理方案。例如：

a) 相关信息可以被完全隐藏，因此用户根本不会察觉其存在；

b) 相关信息可能被遮蔽，或被替换为提示用户某些信息受限制的文字说明。

在需要拒绝访问的情况下，可能适用法律、监管或当地政策要求。**拒绝访问的方法**详见**8.11**。

如5.15所述，在紧急情况下可能需要覆盖某些访问控制或限制。

应特别关注那些不希望其个人健康信息被邻居、同事或亲属等医护人员查阅的受照护者的关切。同样地，工作人员也应予以重视。
成员通常不愿被迫无谓地查阅有关朋友、亲属或邻居的信息。有效的健康信息管理系统应解决这些顾虑。

所有对个人健康信息的访问行为（包括对访问限制的豁免，例如紧急访问）均应进行记录（参见8.15；对于受照护对象的权利，参见ISO 27789:2021第5.2.2节）。未经授权的访问尝试或可疑行为模式（如过度查看记录）应触发警报以供立即调查。

其他健康信息

有关医疗保健领域信息同意管理的更多信息，可参阅ISO/TS 17975标准。

ISO/IEC 27701 是 ISO/IEC 27001 和 ISO/IEC 27002 的扩展标准，为隐私信息管理提供了相关要求与指南。其中多项管控措施可应用于医疗健康领域。

另见附件D。

5.35 信息安全的独立审查

应遵循ISO/IEC 27002:2022标准第5.35节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

鉴于医疗保健领域的特殊性——包括安全性与信息安全之间的相互依存关系——应考虑聘请熟悉该行业的独立评审人员进行评估。

尽管此类评估未必由相关专家执行，且不具备绝对独立性，但来自同行机构的同事所进行的评估可作为正式独立评审的有效补充。

5.36 符合信息安全相关的政策、规则和标准

应遵循ISO/IEC 27002:2022标准第5.36节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应建立一套合规审计计划，涵盖运营的整个生命周期。

a) 识别问题；

b) 审查结果；以及.....

c) 决定对ISMS进行更新。

审计计划应以12至18个月为周期进行正式规划，以确保全面覆盖。

a) 本文件的所有要素，

b)所有风险领域；

c) 所有已实施的控制措施。

在适用情况下，信息安全咨询小组（参见5.2）应确立建立分级合规审计框架的目标，其底层由流程操作人员和管理人员进行自我审计。随后，代表信息安全咨询小组开展的信息安全管理体系（ISMS）审计、内部审计、控制保证评估以及最终的外部审计，均应以确保每一层级都能从其下所有层级获得信任的方式进行定义。

5.37 已记录的操作规程

应遵循ISO/IEC 27002:2022标准第5.37节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

5.38 HLT -信息安全需求分析与规范

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的	#保密性 #诚信 #可用性	#识别	#信息保护#系统与网络安全， #应用安全，#安全配置，#身份和访问管理，#连续性:	#保护，#防御，#韧性

控制

与信息安全相关的要求应纳入新信息系统的开发要求或现有信息系统的改进要求中。

目的

确保在整个信息系统生命周期中有效应对与信息系统开发、采购或两者相关的信息安全风险。

指导；建议

信息安全要求应通过多种方法进行确定，例如根据政策和法规推导出合规要求、进行威胁建模、开展事件审查或采用漏洞阈值。确定结果应予以记录，并由所有利益相关方共同审核。

信息安全要求与控制措施应体现所涉信息的价值（参见5.12和**5.13**），以及缺乏充分安全措施可能造成的潜在负面影响。同时还需考虑其对安全方面的影响。

信息安全需求及相关流程的识别与管理应在信息系统项目的早期阶段就予以整合。在设计阶段等早期阶段就考虑信息安全需求，能够有助于制定更有效且更具成本效益的解决方案。

信息安全要求还应考虑以下方面：

a) 为确定用户身份验证要求，需对用户声称的身份信息达到何种置信度；

b) 为所有类型的用户（包括特权用户和技术用户）提供资源调配与授权流程；

c) 向用户和操作人员明确告知其职责与责任；

d)所涉资产所需的保护要求，特别是关于可用性、保密性及完整性；

e)源自运营流程的要求，例如交易日志记录与监控、不可抵赖性　　所需的东西;

f) 其他安全控制措施所要求的功能，例如：与日志记录与监控系统或数据泄露检测系统的接口。

对于通过公共网络提供服务或实现事务处理的应用程序，应考虑采用专用控制**8.26**。

若采购产品，应遵循正式的测试与采购流程。与供应商签订的合同必须明确规定的安全要求。若拟议产品的安全功能未能满足指定要求，则应在购买前重新评估所涉及的风险及相关控制措施。

应评估并实施与该系统最终软件或服务堆栈相匹配的产品安全配置指南。

应明确产品验收标准（例如基于其功能特性），**这将**确保满足已识别的安全要求。在采购前，应对产品按照这些标准进行评估；同时需审查新增功能，以确保不会引入不可接受的额外风险。

其他信息

详见附录 D。

ISO/IEC 27005提供了关于如何运用风险管理流程来确定符合信息安全要求的控制措施的指导。

5.39 HLT -唯一识别照护对象

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的	#保密性 #诚信 #可用性	#识别	#信息安全保护，#系统与网络安全，#应用安全，#安全配置，#身份和访问管理，#连续性	#保护，#防御，#韧性

控制

应制定相关政策和程序，确保每位受照护对象拥有唯一的唯一标识符，并具备在同一受照护对象存在重复或多条记录时进行合并的功能。

目的

为防止关于受照护对象的信息和记录不完整或不一致。

指导；建议

在紧急医疗护理及其他无法准确识别受照护对象的情况下，可能导致同一受照护对象存在多份病历记录。此外，由于行政原因（例如先前独立运营的医疗机构合并或被收购），受照护对象也可能拥有多份病历记录。

健康信息系统应具备将同一受照护对象的多条记录合并为单一记录的功能。数据合并过程需要高度谨慎的操作、经过专业培训的人员以及适当的技术工具，以确保原始记录中的信息能够被整合为一个统一的整体。

处理个人健康信息的组织应确保：能够推导出个人身份信息的数据仅在必要时予以保留；并尽可能充分地采用删除、匿名化和假名化技术，以最大限度降低个人信息被无意泄露的风险。

5.40 HLT 显示/打印数据的验证

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的	#保密性 #诚信 #可用性	#识别	#信息保护 #系统与网络安全，#应用安全，#安全配置，#身份和访问管理，#连续性	#保护，#防御，#韧性

控制

当显示或打印个人任何个人健康信息时，应包含可识别护理对象的信息。

目的

旨在确认信息适用于正确的护理对象，并防止使用与他人相关的信息。

指导；建议

在依赖健康信息系统提供的个人健康信息之前，医疗专业人员需要获得充分的信息，以确保其所治疗的患者信息与系统所呈现的信息相符。将正在接受治疗的患者信息与现有记录进行匹配并非易事。部分系统通过在每位患者的记录中附加照片身份信息来增强安全性。然而，此类改进措施本身也可能引发隐私问题，因为它们可能隐式捕获面部特征（如种族）等未作为数据字段记录的信息。不同司法管辖区对患者身份识别的要求以及用于支持该识别的数据可用性也存在差异。在设计健康信息系统时必须格外谨慎，以确保医疗专业人员能够信任系统能够提供所需信息，从而确认检索到的每条记录均与实际接受治疗的患者相符。

健康信息系统应能够核验纸质打印输出内容是否完整（例如：“第3页，共5页”）。

5.41 HLT -公开可获取的健康信息

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的	#诚信	#保护	#治理，#资产管理，#信息安全保护，#法律与合规	#保护，#防御

控制

公开提供的卫生信息在其整个生命周期内应受到保护、可追溯、妥善保存和管理。

目的

为确保公开可用的健康信息在需要时能够及时获取，必须保证其完整性不受损害、来源信息得到记录、存在审计追踪机制，并且历史信息可被检索。

指导；建议

公开可获取的健康信息（与个人健康信息不同）可在网站及各类门户网站上找到，其内容通常以医疗建议的形式呈现。例如，其中包含何时预约医生、助产士或其他临床医师的指导信息，而非直接前往急诊科就诊的相关建议。

相关部门可立即提供相关信息。关于处方药及其他药物的信息（包括其副作用）通常也公开可查，同时附有多种疾病的诊断与治疗说明。

照护对象、其陪同人员或代理人可根据公开可获取的健康信息作出重要决策；医疗专业人员亦可依赖此类信息。因此，确保公开可获取的健康信息可靠、准确且及时更新被视为至关重要。为实现这一目标：

a) 必须保护信息的完整性和可用性；

b) 在公开信息之前，必须说明其来源并核实其出处；

c) 必须建立完整的审计追踪记录，以便明确哪些人员创建、修改、删除或对信息进行了其他操作。

d)应建立全面的信息档案库，并提供查阅历史信息的途径，以便明确特定时间点可获取的具体内容。

其他信息

对于仅限组织内部人员访问的内联网、内部知识库及类似资源的信息，也应适用相同的原则。

5.42 HLT -紧急通信

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#纠正性	#可用性	#响应，#恢复	#治理、#信息安全保护、#人力资源安全、#威胁与脆弱性管理、#连续性、#供应商关系安全、#信息安全事件管理、#信息安全保障。.	#保护，#防御，#韧性

控制

应在卫生组织内部规划、实施、维护并测试应急通信渠道，这些渠道应在该组织的信息通信技术（ICT）连续性中断时发挥作用。

目的

确保在信息通信技术（ICT）中断期间仍能实现关键通信。

指导；建议

人际沟通日益依赖信息通信技术（ICT），从而导致对ICT的依赖程度相应增加。一旦ICT出现故障，基于ICT的沟通将迅速无法进行——这对于提供医疗服务而言是不可接受的。因此，应制定、实施并持续维护不依赖（组织级）ICT的应急通信机制，并定期检验其有效性。例如，可采用移动通信替代网络通信，也可使用纸质表格来传递病理检查申请及结果。

5.43 HLT -外部事件报告

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#侦探， #纠正性	#完整性，#可用性	#回应	#治理, #威胁与漏洞管理#供应商关系安全，#法律与合规	#治理与生态系统

控制

适用于信息安全事件报告的法律、法规、监管及合同要求均应予以明确、记录并保持最新状态。

目的

确保履行与信息安全事件相关的法律、法规、监管及合同义务。

指导；建议

在医疗保健及其他领域，向监管机构或合同合作伙伴（**或两者**）报告信息安全事件的需求日益增长。这有助于相关方快速发现网络犯罪的规律。为确保履行此类报告义务，**应**制定一份明确的义务清单。基于此：

a) 应任命组织内的相关人员，负责（若干）单项报告的编制工作；

b) 每份报告的范围（长度与广度）应基于报告要求与个人（健康）信息保护之间的平衡来确定。

每次提交外部事件报告后，均应将此情况告知管理层。

其他信息

另见5.31。

6 人员控制

6.1 筛选

应遵循ISO/IEC 27002:2022标准第6.1节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

所有处理个人健康信息的组织均应制定人员筛查政策。该政策至少应要求核实相关人员的身份、现住址及既往就业情况。

所有拟聘任为工作人员的候选人的背景调查均应包括对其适用的卫生专业资格的核实；在适用情况下，还需确认其是否获得执业认证或执业许可。如适用，应进行犯罪背景调查。所有调查均应定期重复进行。

6.2 雇佣条款与条件

应遵循ISO/IEC 27002:2022标准第6.2节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

职位描述应明确说明处理个人健康信息所适用的安全职责与责任。

健康用途（补充）

确保对受照护者的隐私予以重视并予以充分理解。

健康指导

各组织应确保相关人员负有报告健康信息安全或患者隐私泄露事件的义务。

相关政策应涵盖所有类型的人员，无论其是否为正式员工，具体包括：

a) 临时或访视性质的临床人员，包括代班医师、培训医师、实习医师、学生以及“值班”或机构派遣的工作人员；

b) 提供直接护理支持的人员，包括行政及辅助工作人员、神职人员、慈善工作者及其他志愿者。

其他健康信息

有关卫生组织工作人员的更多信息，请参见附件C。

6.3 信息安全意识、教育与培训

应遵循ISO/IEC 27002:2022标准第6.3节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

认知、教育及培训可包括定期评估或测试，或两者兼有。

社会工程学威胁是医疗卫生机构尤为关注的问题。被冒充的人员示例如下：

a) 机构内部或外部的临床医生或其他医疗保健人员；

b)受照护对象的亲属或朋友；

c) 警察、社会服务人员；对于儿童而言，则包括教师及其他学校工作人员。

意识、教育和培训工作应充分考虑社会工程学的影响。
包括鼓励及时报告（参见6.8）社会工程攻击行为，无论其是否成功。

6.4 纪律处分程序

应遵循ISO/IEC 27002:2022标准第6.4节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

纪律程序应规定（既作为一种威慑手段，也因为这是必要的），对于严重的违规行为，**将向一个或多个外部机构举报有关个人。**

例如，可向临床医生的监管或注册机构报告其情况；学生和培训人员的情况可向其所属的学术机构报告。

6.5 终止或变更雇佣关系后的责任

应遵循ISO/IEC 27002:2022标准第6.5节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

许多医生、护士及其他临床医师会通过培训项目及其他“轮转”经历，其临床职责及所负责照护的对象可能发生根本性变化。

为确保终止其职务所需的所有访问权限及相关权利（这些权限与权利已不再必要），员工离职时的变更手续应首先按照离职员工的处理流程进行办理。

其他健康信息

就业变动也可能影响个人能够或被允许进入的实体场所。应制定相应安排，确保对安全通行证及其他实体与场所安保措施进行适当调整。

参见5.15和5.18。

6.6 保密协议或非披露协议

应遵循ISO/IEC 27002:2022标准第6.6节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

所有获授权访问个人健康信息的人员均应正式承诺对相关信息予以保密处理。

健康用途（补充）

正式维护员工或第三方可访问信息的保密性。

健康指导

例如，正式的约束力可以来自一份签署的协议，如保密协议、监管**要求**、或保密协议，也可以来自法律。

6.7 远程办公

应遵循ISO/IEC 27002:2022标准第6.7节规定的控制措施、相关属性表、目的、指导原则及其他信息。

其他健康信息

在医疗保健领域，远程工作可跨越司法管辖边界，甚至可在位于任何国家管辖范围之外的飞机和海上船舶上进行。临床医生通常会跨区域审阅医学影像等资料；参与灾害救援的国际团队亦可依赖其本国管辖范围之外的卫生信息系统。在设计和部署卫生信息系统时，必须充分考虑相关的法律、责任及伦理问题。

参见 ISO 13131。

6.8 信息安全事件报告

应遵循ISO/IEC 27002:2022标准第6.8节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应鼓励尽早报告实际发生的、疑似或潜在的安全事件。相关安排应确保相关人员无需担心受到责备或报复。组织还应考虑是否部署支持匿名报告的功能，并配备技术防护措施以保护举报者的身份信息。

当健康信息的不可用性或完整性丧失可能对患者的诊疗产生不利影响时，医疗机构应立即告知患者。信息安全事件可包括涉及数据处理或信息传输的患者安全事件。

当个人健康信息被不当披露时，相关机构应立即通知信息主体。在某些司法管辖区，法律对此有明确规定；而在多数司法管辖区，则有法律要求将涉及 PII 的数据泄露事件报告给个人信息遭泄露的数据主体。

6.9 HLT 管理培训

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的； #纠正性	#保密性，#完整性，#可用性	#保护，#响应，#恢复	#治理，#法律与合规，#信息安全保障	#治理与生态系统，#保护 #国防，#韧性

控制

组织管理人员应接受适当的培训，培训内容应与其在信息安全及信息安全管理方面的角色和职责相关。

目的

确保管理层能够履行其在信息系统管理体系（ISMS）方面的职责并承担相应责任。

指导；建议

根据本文件、ISO/IEC 27002及其他相关标准，组织管理层被赋予了多种角色与职责。应详细清单化这些具体角色与职责，随后开展差距分析，以确定所需开展的培训内容。

由于该组织管理团队的成员构成可能定期发生变化，上述步骤应根据需要重复执行。

管理培训应包含针对勒索软件攻击和数据泄露等网络事件的危机应对模拟演练。

其他信息

另见6.3。

7 物理控制

7.1 物理安全边界

应遵循ISO/IEC 27002:2022标准第7.1节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

许多医疗操作区域都涉及照护对象。与此同时，必须保障公众（包括照护对象及其陪同人员）的人身安全与安保，以及该环境中可访问的数据和系统的安全性。例如，即使诊室内设有正常运行的工作站，照护对象仍可能被单独留在检查室（例如以便更换检查服进行体格检查）。因此，医疗保健领域的工作站安全防护不能完全依赖于将照护对象排除在安全防护范围之外。

在医疗保健领域，可能存在患者（或其他相关人员）并非总是理性行事的情况。例如，这种情况可能出现在幼儿、存在心理健康问题者、近期遭遇令人痛苦消息的人、神经多样性个体、受药物或酒精等物质影响的人群等。相应的物理安全措施应充分反映这一特性。

在受照护者无法自行保障安全的情况下，应充分考虑其所属信息通信技术（ICT）设备（包括移动电话）的安全性。

针对数据和系统的物理安全措施，应与更广泛的物理安全及防护措施相协调。

7.2 物理入口

应遵循ISO/IEC 27002:2022标准第7.2节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

医疗服务的提供过程中存在特定情形，即公众（受照护者及其陪同人员）需实际进入正在处理敏感信息的区域。因此，用于收集健康信息的实体区域，以及配备可通过屏幕查看数据的系统的区域，均应采取额外的预防措施。

在某些情况下，个人健康信息会显示在屏幕上，且可能被无权查看该信息的人看到。例如，在患者入院的行政流程阶段，医护人员会向患者展示相关屏幕信息，而排队等候的其他患者也可能看到这些内容。另一个例子是病房内用于显示病房或病床分配情况的大型信息显示屏（屏幕或白板）。这类显示屏仅供临床及其他工作人员使用，但所有进入病房的访客均可查看。在此类情况下，应采取措施防止信息被未经授权的人员获取，例如通过调整这些显示屏的位置或布局来实现。

7.3 保护办公室、房间及设施

应遵循ISO/IEC 27002:2022标准第7.3节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

7.4 物理安全监控

应遵循ISO/IEC 27002:2022标准第7.4节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

7.5 防范物理和环境威胁

应遵循ISO/IEC 27002:2022标准第7.5节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

7.6 在安全区域工作

应遵循ISO/IEC 27002:2022标准第7.6节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

7.7 清理桌面和屏幕

应遵循ISO/IEC 27002:2022标准第7.7节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在提供相关设施的情况下，应确保暂停功能和自动登出功能得到正确配置。

在某些区域（如手术室和重症监护室）需要特别谨慎；出于安全考虑，可能有必要禁用暂停功能和自动登出功能。在此类情况下，应制定相应的规程，以防止在使用设备时发生未经授权的查看或其他操作。

确实无需使用设备。然而，仍需谨慎，因为即使无人值守或长时间未查看显示屏，设备仍可能处于运行状态。

7.8 设备选址与保护

应遵循ISO/IEC 27002:2022标准第7.8节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

配备健康软件的ICT设备和医疗器械，在其运行环境及操作过程中产生的电磁辐射方面，可能需要采取特殊的安全措施。医疗卫生机构（尤其是医院）应确保此类设备和器械的安装位置及防护措施能够最大限度地降低其暴露于这些电磁辐射的风险。

7.9 场外资产的安全性

应遵循ISO/IEC 27002:2022标准第7.9节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

医疗机构应确保所有在其场所外使用的、包含健康软件的医疗器械均获得授权。这包括远程工作人员使用的设备（即使该使用属于无限期范畴，例如救护车人员、治疗师等岗位的核心工作需求），以及接受照护对象使用的设备。

7.10 存储介质

应遵循ISO/IEC 27002:2022标准第7.10节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

存储在可移动介质上的所有个人健康信息均应进行加密。

健康用途（补充）

防止个人健康信息被滥用，包括未经授权的访问、披露或修改。

健康指导

最广为人知的可移动存储介质类型是安全数字（SD）卡和通用串行总线（USB）驱动器。

在许多情况下，身份识别模块（SIM）卡也是可拆卸的，并通常存储机密信息。除了手机外，平板电脑和笔记本电脑等设备也可配备SIM卡。SIM卡还广泛应用于其他场景，例如建筑及设施管理的远程监控系统、建筑安全报警系统以及机动车辆。

许多设备组件均配备内置存储单元，包括硬盘驱动器（HDD）、固态硬盘（SSD）及非易失性存储器。然而，此类存储装置的存在并不总是被明确记录、显而易见或预期之中。典型实例包括打印机（尤其是面向多台计算机或用户的联网打印机）、独立式复印机以及集成健康管理软件的医疗设备。

对任何含有储存功能的设备进行维护、修理及处置时，均需采取额外的预防措施。

其他健康信息

有关设备维护，请参阅7.13；关于设备的安全处置与重复使用，请参阅7.14；关于加密，请参阅8.24。

7.11 支持性公用事业

应遵循ISO/IEC 27002:2022标准第7.11节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

电力对**医疗保健的诸多环节至关重要，一旦停电**——尤其是某些医疗设备断电——可能对患者造成严重伤害。因此，许多医院及其他医疗机构都配备了应急电源系统，在主电源发生重大故障时，这些系统（通常通过专门设置的插座）能持续为关键医疗设备或信息通信技术设备供电。

应急电源可通过多种方式提供，但其供电质量并不总是与常规电源相同。例如，可能存在电压和频率波动或其他变化。在正常电源与应急电源之间进行切换（无论方向如何）时也会出现这种情况。因此，即使设备通过连接应急电源得到了保护，在某些情况下仍可能需要采取额外措施（例如使用专用不间断电源）。大量证据表明，当需要使用应急电源时，它们并不总能按预期运行——例如备用发电机发生故障或应急电源过载。因此，应针对此类情况制定相应的应急预案。

7.12 电缆安全

应遵循ISO/IEC 27002:2022标准第7.12节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应采取措施防止通过公共区域及其他场所的网络接口进行未经授权的访问。需考虑以下事项：

—禁用未使用的端口（例如位于配线架上的端口，或在可用的情况下，使用合适的网络管理工具进行禁用）；

—禁止对未事先获得授权的设备进行任何形式的访问（包括流量监控）；

一 使用入侵检测工具；

一 监测设备意外物理断开连接的情况——这可能表明网络电缆已被拔出，以便连接未经授权的设备。

网络插座同样容易遭受物理损坏。儿童及部分成年人可能出于无意或故意行为造成破坏。应采取预防措施，防止幼儿将物体或物质插入插座，尤其是在专为儿童设置的区域。

其他健康信息

其他物理安全考虑事项详见7.1。

7.13 设备维护

应遵循ISO/IEC 27002:2022标准第7.13节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在准备和执行所有设备维护活动时，均应考虑患者安全。

应制定确保设备维护安全可靠的政策。维护计划（**包括**最新的风险评估及应急安排）应按照相关规定制定。

相关政策。在进行维护之前，已完成的计划必须获得高级管理层的书面批准。

在所有情况下，均应采取相应措施，确保不会发生任何意外事件（尤其是中断，例如网络连接中断），这些事件可能影响依赖所维护设备的系统和设备。当维护工作由远程方式或第三方执行时，更需格外谨慎。

7.14 设备的安全处置或重复使用

应遵循ISO/IEC 27002:2022标准第7.14节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

几乎所有数字设备均配备某种形式的非易失性存储器，无论该设备是否内置（固态或机械）硬盘或可移动存储介质接口。这包括搭载健康管理软件的医疗设备。此外，非医疗设备（如打印机和网络设备）亦可记录或存储健康信息及其他机密数据（例如网络配置）。

医疗器械和设备可能有特定的处置规程。例如，可能需要进行去污及其他处理流程，以避免对健康造成后续风险。组织应确保医疗器械和设备的处置方案包含对储存介质的检查环节。

其他健康信息

有关存储介质的更多信息，请参见7.10。

8 技术控制措施

8.1 用户终端设备

控制措施、相关属性表、用途、指导原则及其他信息均遵循ISO/IEC 27002:2022标准第8.1节的规定。

其他健康信息

用户终端设备可以包括移动设备，例如智能手机、便携式医疗设备和可穿戴设备。

8.2 特权访问权限

应遵循ISO/IEC 27002:2022标准第8.2节规定的控制措施、相关属性表、目的、指导原则及其他信息。

其他健康信息

关于医疗保健领域特权管理的指导原则可参阅ISO 22600系列标准。

8.3 信息访问限制

应遵循ISO/IEC 27002:2022标准第8.3节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.4 访问源代码

应遵循ISO/IEC 27002:2022标准第8.4节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.5 安全认证

应遵循ISO/IEC 27002:2022标准第8.5节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

处理个人健康信息的系统至少应采用双因素认证。

健康用途（补充）

为确保获取个人健康信息的安全性得到进一步提升。

健康指导

在医疗信息系统允许访问患者全部或部分个人信息的情况下，应特别重视那些能够确保患者身份安全验证的技术措施。

还应考虑此类措施对于存在无障碍或其他问题的照护对象的使用便捷性。此外，还需充分考虑照护代理人的需求。

8.6 容量管理

应遵循ISO/IEC 27002:2022标准第8.6节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

能够或需要（无论是无线还是有线）连接至网络的医疗器械比例正在迅速增长，容量管理必须充分考虑这一趋势。还需考虑的其他因素包括：患者娱乐系统及访客网络的需求量可能处于较高水平且持续上升。

8.7 恶意软件防护

应遵循ISO/IEC 27002:2022标准第8.7节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在配备健康软件的医疗器械中，若可安装防恶意软件软件，则该软件可能干扰设备的安全运行。防恶意软件的安装或更新必须严格遵循 manufacturers ‘instructions 及本地政策规定。

在无法使用反恶意软件的情况下，应根据风险评估结果，在必要时实施相应的替代控制措施。

8.8 技术漏洞的管理

应遵循ISO/IEC 27002:2022标准第8.8节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

在大规模环境中，组织内部及组织之间的数据交换量可能非常庞大。这种数据交换可能通过多种不同的接口进行，涉及大量系统和设备，并采用多种技术。因此，必须对这些接口所导致的技术漏洞进行详细评估。

对于某些集成健康软件的医疗器械而言，出于临床安全考虑，无法或不宜采用与标准信息通信技术（ICT）设备相同的方式实施措施（如软件更新或补丁应用）。在无法进行软件更新或补丁应用的情况下，应根据风险评估结果在必要时实施相应的补偿性控制措施。

其他健康信息

更多信息见附件C。

8.9 配置管理

应遵循ISO/IEC 27002:2022标准第8.9节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

连接配置

为实现可互操作的电子健康记录，与组织内部及外部其他系统实现互操作的医疗信息技术系统，在初始配置时应遵循建议指南。同时，这些系统需持续维护，以确保在连接参数发生变化时（无论这些变化源于组织控制范围内的系统变更，还是组织外部因素导致的变化）仍能有效执行所采用的标准。

配置医疗设备

出于患者安全考虑，根据法律或当地政策要求，医疗器械的配置与维护通常必须由具备资质或执照的临床工程师/科学家负责。

许多集成健康软件的医疗设备能够与其他设备或健康信息技术系统交换信息。此类信息交换可通过永久性或临时性网络连接实现，也可通过直接连接等其他方式完成。相关接口通常由信息通信技术（ICT）专业人员负责管理；在某些情况下，这些专业人员还需支持特定医疗设备上的操作系统、系统实用程序、数据库软件及反恶意软件。

因此，临床工程师/科学家与信息通信技术（ICT）专业人士均可承担相应的职责（尽管职责内容有所不同）。同一设备的不同部件（或重叠部分）在配置管理中需予以充分考虑。

类似的考量原则也适用于医疗器械以外的领域。例如，某些用于输送医用气体的设备、患者呼叫系统以及建筑与设施管理系统通常都采用网络化架构，但其管理责任归属于具备资质或执照的工程师。承担此类管理职责的工程师往往并非临床工程师或科学家。

8.10 信息删除

应遵循ISO/IEC 27002:2022标准第8.10节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应考虑信息（暂时）存储在非组织管理的设备上的情况。此类情况的例子包括“自带设备”以及通过私人拥有的个人计算机访问信息。

其他健康信息

另请参阅7.10 和 7.14节，其中涉及存储介质以及信息应删除的具体情形。

8.11 数据掩码

控制措施、相关属性表、用途及其他信息均遵循ISO/IEC 27002:2022标准第8.11节的规定。

健康指导

ISO/IEC 27002中给出的指导原则适用，但“在实施数据掩码技术时应考虑”的条款中的b)和c)除外。对于健康领域，这些问题已在本文件5.34部分中予以阐述。

其他健康信息

有关医疗领域假名化的相关信息，请参阅 ISO 25237 标准。

8.12 数据泄露预防

应遵循ISO/IEC 27002:2022标准第8.12节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.13 信息备份

应遵循ISO/IEC 27002:2022标准第8.13节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康控制（补充）

个人健康信息应以加密格式进行备份。

健康用途（补充）

为保护个人健康信息的保密性。

健康指导

作为一项通用预防措施，尤其为了防范勒索软件攻击，应考虑采取以下措施：将备份数据离线存储或采用不可修改的备份技术。

其他健康信息

有关密码学的使用，请参见**8.24**。

8.14 信息处理设施的冗余性

应遵循ISO/IEC 27002:2022标准第8.14节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.15 日志

应遵循ISO/IEC 27002:2022标准第8.15节规定的控制措施、相关属性表、目的、指导原则及其他信息。

其他健康信息

关于电子健康记录审计追踪的指南可参阅ISO 27789标准。

8.16 监测活动

应遵循ISO/IEC 27002:2022标准第8.16节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.17 周期同步

应遵循ISO/IEC 27002:2022标准第8.17节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.18 特权实用程序的使用

应遵循ISO/IEC 27002:2022标准第8.18节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

正如8.9节所述，来自不同专业的人员可能对特定设备的不同方面承担（不同或重叠的）职责。关于特权实用程序使用的政策和程序应充分考虑这些问题。

8.19 在操作系统上安装软件

应遵循ISO/IEC 27002:2022标准第8.19节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

医疗机构提供的医疗服务可能涉及经过认证的硬件设备和软件系统，这些设备和系统需满足非常具体的配置参数才能确保安全运行。在某些情况下，认证要求禁止对软件堆栈的任何部分进行修改，包括安装安全补丁。**此类情况下，医疗机构应记录运营系统中存在的已知漏洞，以及为确保系统持续安全运行所采取的防护措施。**

8.20 网络安全

应遵循ISO/IEC 27002:2022标准第8.20节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.21 网络服务的安全性

应遵循ISO/IEC 27002:2022标准第8.21节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应考虑（临床）实践网络服务可用性丧失所产生的影响。另见5.29。

8.22 网络隔离

应遵循ISO/IEC 27002:2022标准第8.22节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

补丁更新、软件或固件升级，以及使用防恶意软件软件，都是有助于维护安全的技术手段。在某些情况下（例如，某些集成健康软件的医疗设备），这些技术的使用受到限制（参见附录C），因此需要采取相应的替代控制措施。其中一种用于保护易受攻击资产的控制措施是网络隔离。

通常建议对患者娱乐系统进行隔离。

其他健康信息

参见8.35。

8.23 网页过滤

应遵循ISO/IEC 27002:2022标准第8.23节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应制定相关政策，避免错误屏蔽与医疗保健相关的内容。这些政策应涵盖如何妥善处理误报。

默认情况下，网页过滤系统通常会屏蔽文本、图像、绘图、视频及其他类型的内容——这些内容在医疗保健领域完全适用，但在许多其他情境中却是不可接受的。此类内容涵盖范围广泛：除解剖学术语和图像外，还包括涉及药物滥用、暴力与自伤行为后果、儿童及弱势成年人受虐等相关内容。

假阳性结果可能影响医疗服务的提供，必须及时进行审查。相应地，存在以符合合法医疗目的为借口获取不适当材料的风险，因此应采取相应措施对此进行监控。

8.24 密码学的应用

应遵循ISO/IEC 27002:2022标准第8.24节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

其他健康信息

关于医疗保健领域数字证书的颁发与使用政策以及密钥管理的相关指南，可参阅ISO 17090-3标准。

8.25 安全的开发生命周期

应遵循ISO/IEC 27002:2022标准第8.25节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.26 应用程序安全要求

应遵循ISO/IEC 27002:2022标准第8.26节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应当考虑到以下可能性：个人健康信息未必会被明确识别为此类信息，至少也不会立即被识别。这种情况可能出现在涉及个人**医疗保健支付或报销资格的信息中。**特别值得关注的是那些可能推导出个人健康信息的情形，例如通过患者沟通相关的元数据。

其他健康信息

附录D可用于在应用程序开发或采购过程中评估安全要求。

8.27 安全的系统架构与工程原则

应遵循ISO/IEC 27002:2022标准第8.27节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.28 安全编码

应遵循ISO/IEC 27002:2022标准第8.28节中规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.29 开发与验收过程中的安全测试

应遵循ISO/IEC 27002:2022标准第8.29节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

应对计划中的新信息系统、升级版本及新版本制定验收标准。此类系统、升级版本及新版本应在验收前完成相应的测试。

临床相关系统功能的验收测试应纳入临床使用者参与。

8.30 外包开发

应遵循ISO/IEC 27002:2022标准第8.30节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.31 开发环境、测试环境和生产环境的分离

应遵循ISO/IEC 27002:2022标准第8.31节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

用于处理健康信息的系统开发与测试环境，以及培训环境，应与承载这些健康信息系统的生产环境分开设置。

应明确、记录并实施从开发阶段到生产阶段部署软件的规则与授权流程。

测试不得在生产环境中进行，也不得对个人健康信息实施测试。

8.32 变更管理

应遵循ISO/IEC 27002:2022标准第8.32节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

对个人健康信息处理方式作出不当、未经充分测试或错误的变更，可能对医疗服务的提供及患者安全产生不利影响。

变更流程应明确记录、评估并管理变更相关的风险。

8.33 测试信息

应遵循ISO/IEC 27002:2022标准第8.33节规定的控制措施、相关属性表、目的、指导原则及其他信息。

健康指导

实际个人健康信息不应被用作测试数据，但应采取措施确保测试数据具有真实性（例如参见8.11）。

8.34 审计测试期间的信息系统保护

应遵循ISO/IEC 27002:2022标准第8.34节规定的控制措施、相关属性表、目的、指导原则及其他信息。

8.35 HLT 零信任原则

控制类型	信息 安全性属性	网络安全概念	作战能力	安全域
#预防性的	#保密性	#保护	#信息安全，#系统与网络安全，#身份与访问管理	#保护，#防御

控制

分配到同一网络段的信息服务组、用户及信息系统应尽可能保持规模较小；且仅当两个相关网络段完成身份验证后，方可相互访问对方的网络段。

目的

确保默认情况下，连接到网络的实体不被信任。

指导；建议

零信任安全也被称为无边界安全。其核心理念是“永不信任，始终验证”，即信息服务、用户及信息系统默认不应被信任。

零信任原则通过以下方式实现：

a) 建立强大的身份验证机制；

b)在授予访问权限前验证设备合规性；

c) 确保仅对明确授权的资源进行最低权限访问；

d)双向认证，包括验证用户和设备的身份与完整性，且不受地理位置限制；

e) 基于系统/设备的身份及安全状态，并结合适当的认证机制，提供对信息系统和信息服务的访问权限。

其他健康信息

详见8.22。

附件A
(提供信息的)

医疗健康信息安全管理措施

表A.1中列出的信息安全控制直接源自第5至第8条中列出的控制，并与之保持一致，可在ISO/IEC 27001:2022,6.1.3的背景下使用。

若控制标题包含“HLT”，则该控制措施不适用于ISO/IEC 27001:2022标准的附录A。

若控制标题不包含“HLT”，则该控制措施是对ISO/IEC 27001:2022标准附录A中相应控制措施的补充。

表 A.1——医疗卫生领域的信息安全控制措施

子条款	控制标题	控制
5.1	信息安全政策	信息安全政策应明确信息安全的管理方法，并须获得最高管理层批准，之后至少每年进行一次审查，且在发生任何重大安全事件后也需重新审查。
5.2	信息安全角色与职责	至少应有一名专人负责信息安全工作。
5.9	信息及其他相关资产清单	所有信息流（包括组织内部及组织之间的信息流）及其接口（含集成平台）均应纳入清单范围。
5.11	资产返还	应制定一项政策，要求个人提供书面确认，证明其持有的所有存款中的资产均已妥善归还或酌情予以删除。
5.12	信息分类	个人健康信息至少应被归类为机密信息。
5.14	信息传输	在任何转让发生之前，必须制定相应的规则、程序及协议。
5.15	访问控制	个人健康信息的访问权限应由适当的政策（如基于角色的访问控制）进行规范。
5.16	身份管理	需获取个人健康及其他机密信息的用户，必须经过正式的注册流程。
5.19	供应商关系中的信息安全	应评估外部人员访问系统或其所含数据所带来的风险，并根据所评估的风险实施相应的控制措施。
5.38	HLT -信息安全 需求分析与规范	与信息安全相关的要求应纳入新信息系统的开发要求或现有信息系统的改进要求中。
5.39	HLT -唯一识别照护对象	应制定相关政策和程序，确保每位受照护对象拥有唯一的唯一标识符，并具备在同一受照护对象存在重复或多条记录时进行合并的功能。
5.40	HLT 显示/打印数据的验证	当个人任何健康信息被显示或打印时，必须包含能够安全识别受照护对象的信息。
5.41	HLT -公开可获取的健康信息	公开可获取的健康信息在其整个生命周期内均应受到保护、具备可追溯性、得到妥善保存和管理。

表A.1（续）

子条款	控制标题	控制
5.42	HLT -紧急通信	在信息通信技术（ICT）中断时，卫生组织内部的应急通信系统应当经过规划、实施、维护及测试。
5.43	HLT -外部事件报告	适用于信息安全事件报告的法律、法规、监管及合同要求均应予以明确、记录并保持最新状态。
6.2	雇佣条款与条件	职位描述应明确说明处理个人健康信息所适用的安全职责与责任。
6.6	保密协议或非披露协议	所有被授权访问个人健康信息的人员均应正式承诺对相关信息予以保密处理。
6.9	HLT 管理培训	组织管理人员应接受与其信息安全职责及管理方式相适应的适当培训。
7.10	存储介质	存储在可移动介质上的所有个人健康信息均应进行加密。
8.5	安全认证	处理个人健康信息的系统至少应采用双因素认证。
8.13	信息备份	个人健康信息应以加密格式进行备份。
8.35	HLT 零信任原则	分配到同一网络段的信息服务组、用户及信息系统应尽可能保持规模较小；且仅当两个相关网络段完成身份验证后，方可相互访问对方的网络段。

附件B
(提供信息的)

本文件与 ISO 27799:2016 的符合性

本附录旨在为当前正在使用ISO 27799:2016标准并希望过渡至本版本的组织提供向后兼容性。

表 B.1列出了本文件第5条至第8条中规定的健康控制措施与 ISO 27799:2016 中相应内容的对应关系，应结合 ISO/IEC 27002:2022 的附录 B 一并使用。

表B.1——本文件与ISO 27799:2016中健康 HLT 对照项的对应关系

ISO 27799:2025 控制标识符	ISO 27799:2016 控制标识符	控制名称
5.38	14.1.1	HLT -信息安全需求分析与规范
5.39	14.1.1.1	HLT -唯一识别照护对象
5.40	14.1.1.2	HLT 显示/打印数据的验证
5.41	14.1.3.1	HLT -公开可获取的健康信息
5.42	新的	HLT -紧急通信
5.43	新的	HLT -外部事件报告
6.9	新的	HLT 管理培训
8.35	新的	HLT 零信任原则

附件C
(提供信息的)

医疗机构的信息安全

C.1 引言

本附录概述了医疗保健领域中若干信息安全方面的考量要点。其主要用途包括：

—信息安全专家，包括渗透测试人员及其他具备信息通信技术（ICT）专业知识但不熟悉医疗健康领域的专业人士，例如审计师；

一 在卫生组织工作的医疗设备、工程和信息通信技术专业人员，因此，他们可能需要负责设备、依赖数字技术的系统或服务。

本文档引言部分简要阐述了健康软件及健康信息技术系统在整个生命周期中安全性、保障性与有效性相互依存这一重要主题。该主题在此未作深入探讨，但已在ISO 81001-1及相关IEC标准中得到全面阐述。

C.2 医疗器械和设备的安全性

C.2.1上下文

未能按预期功能运作的医疗器械及其他医疗设备，可能对患者或其他受照护对象造成伤害。

根据具体情况，伤害可能立即显现，也可能在一段时间后才显现。某些伤害事件仅影响一个人，而另一些则可能影响多人。

在最严重的情况下，此类事件可能导致死亡。然而，当事件引发不可逆转且终身性的痛苦等后果时，对个人及他人（如家庭成员）而言也可能造成毁灭性影响。此外，若此类伤害导致需要全天候（24小时）护理，则其经济负担将极为沉重。

为最大限度降低危害风险，所有类型医疗器械（其中许多并不依赖数字技术）及相关设备的整个生命周期均经过严格标准化和全面监管。

C.2.2 专业责任与问责制

一旦医疗设备在医疗机构中投入使用，就必须确保所有类型医疗器械的安全性。这一职责通常由临床工程师、临床科学家、生物工程师或（特别是在涉及电离辐射时）医学物理师等专业人士承担。这些角色的具体名称与职能定位，以及他们之间的职责划分，取决于所涉及的医疗器械类型、相关法规要求及当地政策规定。然而，总体而言，履行这些职责的人员在此均统称为医疗器械专业人员。

同样地，在医疗机构中，建筑设施及建筑管理系统通常由工程专业人员负责，这类人员通常被称为医院工程师。本文亦采用此称谓。在某些医疗机构中，医院工程师还负责所有医疗设备的管理工作。

在卫生以外的许多部门，信息通信技术或类似部门的专业人员通常负责管理依赖数字技术的资产，这项职责可包括信息安全。

然而，医疗器械专业人员和医院工程师的职责可涵盖信息安全的多个方面。其所在部门通常会收到依赖数字技术的设备制造商提供的指导文件，其中明确了相关的信息安全措施以及需要实施的具体任务或活动。

根据资产类型的不同，这些任务可能包括：补丁安装、软件或固件升级、配置修改、更新防恶意软件保护程序等。在执行上述任务前，通常需要将相关资产（安全地）从服务中撤出；完成后需将其重新投入运行。此过程可能涉及测试、重新校准或其他仅限专业人员执行的操作。

许多由医疗器械或医院工程专业人员负责管理的资产均依赖（有线或无线）网络进行连接，或通过终端用户设备（如个人电脑、笔记本电脑或其他移动设备）进行访问。此外，集成健康软件的医疗器械制造商可能要求网络及终端用户设备（包括运行于其上的应用程序）按照特定方式配置，以支持医疗器械的正常运行或满足信息安全需求。

然而，网络架构与终端用户设备的运维通常由信息通信技术（ICT）专业人员负责。因此，信息安全职责可能存在重叠，所有专业团队必须协同开展工作。这种协调对于确保某些设备和系统的信息安全措施不会因其他专业团队负责而被忽视至关重要。

C.3 资产所有权与组织义务

C.3.1总则

识别所有采用数字技术且被医疗机构使用或依赖的资产至关重要。明确所有使用数字技术资产的责任归属与问责机制同样不可或缺。

特别是在大型医疗机构中，由于资产数量庞大且频繁移动或发生其他变化，库存管理可能变得十分复杂。

以下小节概述了若干相关因素。

C.3.2 信息通信技术与医疗设备

C.3.2.1 资产来源与获取

根据医疗机构的性质，采用数字技术的资产可通过多种方式进入该机构。其中部分方式可能属于非正式途径。

在医疗机构中部署并运用数字技术的资产包括：

一 由其购买；

——由其雇佣、租赁或承租；

作为合同服务的一部分提供给 一 ；

——向其提供贷款——例如来自医疗器械制造商或制药公司，用于直接评估或支持临床试验所需物资；

—向其捐款——例如由慈善基金会提供；

一 强加于它；

一 在其内部开发、建造或构筑的；

—共享。

此外，卫生组织的某些部门或单位可享有相当大的自主权。这一原则适用于地理分布分散的组织；同样适用于大型卫生组织——在这些组织中，特定部门或临床专科组被授权无需获得组织内任何中央或企业职能部门的批准或监督，即可采购并实施至少部分采用数字技术的资产。

C.3.2.2资产共享及其他类型的组织

一个卫生组织可以与其他卫生相关组织（或其内部部门）建立关联，包括：

一 为现有及有志成为（即学生、培训学员等）卫生专业人员提供教育与培训的医学院及其他机构；

一 临床研究单位和机构；

一 其他从事临床、医学或健康相关研究的学术机构；

一 大学院系（例如工程学、物理学和计算机科学）研究或开发以下一项或多项技术、设备、装置及软件，以改进医疗保健领域的数字化解决方案。

那些采用数字技术且由这些其他组织拥有或控制的资产，在某些情况下会与卫生组织共享；而在另一些情况下，此类资产仅由卫生组织独家使用。

相应地，该卫生机构中采用数字技术的部分资产可与其他组织或其相关部门共享。

尽管在这些共享场景中维护资产的信息安全更具挑战性，但这一点至关重要；同时，确保明确由哪个组织承担相应责任，也是关键因素。

C.3.2.3其他资产流量

特别是当患者需要在其他医疗机构接受更专业的诊疗时，可紧急在不同医疗机构之间转诊患者。在此类情况下，某些设备（包括配备健康软件的医疗设备）亦可随患者一同转移。

在其他情况下，受照护对象可临时或永久获得配备健康软件的医疗设备，以便在其不再处于医疗机构场所时使用。例如，这适用于监测设备或植入式设备。

C.3.2.4由员工或护理对象拥有的资产

根据具体用途，员工或受照护对象拥有的某些资产需要纳入资产清单。例如，当需要执行软件许可规定或必须能够远程擦除设备数据时，即适用此规定。

C.3.3建筑与设施管理系统

医疗卫生机构可采用多种运营场所。部分场所由所在机构拥有或控制，但情况并非总是如此。例如，医疗卫生机构可能使用多功能建筑（包含办公、零售或兼具两种功能），或与其他医疗卫生机构共享场所（如门诊诊所）。

在并非完全由卫生机构控制的场所内，必须对设施及建筑管理系统实施必要的信息安全活动，并明确哪些部门负责监督或执行这些活动：

这种情况可能相当复杂，尤其是在建筑物管理权已由业主或房东委托给一个或多个第三方的情况下——这些第三方又可进一步进行分包。如果建筑物由多个不同方（如业主或房东、管理机构、租户或其他使用者）共同管理，也会引发复杂问题。

C.4 人民

C.4.1 系统及信息用户

C.4.1.1 总则

与以下因素有关：

一 身份管理、身份验证信息及基于角色的访问控制；

一 制定政策和程序；

一 政策与程序的沟通与执行；

一 意识、教育和培训；

——风险评估与管理。

部分因素将在以下小节中详细阐述。

C.4.1.2 卫生人力资源

医疗卫生 workforce包含多种角色，具体包括：

—医生、牙医、药剂师、护士、助产士、物理治疗师、急救人员；

——医疗助理、技术人员、医疗秘书、临床编码员；

一 行政、财务、文秘及支持人员；

一 志愿者、神职人员、慈善工作者。

医疗机构中的工作人员可包括以下一种或多种身份：

一 经理或主管；

— 全职或兼职；

——身兼多重角色（例如同时担任医生、学术研究员或教育工作者）；

一 在其他医疗机构任职或工作（定期或临时）。

个人可进入劳动力市场的依据包括：

一 长期合同；

——短期或临时合同；

一 借调或安排；

—职位；

一 代理机构工作人员（由外部机构提供）；

—银行员工（来自组织内部的人员池）；

—访问（有时是为了获取“第二意见”）专家或顾问。

在获得完全专业资格之前，个人可作为学生、培训生或实习生参与劳动力市场。

部分员工仅在标准办公时间之外工作。为应对突发缺勤情况，某些员工可能仅需在其他病房或科室工作数班甚至仅工作一班。

虽然许多医疗保健人员仅在医院等固定场所工作，但仍有大量临床医生在社区工作，为居住在自己家中或养老院、护理院等其他住所的居民提供医疗服务。

所有这些劳动力因素均具有多重影响，包括确保：

——个人健康信息仅限于具有合法访问需求的劳动力成员查阅；

一 对系统的访问权限得到正确管理。

为避免方案变得难以管理，有时必须做出某些妥协。

ISO 21298进一步探讨了其中部分因素，并列出了医疗领域受监管的专业角色清单。

C.4.1.3照护对象及其代理人

受照护对象（及其代理人）可获得其个人健康信息的访问权限。在某些情况下，用户可直接访问健康信息系统；而在其他情况下，其个人健康信息需通过应用程序进行访问。

问题包括：

——确保检索或下载的信息在所使用的设备上保持安全；

——赋予用户更新个人健康信息的能力所带来的影响，不仅包括直接输入信息，还包括通过以下方式上传信息：

—健康、福祉或健身设备（可属于健康机构或用户）或应用程序；

——来自其他医疗机构的记录，其中记录了接受治疗的患者信息；

一 需照护的对象包括：儿童、存在无障碍需求或学习障碍者；

一 不得限制照护对象查阅其自身记录中的任何信息；

——护理对象希望对其授权代理人可访问的内容及访问方式所施加的限制，以及这些限制的管理方式；

——如何管理代理用户作为用户的授权权限，以及护理主体能否对此进行控制的程度。

C.4.1.4 其他用户

其他可能需要或有权访问个人健康信息及其他机密信息的用户，以及存储此类信息的系统，包括监管与检查机构人员、保险公司代表、财务及其他审计机构人员、医疗专业人员，以及调查临床或其他事件的相关人员。为开展犯罪调查，警方及其他执法机构亦可获得个人健康信息的访问权限。

即使其他类型的用户持不同观点，也不总是适合允许他们无限制地获取有关特定护理对象或其他个人（例如劳动力成员）的信息。

C.4.2.1 目标

由于信息安全对医疗机构的影响极为广泛，设立信息安全咨询小组（此类小组亦可称为董事会、委员会或论坛）将大有裨益。

该小组的目标可能包括：

——确保为信息安全工作制定明确的方向，并获得管理层的切实支持；

— 及时向用户通报其需关注的信息安全问题（例如新型网络钓鱼手段或恶意软件威胁）；

——从组织内部及外部的信息安全事件及险些发生的安全事故中汲取经验教训；

- 协调开展针对劳动力群体的意识提升、教育及培训工作——不仅面向新入职人员，也包括对现有员工的培训与知识更新；

一 就拟议的变更提供咨询，因为这些变更可能影响临床实践、业务流程或两者兼有；例如，缩短会话无操作超时时间或重置大量密码可能会产生意想不到的后果，例如在临床紧急情况下阻止或延迟系统访问，或导致界面故障。

C.4.2.2 会员资格

最佳做法是确保集团内部始终有来自最高管理层及组织信息安全专家的代表。可代表的利益相关方取决于组织的类型、规模及其健康状况（即运营状况）。这些代表可能包括：

一 临床医生及其他直接参与患者诊疗工作的医护人员；

一 学术、教学和研究人员；

一 其他使用不同系统的非临床工作人员，通常来自财务、人力资源、采购/物资供应、新闻与传播等部门。

不同临床专科的临床与业务流程以及所使用的系统可能存在显著差异。因此，为在大型组织中获得更全面的视角，由来自多个临床专科的成员参与讨论小组将大有裨益。同时，让部分初级员工、培训学员或学生参与讨论也十分必要——因为他们的经验以及对各类信息和系统的熟悉程度，与资深员工或管理层可能存在显著差异。

C.4.3 技术岗位与协调工作

如前所述，**医疗器械**、医院工程及信息通信技术（ICT）领域的专业人士可能负责信息安全的多个方面，因此需要协调各方工作。

然而，在其他团队或专业领域中，也可能存在承担技术信息安全职责的人员，例如负责安装补丁和更新软件。这些人员通常担任专业临床或部门系统的系统管理员或系统管理者。因此，他们的日常职责可能包括授权系统用户、执行备份等操作。具体示例如下：

— 病理学实验室分析仪及相关设备可配备实验室信息系统。此类系统通常通过接口导出检测结果，仅限实验室工作人员直接访问该系统。系统管理员通常为相关部门成员，可以是病理学家或实验室经理。

一 医院物理安保部门的工作人员可能负责管理各类系统，例如身份卡与安全通行证系统、门禁系统、入侵报警系统及监控系统。

因此，部门系统管理人员或其他能够执行技术信息安全任务的人员，与组织整体信息安全专业人员之间进行协调至关重要。

另一个影响信息通信技术（ICT）与医院工程部门的领域是支撑ICT的建筑基础设施。该领域可能存在职责重叠的情况，反之亦然——通常会出现（通常是无意的）覆盖空白。此类基础设施包括网络布线、配线架、网络插座、通信机房、计算机机房以及不间断电源。

C.5 资产类型及用途

C.5.1 总则

以下小节列举了多种运用数字技术的资产类型实例。由于此类资产种类极为广泛，所举实例无法面面俱到。这些示例旨在提供框架性检查清单，并强调采用严谨的方法可确保库存清单中不遗漏任何资产。

C.5.2 信息通信技术与物联网

C.5.2.1 通用设备与服务

与许多其他领域一样，医疗领域广泛采用了通用信息通信技术（ICT），以及日益普及的物联网（IoT）技术。

一个值得关注的领域是患者娱乐系统，这类系统可在病床旁提供电视及流媒体服务。这些系统通常会对医院网络产生极高的负载，其流量甚至超过所有其他网络流量之和。此外，当大量用户同时试图访问同一广播内容时（例如在重大新闻或体育赛事期间），对这些系统的流量需求可能急剧攀升。

C.5.3 医疗设备

医疗器械可根据多种不同方式进行分类或归类。下文所列包含健康软件的医疗器械的分组及排列顺序并无特殊意义：

一可植入设备，例如起搏器和除颤器；

—影像设备：数字放射成像（DR）及其他基于X射线的设备、CT（计算机断层扫描）扫描仪、MRI（磁共振成像）扫描仪、超声扫描仪、内窥镜设备；

一 麻醉机；

— 血液透析机；

—放射治疗设备；

一 手术机器人；

一呼吸机；

一 外置除颤器；

一 临床/病理实验室分析人员；

一 输液泵、注射器驱动器；

一 床旁检测设备；

一 监测与诊断设备，包括用于测量以下指标的设备：体温、心率、呼吸频率、血压、血氧饱和度、血糖水平、心电图（ECG）和脑电图（EEG）。

所列出的许多设备通常仅存在于专门用于医疗保健的场所或地点（如医院、诊所、诊断中心、临终关怀机构和护理院）。然而，一些配备健康软件的医疗设备也常见于移动拖车单元（尤其适用于某些类型的影像设备）和船舶。急救服务使用的救护车及其他交通工具（如直升机）同样配备了搭载健康软件的医疗设备。

C.5.4 建筑与设施管理

C.5.4.1通用设备和服务

提供医疗服务的场所通常配备有系统、设备及机械装置，这些设施分布于多种类型的建筑中且具有通用性。此类通用设备可提供以下功能：

一供暖、通风与空调（HVAC）及环境控制系统；

——火灾探测与扑救；

一照明控制系统，例如包含 occupancy感测功能；

一 能源管理；

一 数字标牌及公共广播系统。

C.5.4.2 物理安全系统

医疗机构可配备通用安全系统，例如：

一 门禁控制及门禁系统；

一 监控系统，包括安全摄像头；

一 入侵检测与报警系统；

一为劳动者配备个人警报器和随身摄像头。

C.5.4.3 专用健康设备

适用于医疗领域的专用设备（其中部分被归类为医疗器械）以及专用于医疗建筑的相关系统包括：

一医用气体及真空设备，包括监测仪和报警器；

一冷藏与温控储存（适用于血液制品、药品、病理样本等）；

一永久安装的灭菌器（亦称高压灭菌锅）；

一护士呼叫系统及类似警报系统，以及其他床边服务。

C.5.5 个人健康信息的用途

C.5.5.1总则

全面审查医疗机构中个人健康信息的使用或处理方式，有助于既识别采用数字技术的资产，又确认信息库存的完整性。

C.5.5.2处理个人健康信息的目的分类

ISO/TS 14265 对个人健康信息处理的目的进行了详细分类。该分类体系最高层级的主要条目如下：

a)以患者为中心的照护流程，直接或间接促进个体的健康与照护；

b) 卫生服务管理和质量保证——利用**个人的个人数据来监测和提高**对广大人群**的卫生保健服务的质量、安全性和公平性**的流程；

c) **人口与公共卫生——**加工个人**健康数据，以追踪公共卫生问题，**管理对个人和人群的公共卫生风险，并制定有效策略；

d)临床研究——指临床试验的设计与实施、真实世界数据研究以及其他涉及个人健康数据处理的知识生成活动；

e)教育与培训：处理个人健康数据，用于开发教育与培训材料、开展教学活动或评估学习效果；

f) 遵守法律义务——按照法律法规或司法指令披露或处理个人数据。

C.5.5.3记录生命周期事件

除考虑处理个人健康信息的总体目的外，还可审查对记录可能采取的行动，以识别采用数字技术的资产并确认库存的完整性。

ISO/TR 21089规定了以下记录生命周期事件：访问/查看、添加法定保留、修订（更新）、归档、验证、解密、去标识化。 （匿名化）、淘汰、销毁/删除、披露、加密
提取、链接、合并、创建/保留、匿名化、重新激活、接收/保留、重新识别、移除合法的
持有，报告输出、恢复、转换/翻译、传输、解除链接、解合并、验证。

这些事件也是ISO 27789标准规定必须记录在审计日志中的内容。

C.5.6 健康及其他应用

C.5.6.1 卫生组织

提供医疗服务的医院及其他场所可配备多种健康信息技术系统（其名称可能有所不同），这些系统主要用于直接医疗服务目的，具体包括：

一 电子病历（EPR）系统；

一患者管理系统（PAS）；

一 图像归档与通信系统（PACS）；

一 实验室信息管理系统；

——放射学信息系统（RIS）；

一 药房/配药系统；

— 针对特定专科的临床系统（大型医疗机构中此类系统往往十分丰富），例如产科、心脏病学或眼科；

一 部门系统，例如剧院、无菌耗材或感染控制系统；

一 接口引擎。

这些系统可提供多种功能，包括：存储健康记录、临床决策支持，以及预约、咨询和手术的排程与预订。

根据ISO/TS 14265中对用途的分类可知，处理个人健康信息的系统还可有多种类型。此外还包括文档与内容管理系统、网站、内联网等；以及用于行政管理、财务管理、员工考勤管理、教育培训（含学习管理系统和虚拟学习环境）、零售服务（如员工及访客茶点供应）等其他用途的系统。

关键在于，根据不同的医疗机构类型，其系统和数据库的数量可能出乎意料地庞大，其中许多系统存储着个人健康信息或其他机密数据。特别是在大型教学医院中，有证据表明此类系统可能多达数百个。

展望未来，采用人工智能（AI）、基因组信息或两者结合的系统应用必将显著增加。

C.5.6.2 资产与人员跟踪

采用RFID（射频识别）标签、条形码或其他技术的资产追踪与管理系统可用于多种用途，包括定位医疗设备、药品分发以及管理耗材、血液制品或手术器械的库存。对病理样本使用条形码的做法非常普遍。

某些健康组织会追踪其部分员工的行踪。此举出于多种原因，例如业务流程分析与优化。在社区工作的临床医师亦会接受行踪追踪，以保障其人身安全。

医院住院患者通常佩戴身份识别腕带，这些腕带可带有条形码。部分医疗机构会对特定护理对象采用追踪技术，例如：

—因患有痴呆症或其他疾病而可能迷失方向或出现定向障碍的个体；

—新生儿（若从指定区域转移，系统将触发警报以防止被绑架）。

C.5.6.3 应用程序

健康、福祉及健身应用程序已日益普及。其中部分应用程序专为与其他产品配合使用而开发，例如便携式医疗设备、健身监测器、可穿戴设备等。

一些健康组织会为患者或其工作人员开发或授权应用程序。然而，许多健康类应用程序的获取方式（通常来自“应用商店”）与其他类型的应用程序并无二致。

某些健康相关应用程序具有积极作用。然而，许多健康相关应用程序存在安全、隐私或安保风险，且这些风险往往同时存在。

C.5.7接口

关于患者护理信息通常存储在相互连接的医疗信息技术系统中（这些系统可能包括集成**医疗软件的医疗设备、中间件、**多个数据库等）。为实施护理或其他目的，需共享或交换大部分此类信息；通常采用接口来传输相关数据。

组织内部及组织之间的接口都可能带来多种不同的安全与隐私风险。因此，必须将所有此类接口纳入资产清单。

某些接口采用专有协议和数据格式。然而，医疗信息技术系统以及集成健康软件的医疗设备具有异构特性，因此接口（尤其是不同制造商产品之间的接口）通常采用统一标准来交换健康信息。

最常被指定和使用的健康信息交换标准如下：

一 HL7 2.5 版本，具体要求遵循 ISO/HL727931 标准；

一 HL7 FHIR（快速医疗互操作性资源）；

一 符合 ISO 12052 标准规定的医学数字成像与通信（DICOM）规范；

一ISO/IEEE11073系列。

由IHE（整合医疗保健企业）开发的Dicom和HL7标准规范也十分普遍。

附件D
(提供信息的)

健康信息系统安全与隐私要求示例及其与ISO 27799控制措施和IEC/TS 81001-2-2安全能力的对应关系

D.1 目的

本附件提供了示例性的安全与隐私要求，这些要求可：

— 从安全与隐私角度，指导健康软件产品及信息系统采购、升级与评估工作；

——协助实施本文件所规定管控措施与指导原则的组织，共同制定信息隐私与安全政策、法规、指南、协议及操作流程；

——推动在医疗信息技术系统全生命周期中实施安全管控措施。

本文件中的示例安全与隐私要求源自 ISO/TS 14441:2013 标准，该标准现已由本文件取代并废止。本文件中示例要求的编号与 ISO/TS 14441:2013 中保持一致，但相关要求本身已进行了修订和更新。

以本附件作为评估依据的组织可根据自身流程的具体情况，对建议的要求进行相应调整。此外，本附件阐明了健康信息系统中这些示例性安全与隐私要求与本文件所规定控制措施之间的对应关系，并提供了与IEC/TS 81001-2-2:2025标准中所述安全能力的对照对照。

IEC/TS 81001-2-2:2025 提供了一套信息丰富的通用、高层次安全相关功能，这些功能需在整个医疗软件和医疗信息技术系统的生命周期中使用，以实现医疗器械制造商、医疗软件制造商、医疗提供机构和/或其他利益相关方之间的信息交换。这些安全功能详见表D.1。

表 D.1——IEC/TS 81001-2-2:2025 第 5 条中描述的安全功能

子条款	能力	缩写词
5.2	自动注销	ALOF
5.3	审计控制	AUDT
5.4	授权	授权
5.5	网络安全产品升级	CSUP
5.6	健康数据去标识化	DIDT
5.7	数据备份和灾难恢复	DTBK
5.8	紧急通道	电磁辐射发生器
5.9	健康数据的完整性和真实性	IGAU
5.10	恶意软件检测/防护	MLDP
5.11	节点认证	NAUT
5.12	人员身份验证	PAUT
5.13	产品的物理锁	PLOK
5.14	产品生命周期路线图中的第三方组件	RDMP
5.15	系统与应用程序加固	SAHD
5.16	健康数据存储保密性	STCF
5.17	传输保密性	TXCF
5.18	传输完整性	TXIG

D.2 观众；听众

尤其能从本附件信息中获益的组织和个人包括以下两类：

—负责健康软件及健康信息技术系统的供应、采购、配置、集成与实施；

—负责从隐私与安全角度出发，规划、部署及测试医疗信息技术系统。

D.3 映射表

示例中的安全与隐私要求与本文件所述控制措施之间的关系属于多对多关系。为简化映射操作，这些关系被分别呈现于两个表格中，每个表格均包含一组一对多关系。

—表 D.2：示例安全与隐私要求与本文件中控制措施之间的对应关系，以及与 IEC/TS 81001-2-2:2025 中安全能力的附加映射。制造商还可参阅 IEC/TS 81001-2-2:2025 的附录 A，了解医疗器械制造商如何通过该映射获益的具体示例。该信息性附录包含一个展示安全信息交换的示例场景，分为两部分：引言和医疗器械安全制造商披露声明（MDS2）示例。

—表 D.3：本文档中的控制措施与示例安全及隐私要求之间的关系。

表 D.2——示例安全与隐私要求、IEC/TS 81001-2-2:2025第5条款中的安全能力与本文件控制措施之间的关系

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
数据主体对收集、使用或披露个人健康信息的同意		
R1 记录同意：当数据主体根据法律或惯例有权拒绝或撤销其对收集、使用或披露其个人健康信息的同意时，适用于健康信息系统： a)应提供一种机制，用于记录数据主体的同意指令，包括同意的保留或撤销； b) 应能够以一种方式实现这一目标，使每个组织都能遵守其自身的关于知情同意的法律或政策要求； **R2 最低记录数据要求：**当健康信息系统记录数据主体的同意指令时，必须记录该指令的具体内容（例如拒绝同意或撤销先前已给予的同意），以及在承认两种及以上同意类型的司法管辖区中应记录的同意类型（例如默示同意与明示同意），同时记录指令下达日期。**R3 指令应随数据一并记录：**若数据主体根据法律或习俗有权拒绝或撤销对其个人健康信息收集、使用或披露的同意，健康信息系统应提供一种机制，可在披露数据时同步传输对后续（即后续）披露的限制条款——尤其当数据接收方无法通过其他方式知晓并遵守数据主体的同意指令时。健康信息系统应能以符合发送方与接收方各自法律要求或同意政策的方式实现这一功能。 **R4 紧急访问权限：**紧急医疗护理（例如对失去意识的受照护者提供的护理）或法律或政策允许的其他特殊情况（例如传染病暴发期间的公共卫生调查），可能需要访问存储在健康信息系统的患者记录；在此情况下，法律或政策允许在事先记录的同意指令基础上进行部分合规访问。此类紧急访问权限仅应提供给授权用户，且其访问操作（连同用户 override 同意指令的原因）必须记录在审计日志中。除非法律或政策允许部分 override 同意指令，且为消除用户是否意图 override 受照护者同意指令的不确定性，系统应允许用户明确调用紧急访问权限；或者，在授予访问权限前，系统应告知访问用户该访问属于紧急访问。 **R5 应急记录访问：**健康信息系统应具备以下功能： a)当处理同意指令时禁止披露数据的情形； b)记录任何覆盖数据主体同意指令的用户的身份、紧急访问的原因、可后续用于识别数据主体的唯一标识符，以及紧急访问发生的时间和日期； c) 向负责确保隐私合规的人员发出紧急访问通知。 **R6 法定授权代表提供的同意：**当法定授权代表代表照护对象作出同意指示时，健康信息系统应能够记录该授权代表的身份及其与照护对象的关系。 **R7 报告知情同意变更：**对于任何特定受照护对象，健康信息系统记录的知情同意指令应能够显示在任何特定时间点生效的知情同意指令（如有）及其变更时间。	AUDT 授权 DIDT 电磁辐射发生器 IGAU NAUT PAUT STCF TXCF TXIG	5.1 信息安全政策 5.2 信息安全角色及责任 5.15 访问控制 5.20 在供应商协议中解决信息安全问题 5.33 记录保护 5.34 PII 隐私与保护 8.15 日志 8.16 监测活动

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
限制使用和披露		
R8 仅记录和存储那些具有明确收集、使用或披露目的的数据：个人健康信息仅应用于与其收集目的一致的目的。 R9**限制向与数据主体存在业务关系的医疗保健提供者披露数据主体信息：**应在记录中注明（例如拒绝提供知情同意或撤回先前已给予的同意），同时明确在承认两种及以上同意类型的司法管辖区中同意的性质（例如默示同意与明示同意），以及下达该指令的具体日期。**R10 限制数据出口：**健康信息系统之间以电子或印刷格式进行的数据传输，仅限于明确规定的用途，例如临床诊疗、数据备份，或应数据主体（或其代理人）要求进行的数据传输。	AUDT 授权 DIDT 电磁辐射发生器 NAUT PAUT STCF TXCF TXIG	5.1 信息安全政策 5.12 信息分类 5.13 信息标注 5.15 访问控制 5.20 在供应商协议中解决信息安全问题 5.33 记录保护 5.39 唯一识别护理对象
数据主体对个人健康信息的访问及信息更正		
R11 数据主体访问：当数据主体对自身记录中信息的完整性或准确性提出质疑，且组织不同意数据主体关于信息不完整或不准确的评估时，健康信息系统应能够记录该异议或拒绝更新记录的理由，或同时记录两者。 **R12 可访问性：**健康信息系统应能够以患者（包括残疾人士、存在功能障碍或感觉丧失者）可阅读的格式输出或显示个人健康信息。	IGAU STCF	5.12 信息分类 5.13 信息标注
数据准确性		
R13 准确性：健康信息系统应包含相关措施，以确保个人健康信息在用于其预定目的时具有必要的准确性和完整性。例如：实施数据输入验证控制，并采用校验和、哈希值等完整性检查方法。 **R14 照护对象识别：**健康信息系统应通过唯一标识符准确识别系统内的照护对象，用户在访问或修改该对象记录时可对这些标识符进行搜索。	AUDT IGAU STCF TXCF TXIG	5.39 HLT -唯一识别照护对象 5.40 HLT -输出数据验证
用户身份识别与认证		
R15 用户标识：健康信息系统的用户应被分配一个标识符（用户ID），该标识符（必要时可与其他标识符如机构标识符、管辖区域标识符组合使用）能唯一识别每位用户，并用于用户身份验证和审计日志记录。当交易跨越组织或管辖边界时，用户ID需结合其他用户注册信息（例如用户名、地址、机构标识符、管辖区域标识符）实现以下功能： 唯一标识每位用户；）实现访问控制决策； c) 便于编制审计记录，从而能够明确无误地将用户身份与其被审计的操作行为相关联。	ALOF AUDT 授权 电磁辐射发生器 NAUT PAUT	5.16 身份管理 5.17 认证信息 5.18 访问权限 5.38 信息安全需求分析与规范

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
R16 用户标识符：健康信息系统应支持不区分大小写的用户标识符，这些标识符可包含来自 ISO/IEC 8859 系列（例如 ISO/IEC 8859-1，亦称 US ASCII）或 ISO/IEC 10646（亦称 Unicode）的字符。 R17 安全认证：健康信息系统在授予任何实体（例如用户、应用程序、系统服务）访问个人健康信息的权限之前，必须对其身份进行认证。 R18 用户身份验证：健康信息系统应在向用户授予访问个人健康信息或相关健康信息系统服务的权限之前，对每位用户进行身份验证。为明确起见，此规定适用于未连接网络时授予的访问权限（例如，当健康信息系统支持离线访问时）。 R19 身份验证方法：健康信息系统应支持多因素用户身份验证。 R20 系统认证：健康信息系统必须对所有试图访问个人健康信息的系统实体进行认证。当通过互联网或其他已知开放网络使用基于安全标准的协议传输个人健康信息时，健康信息系统应确保远程节点的真实性（即节点间的相互认证）。 R21 保护用户配置文件、密码及其他身份验证令牌：健康信息系统用户身份验证过程中使用的所有数据或参数均应以安全方式存储或传输，并防止未经授权的访问（包括查看、修改或删除）。当使用用户密码时，应采用安全的密码加盐及哈希方法，或使用密码学安全算法对密码进行加密。 R22 密码管理：使用密码、密码质量、密码重置及用户变更——当使用密码时，健康信息系统须实施以下规定： a) 密码强度：在用户设置密码时需检查其强度，具体方法包括：确保密码由足够数量的大写字母、小写字母、数字和特殊字符组合而成；不包含用户的个人信息（如电话号码）；且不含有连续的字母或数字。 b) 密码更改频率：实现一项功能，要求用户根据可调节的最大时间周期更改密码； c) 密码历史记录策略：实施一项管理功能，防止用户重复使用相同的密码达到特定次数（例如最近10次密码）。 d) 密码重置：完成密码重置后，用户在下次成功登录时必须设置新密码。 e) 大小写敏感性：支持包含来自 ISO/IEC 8859 系列（例如 ISO/IEC 8859-1，亦称 US ASCII）或 ISO/IEC 10646（亦称 Unicode）字符的区分大小写的密码。 R23 登录尝试失败次数：健康信息系统应设置用户连续无效登录尝试的上限，以防止用户发起进一步（可能具有恶意性质的）身份验证尝试。合适的机制包括：在管理员解除锁定前冻结账户/节点；根据可配置的时间段锁定账户/节点；或按照可配置的延迟算法推迟下一次登录提示。 R24 认证过程中的用户反馈：健康信息系统在认证过程中仅应向用户提供有限的反馈信息，且这些信息不得帮助用户发现其用户名和密码。		6.7 远程办公 8.1 用户终端设备 8.2 特权访问权限 8.3 信息访问限制 8.4 访问源代码 8.5 安全认证 8.11 数据掩码 8.12 数据泄露预防 8.15 日志 8.16 监测活动 8.24加密技术的应用

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
访问控制		
R25 访问控制：健康信息系统应核实所有经过身份验证、试图访问个人健康信息的人员或实体均具备相应的访问权限。 **R26 授权控制**：在执行与个人健康信息相关的数据功能系统之前，健康信息系统必须验证请求用户或实体是否拥有所需的访问权限。 **R27 基于角色的访问控制**：健康信息系统应支持基于角色的访问控制（RBAC），该机制能够将每个用户映射到一个或多个角色，并将每个角色映射到一个或多个系统功能或访问权限。 **R28 其他形式的访问控制**：健康信息系统还应能够将每位用户与根据其权限分配或限制的访问权限进行对应映射。 a)用户所属的工作组；或 b) 交易的具体情境（例如：一天中的时间、工作站位置或紧急访问情况）。 **R29 授权访问受照护对象的个人健康信息：** 健康信息系统应能够维护选定用户与受照护对象记录之间的关联关系，并基于该关联关系授予访问权限。健康信息系统还应能够根据已获得受照护对象记录授权访问权限的用户，向其他用户授予相应记录的委派访问权限。 在实施此类访问权限授予的情况下，不得..... a) 通过系统手段，允许用户在自身未拥有某条记录访问权限的情况下，向其他用户授予对该记录的访问权限； b)超出被授予访问权限用户的基于角色的访问权限。**R30 报告访问权限**：健康信息系统应能够针对特定用户，报告该用户是否可访问特定护理对象的记录，以及用户对该对象记录所拥有的权限（查看、修改等）。**R31 访问权限限制**：当用户被分配了多个用户角色时，健康信息系统应允许用户选择在当前会话中应用其被分配的角色。 **R32 撤销访问权限**：健康信息系统应支持撤销用户的所有访问权限，而无需从系统中删除该用户账户。健康信息系统应防止已全部撤销访问权限的用户登录系统，例如通过将用户账户设为非活动状态。	AUDT 授权 电磁辐射发生器 NAUT PAUT PLOK STCF	5.2 信息安全角色；责任 5.15 访问控制 5.18 访问权限 5.22 供应商服务的监控、审查与变更管理 5.33记录保护 5.34 PII 隐私与保护 6.7 远程办公 7.14 设备的安全处置或重复使用 8.3 信息访问限制
可接受的用途		
R33 对用户的通知：在每个用户的会话期间，无论是在用户登录前、登录后立即，还是在其他定期间隔内，健康信息系统均应显示可配置的警告或登录横幅，提醒用户注意从系统可获取的个人健康信息的保密性及正确使用方式，和/或滥用系统的相应处罚措施。	授权 电磁辐射发生器 PAUT	5.10信息及其他相关资源的合理使用 资产

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
安全与超时		
R34 工作站超时机制：当特定用户的会话在无人值守的工作站上处于活动状态时，健康信息系统应在设定的无活动时段后通过自动超时机制防止未经授权的访问。此类保护措施的示例包括启用屏幕保护程序，或设置屏幕超时机制，要求合法用户重新认证身份。 **R35 应用会话超时机制：**健康信息系统应在用户处于非活动状态达到可配置时长后，通过自动应用超时机制防止未经授权人员访问闲置的应用会话。此类防护措施包括实施应用锁定机制、要求合法用户重新认证等。应用超时前应提前发出警告（以可配置的时间间隔显示），提示即将发生超时。当应用会话超时后，原用户可通过重新认证重返该会话；或由其他用户直接终止当前会话（无需重新激活），从而能够启动新的会话。 **R36 连接超时：**健康信息系统应具备相应机制，在需要时将连接持续时间限制在可配置的时间范围内，并在超时后强制重新建立连接。 **R37 会话安全性：**健康信息系统应具备通信会话安全控制机制，以防止用户的会话被劫持或窃取。	ALOF AUDT 授权 电磁辐射发生器 MLDP NAUT PAUT PLOK SAHD TXCF TXIG	8.1 用户终端设备 8.5 安全认证 8.27 安全的系统架构与工程原则
保持数据可用性		
R38 备份：健康信息系统应支持生成应用程序数据、安全凭证、审计日志文件以及健康信息系统正常运行所需其他数据和文件的备份副本。 **R39 同步备份：**若健康信息系统持续可用，则该系统应具备在应用程序运行的同时执行备份的能力。 **R40 恢复：**健康信息系统数据恢复应使用户能够将系统恢复至完全可运行且安全的状态。该状态应包括应用程序数据、安全凭证及审计文件的恢复，并应能够验证所恢复数据的完整性。 **R41 在先前时间点重建电子健康记录的内容** 时间：健康信息系统应能够显示任何数据主体记录在任意先前日期或时间的状态。	AUDT DTBK IGAU	5.11 信息安全政策 5.30 企业持续运营所需的ICT基础设施准备 8.13 信息备份 8.14 信息处理设施的冗余性 8.15 日志 8.16 监测活动
传输过程中保护数据		
R42 传输过程中的数据加密：在由分布在多台计算机或系统上的组件构成的健康信息系统中，这些组件之间的通信（在互联网或其他开放网络上）应提供以下安全组件： a)合作伙伴身份验证（例如客户端和服务器）； b)数据完整性; 数据保密性。 **R43 数据传输确认：**为确保传输的数据能够被正确接收，当数据通信发生在保护信息处理设施的物理安全边界之外时，临床系统应实施安全控制措施，以确认数据的传输或接收。	AUDT 授权 IGAU NAUT PAUT TXCF TXIG	5.14 信息传输 5.19 供应商关系中的信息安全 8.12 数据泄露预防 8.20网络安全 8.21 网络服务的安全性 8.22 网络隔离 8.24 密码学的应用

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
保护存储中的数据		
R44 保护运营数据：健康信息系统应确保个人信息、审计日志及用户配置文件等安全相关数据，在永久存储（例如存储在数据库或文件系统中）或临时存储（例如缓存内存中）时，均受到保护，防止未经授权的访问和修改。 **R45 保护便携式或可移动设备上的数据：**当在任何旨在便携或可移动的介质或设备（例如，闪存驱动器、光介质或笔记本电脑）上存储个人健康信息时，健康信息系统应采用行业标准加密格式。 **R46 保护数据存储库中的数据：**存储机密和敏感数据（包括个人健康信息及安全关键系统数据，例如用户配置文件数据和审计日志）的健康信息系统，必须防止这些数据被未经授权的人员访问。	AUDT 授权 电磁辐射发生器 MLDP NAUT PAUT PLOK SAHD STCF TXCF TXIG	7.10 存储介质 7.14 设备的安全处置或重复使用 8.1 用户终端设备 8.11 数据掩码 8.12数据泄露预防 8.15 日志 8.16 监测活动 8.33 测试信息 8.34 审计测试期间的信息系统保护
数据完整性		
R47 数据输入完整性：从任何来源（例如健康信息系统、医疗设备或便携式设备）导入的数据，均应准确关联至受照护对象、负责医师、导入地点、导入日期与时间以及数据导入用户。用于导入数据的健康信息系统应显示关于潜在风险的警告提示。 **R48 数据处理过程中的完整性：**健康信息系统内应建立相应的控制措施，以确保数据完整性，并防止用户操作或系统故障导致数据不一致或完整性失效。 **R49 数据输出完整性：**健康信息系统应确保读者能够核验纸质打印输出内容的完整性。	DIDT IGAU TXIG	5.3 8 HLT信息安全需求分析与规范 5.39 HLT -唯一识别照护对象 5.40 HLT -输出数据验证 5.41 HLT -公开可获取的健康信息
记录保留		
R50 保留期限：健康信息系统应能够存储具有可配置保留期限的数据，并支持保留计划制定方法与流程，以管理法律或组织政策所规定的各类数据。当数据不再需要时，应采用安全的销毁方式予以处理，例如：数据擦除、加密擦除、存储介质格式化或数据匿名化处理。	AUDT DIDT DTBK IGAU PLOK STCF	8.10信息删除
数据标注		
R51标注：健康信息系统应能够向每位用户明确告知其所访问的个人健康信息属于机密信息。例如，在用户登录系统时或显示个人健康信息时，应在统一的位置和方式下显示保密标识。	IGAU STCF	5.12 信息分类 5.13 信息标注

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
系统和审计日志		
R52 系统日志：健康信息系统应支持记录系统事件和操作，例如系统启动与关闭、用户活动、系统性能、系统资源使用情况以及系统错误和警告。 **R53 记录的信息**：对于每一起此类事件，均应记录控制信息，例如事件发生时间、用户身份及用户角色（在用户可在开始会话前选择多个角色的情况下）。 **R54 保护审计日志**：审计日志文件应具备适当的安全控制措施，以防止篡改和未经授权的访问。此类控制措施包括访问控制、持续监控以检测任何异常活动或数据泄露、加密技术，以及定期或持续备份日志文件。 **R55 审计接口**：对审计数据的访问必须受到严格控制，并本身也需接受审计。访问应通过能够实施这些控制的适当信息系统进行，而非直接访问审计跟踪本身。审计系统应具备从审计记录中读取审计信息以及查询审计日志的功能和调查工具。 a) 识别在特定时间段内访问或修改过特定数据主体记录的所有用户； b) 识别特定用户在指定时间段内的操作行为（包括对数据主体记录的所有访问）。 **R56 审计日志保留**：尽管审计日志文件的保留期限属于组织政策范畴，且可能因司法管辖区而异，但审计系统应支持审计日志条目的保留。 **R57 应用审计日志**：健康信息系统应记录系统内的事件和操作，包括以下详细信息： a) 所创建或访问（例如：屏幕显示、打印、下载）或更新的照护对象记录； b)根据照护对象或相关人员的指令，可访问被锁定或屏蔽的数据（紧急访问权限）； c)对受照护对象或相关人员的知情同意指令进行制定与修改； d) 个人健康信息的数据查询； e)个人健康信息导入（接收），包括数据传输、数据交换； f) 个人健康信息导出，包括数据传输、数据交换及打印； g) 用户、角色和组管理活动； 访问审计日志。 健康信息系统审计日志还应能够记录以下事件： 系统启动和停止； 用户身份验证尝试及其结果（成功或失败）； 用户注销、会话超时、账户锁定； 备份与恢复（由系统自身启动）； 数据库访问； 节点认证失败； 数字签名已创建/验证； 安全管理事件，包括密码更改； 记录处置。 健康信息系统应允许授权管理员设置是否纳入或排除上述列表中未包含的可审计事件。	AUDT SAHD	8.15 日志 8.16 监测活动 8.33 测试信息 8.34 审计测试期间的信息系统保护

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
R58 记录信息的最低内容：健康信息系统审计日志条目应包含以下信息： ）用户身份记录； b) 授权机构的身份记录——即批准数据录入或访问权限的人员身份，若该人员与用户身份不同； c)用户正在行使的角色（在用户可在开始会话前从多个角色中进行选择的情况下）； d) 访问用户的组织信息（适用于用户代表多个组织访问信息的情况）； e) 被审计事件的性质及关联数据的身份信息（例如：受照护对象的ID、消息ID）； f) 用户执行的功能； g) 时间戳（事件的数据和时间）； h) 在需要紧急访问被屏蔽或加密的记录或记录部分内容的情况下，用户应自行选择紧急访问的理由； i) 当由替代决策者对知情同意指令作出修改时，需明确该决策者的身份； j) 终端用户设备或接入点（如可用）； k) 在密码更改的情况下，指其密码已被更改的用户； ）序列号用于防范恶意篡改审计日志的行为，例如通过修改系统日期等方式。 R59审计接口：健康信息系统应支持向统一审计引擎记录数据[例如，采用 IHE 审计轨迹与节点认证（ATNA）规范中审计日志部分规定的模式及传输协议]。 该系统应允许授权管理员通过以下至少一种方式从审计记录中读取审计信息： a) 该系统应具备根据日期和时间范围生成报告的功能。 b)该系统应能够以支持基于日期和时间（例如UTC同步）进行关联分析的方式导出日志。 R60 保护审计日志：健康信息系统应： a) 禁止用户访问审计日志条目，仅限已获得明确读取权限的授权用户。 b)禁止用户修改审计日志条目。 该系统应确保对审计记录的访问权限，并保护对系统审计工具及审计跟踪的访问权限，以防止滥用或数据泄露（包括删除或篡改）。 R61 连续记录：健康信息系统审计日志功能须始终保持启用状态，且用户不得有任何方式禁用审计日志功能。 R62 保留个人健康信息历史记录：健康信息系统不得删除记录或审计日志条目，亦不得修改数据主体记录，以免妨碍对特定医疗对象在先前时间点记录的重建。		

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
软件版本控制与文档编制		
R63 健康信息系统版本控制：健康信息系统的所有组件均需被识别，并配备具有唯一明确标识（唯一ID、名称、供应商及版本号）的关联软件版本。 **R64健康信息系统文档：**健康信息系统应需提供涵盖系统需求与容量、安装与测试、管理与操作、已知安全问题、用户身份识别与认证、权限管理与访问控制、安全通信、审计、软件变更管理、时间同步以及数据备份与恢复等方面的完整文档。 **R65 文档变更：**文档应包含所有变更的历史记录。**R66 文档与软件版本：**所有文档项均应在开头明确标注其版本号及所适用的软件版本。**R67 软件版本：**健康信息系统应具备允许用户查看其软件组件版本的功能。 **文档中包含的R68主题：** 健康信息系统应具备可获取的文档，涵盖以下所有内容： a) 系统要求，包括正常运行所必需的服务和网络协议，以及对其他 EHR 组件的依赖关系； b) 系统产品容量（例如：用户数量、护理对象数量、记录数量、网络负载）以及针对这些容量所假设的基线代表性配置（例如：处理器数量或类型、服务器/工作站配置及网络容量）； c 系统安装、启动及连接，包括通信安全配置； d)确认系统安装已完成且系统可正常运行所需的步骤； e) 系统管理与操作； f) 安全机制与实践，包括用户账户的创建、修改和停用；角色管理、密码重置、密码约束配置以及权限管理的其他方面；通信安全；以及审计日志的配置与管理。 g) 已知与安全服务（包括防病毒、恶意软件清除、入侵检测及防火墙）存在的问题或冲突，并在适用情况下解决相关冲突； h) 软件变更管理及热修复流程； i) 适用时，实现系统时间（周期）同步； j) 向用户和管理员显示系统错误或性能提示信息，并提供相应的操作指引； k)数据备份流程，包括在创建或恢复备份副本时进行的数据完整性检查。 **R69 文档与版本控制：**所有健康信息系统手册均应在文档开头明确注明其适用的版本（或多个版本）。 所有更新后的健康信息系统手册均应为读者提供自上次重大修订以来的变更摘要。 **R70 文档变更要求：**文档应以用户可读的形式记录所有变更的历史记录，以便用户能够查阅最新版本中所做的所有修改。	CSUP MLDP RDMP SAHD	8.6 容量管理 8.7 恶意软件防护 8 8技术漏洞的管理 8.9 配置管理 8.17 钟 同一时刻 8. 18特权实用程序的使用 8. 19在操作系统上安装软件 8. 25安全的开发生命周期 8.26 应用程序安全要求 8.27 安全的系统架构与工程原则 8.28 安全编码 8.29 开发与验收过程中的安全测试 8.30 外包开发 8.31 开发环境、测试环境和生产环境的分离 8. 32变更管理

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
时间同步和时间/日期格式化		
R71 时间格式：健康信息系统应采用统一的时间呈现方式，以便于控制和审计。 **R72 周期同步：**健康信息系统应采用公认标准进行时间同步，并在所有记录（包括时间记录）中使用该同步时间。 **R73 导出记录中的时间格式：**导出数据中包含的所有控制与审计时间数据（除向时间戳认证机构发送或从该机构接收的时间戳请求及响应外），均应采用 ISO 8601 格式表示，以显示本地时间与 UTC 之间的差值。 **R74 安全时间源：**健康信息系统应使用一致且安全的时间源。	AUDT CSUP SAHD	8.17周期同步
隐私与安全事件管理		
R75 事件管理：每当检测到系统滥用的潜在事件时，健康信息系统或支持性审计系统应向组织内负责管理隐私或安全事件的相关人员或安全系统触发可配置的通知。 **R76 事件通知：**健康信息系统应提供相应机制，使用户能够向责任人员报告安全事件或问题。	AUDT	5.5 与当局取得联系 5.24 信息安全事件管理的规划与准备 5.25 对信息安全事件的评估与决策 5.26信息安全事件应对措施 5.27 从信息安全事件中学习 5.28 证据收集 5.43 HLT -外部事件报告 6.8 信息安全事件报告

表 D.2（续）

安全和隐私要求示例（见D.1条）	根据 IEC/TS 81001-2-2 标准提供的适用安全功能	本文件的控制措施
数字证书和数字签名		
R77 为用户提供数字签名：在需要用户使用电子形式签名（相当于手写签名）的健康信息系统中，应允许用户使用数字签名。 **R78 数字签名验证：**当健康信息系统生成或接收包含数字签名的数据时，系统应在生成及接收时确认该签名在应用时处于有效状态。**R79 数字签名保存：**允许用户应用数字签名或接收数字签名数据的健康信息系统，应在存储、备份或归档签名数据时同步保存、备份或归档数字签名；并在传输签名数据时一并传输数字签名。 **R80 数字签名：**所有具备要求用户使用电子形式手写签名功能的健康信息系统，均应支持符合信息安全政策和法规的适当数字签名标准。 **R81 验证、保存和传输数字签名：**健康信息系统应： a) 收到后确认签名有效（即相关的签名证书及所有关联的链证书均未被撤销）； b) 在存储、备份或归档已签名数据时，必须同步存储、备份或归档数字签名及所有相关数据（包括根证书、证书链、签名证书及撤销信息等相关信息）。 c) 在传输已签名数据时，应随数据一同传输数字签名或通过引用方式传输； d) 允许用户在访问已签名数据时确认：该签名在签署时有效（即关联的签名证书未被撤销）。 **R82 签名目的及签署方角色：**具备数字签名功能的健康信息系统应包含承诺类型指示属性及签署方角色（即用户的角色属性）。	AUDT PAUT TXCF TXIG	8.24加密技术的应用

施与示例安全及隐私要求之间的关系（参见条款 D.1）

本文件的控制	安全和隐私要求示例（D.1条款）
第5条 组织控制	
5.1 信息安全政策	R1 录音同意书 R2：记录的最小数据 R3指令遵循数据要求 R4 急救通道 R5 记录紧急访问 R6：由法定授权代表签署的同意书 R7：变更同意书内容的报告 R8 仅记录和存储那些具有明确收集、使用或披露目的的数据； R9 限制向与数据主体存在业务关系的医疗保健提供者披露数据主体的信息； R10 限制数据出口。 R50 记录保存 R56 审计日志保留期限 R62 保存个人健康信息的历史记录
5.2 信息安全角色与职责 5.3 职责分离 5.4 管理职责 5.5 与当局取得联系 5.6 与特殊利益集团接触	R25 访问控制 R26 授权控制 R27 基于角色的访问控制 R28 其他形式的访问控制 R29 授权访问受照护对象的个人健康信息 R30 报告访问权限 R31 访问权限限制 R32 撤销访问权限 R75 事件管理 R76 事件通知
5.7 威胁情报	没有一个
5.8 项目管理中的信息安全	没有一个
5.9 信息及其他相关资产清单 5.10 信息及其他相关资产的合理使用 5.11 资产返还	R33：向用户发送通知 R62 保存个人健康信息的历史记录
5. 12信息分类5.13 信息标注	R14 护理对象识别 R51 标签
5.14 信息传输	R10 限制数据导出 R42 在传输过程中加密数据

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
5.15 访问控制	R4 急救通道 R5 记录紧急访问 R8 仅记录和存储那些具有明确收集、使用或披露目的的数据； R9 限制向与数据主体存在业务关系的医疗保健提供者披露数据主体的信息； R10 限制数据出口。 R27 基于角色的访问控制 R28 其他形式的访问控制 R29 授权访问受照护对象的个人健康信息 R30 报告访问权限 R31 访问权限限制
5.16 身份管理	R15 用户身份识别 R16 用户 ID
5.17 认证信息	R17 用户身份验证 R18 用户身份验证（在授予数据或系统服务访问权限之前） R19 身份验证方法 R20 用户和系统身份验证 R21 保护用户配置文件、密码及其他身份验证令牌 R22 密码：使用密码、密码质量、密码重置及用户密码修改 R23 登录尝试失败 R24：身份验证期间的用户反馈
5. 18访问权限	R25 访问控制 R26 授权控制 R27 基于角色的访问控制 R28 其他形式的访问控制 R29 授权访问受照护对象的个人健康信息 R30 报告访问权限 R31 访问权限限制 R32 撤销访问权限
5.19 供应商关系中的信息安全 5.20 在供应商协议中解决信息安全问题 5.21 管理信息通信技术供应链中的信息安全 5. 22供应商服务的监控、审查及变更管理 5.23 云服务使用的信息安全	没有一个

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
5.24 信息安全事件管理的规划与准备 5.25 信息安全事件的评估与决策 5.26 信息安全事件的响应 5. 27从信息安全事件中学习 5. 28证据收集	R75 事件管理 R76 事件通知
5.29 故障期间的信息安全 5.30 保障业务连续性的ICT准备度	R48 处理过程中的数据完整性 R57 可审计事件
5.31法律、法定、监管及合同要求 5.32知识产权	R68 文档中包含的主题
5.33记录保护 5.34 PII 的隐私与保护	R1 录音同意书 R2：记录的最小数据 R3指令遵循数据要求 R4 急救通道： R5 记录紧急访问 R6：由法定授权代表签署的同意书 R7：变更同意书内容的报告 R27 基于角色的访问控制 R29 授权访问受照护对象的个人健康信息 R31 访问权限限制
5.35 信息安全的独立审查 5.36 遵守信息安全相关的政策、规则和标准	R1 录音同意书 R2：记录的最小数据 R3指令遵循数据要求 R4 急救通道： R5 记录紧急访问 R6：由法定授权代表签署的同意书 R7：变更同意书内容的报告 R8 仅记录和存储那些具有明确收集、使用或披露目的的数据； R9 限制向与数据主体存在业务关系的医疗保健提供者披露数据主体的信息； R10 限制数据出口。 R50 记录保存 R56 审计日志保留期限 R62 保存个人健康信息的历史记录
5.37 有文件记录的操作程序	R68 文档中包含的主题
5.38HLT-信息安全需求分析与规范	R68 文档中包含的主题
5. 39HLT——唯一识别护理对象 5.40HLT-输出数据验证	R14 护理对象识别
5.41HLT-公开可获取的健康信息	没有一个
5.42HLT-紧急通信	没有一个
5.43HLT- 外部事件报告	R75 事件管理 R76 事件通知

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
第6条 人员控制	
6.1 放映 6.2 雇佣条款与条件 6.3 信息安全意识、教育和培训 6.4 纪律处分程序 6.5 雇佣关系终止或变更后的责任 6.6 保密协议或非披露协议	没有一个
6.7 远程办公	R15 用户身份验证 R16 用户 ID R17 用户身份验证 R18 用户身份验证（在授予数据或系统服务访问权限之前） R19 身份验证方法 R20 用户和系统身份验证 R21 保护用户配置文件、密码及其他身份验证令牌 R22 密码：使用密码、密码质量、密码重置及用户密码修改 R23 登录尝试失败 R24：身份验证期间的用户反馈 R25 访问控制 R26 授权控制 R27 基于角色的访问控制 R29 授权访问受照护对象的个人健康信息 R30 报告访问权限 R31 访问权限限制 R32 撤销访问权限
6.8 信息安全事件报告	R75 事件管理 R76 事件通知
6.9 HLT 管理培训	没有一个
第7条 物理控制	
7.1 物理安全边界 7.2 物理入口 7.3 保护办公室、房间及设施 7.4 物理安全监控 7.5防范物理和环境威胁 7.6 在安全区域工作 7.7 清理桌面和屏幕 7.8 设备选址与保护 79 场外资产的安全性	R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护数据仓库中的数据

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
7.10 存储介质	R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护数据仓库中的数据
7.11 支持性公用设施7.12电缆安全 7.13 设备维护 7.14 设备的安全处置或重复使用	R45 保护便携式存储介质上的数据
第8条 技术控制措施	
8.1 用户终端设备	R15 用户身份识别 R16 用户 ID R17 用户身份验证 R18 用户身份验证（在授予数据或系统服务访问权限之前） R19 身份验证方法 R20 用户和系统身份验证 R25 访问控制 R34 会话安全性 R35 用户会话超时 R36 连接超时 R37 会话安全性 R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护数据仓库中的数据
8.2 特权访问权限 8.3 信息访问限制 8.4 访问源代码	R15 用户身份识别 R16 用户 ID R17 用户身份验证 R18 用户身份验证（在授予数据或系统服务访问权限之前） R19 身份验证方法 R20 用户和系统身份验证 R25 访问控制 R26 授权控制 R27 基于角色的访问控制 R28 其他形式的访问控制 R29 授权访问受照护对象的个人健康信息 R30 报告访问权限 R31 访问权限限制 R32 撤销访问权限
8.5 安全认证	R17 用户身份验证 R18 用户身份验证（在授予数据或系统服务访问权限之前） R19 身份验证方法 R20 用户和系统身份验证 R21 保护用户配置文件、密码及其他身份验证令牌 R22 密码：使用密码、密码质量、密码重置及用户密码修改 R23 登录尝试失败 R24：身份验证期间的用户反馈 R34 会话安全性

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
8.6 容量管理 8.7 恶意软件防护 8.8 技术漏洞的管理 8.9 配置管理	R68 文档中包含的主题 R69 文档与版本控制 R70 文档变更
8.10 信息删除	R50 固定装置
8.11 数据掩码 8.12 数据泄露预防	R21 保护用户配置文件、密码及其他身份验证令牌 R32 撤销访问权限 R42 传输过程中对数据 进行加密 R43 数据传输确认 R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护数据存储库中的数据 R54 保护审计日志 R58 记录的信息最低含量
8.13 信息备份 8.14 信息处理设施的冗余性	R38 备份 R39 同步备份 R40修复工程 R41 在先前时间点重建电子健康记录的内容
815日志记录 8.16 监测活动	R5 记录紧急访问 R15 用户身份识别 R38 备份 R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护 数据存储库中的数据 R54 保护审计日志
8.17 周期同步	R68文档中包含的主题——与周期同步相关的要求 R71 时间格式 R72周期同步 R73 导出记录中的时间格式 R74 时间源
8. 18 特权实用程序的使用 8.19 在操作系统上安装软件	R64健康信息系统文档；R68文档涵盖的主题——软件安装 相关要求
8. 20网络安全 8.21网络服务的安全性 8.22网络的分离	R42 传输过程中对数据进行加密 R43 数据传输确认
8.23Web过滤	没有一个

表 D.3（续）

本文件的控制	安全和隐私要求示例（D.1条款）
8. 24 加密技术的应用	R21 保护用户配置文件、密码及其他身份验证令牌 R42 传输过程中对数据进行加密 R43 确认数据传输完成 R77 为用户提供数字签名 R78 验证数字签名 R79 保留数字签名 R80 数字签名 R81 数字签名的验证、保存与传输 R82 签名的作用及签署方的角色
8. 25 安全的开发生命周期 8.26 应用程序安全要求 8.27 安全的系统架构与工程原则 8.28 安全编码 8.29 开发与验收过程中的安全测试 8.300外包开发 8. 31. 开发环境、测试环境和生产环境的分离 8. 32变更管理	R63健康信息系统版本控制 R64 健康信息系统文档 R65 文档变更 R66 文档与软件版本 R67 软件版本 R68 文档中包含的主题 R69 文档与版本控制 R70 文档变更
8.33 测试信息 8.34审计测试期间的信息系统保护	R44 保护运营数据 R45 保护便携式存储介质上的数据 R46 保护数据存储库中的数据 R54 保护审计日志
8.35HLT-零信任原则	没有一个

参考文献

[1] ISO 8601（所有部分）；*日期和时间——用于信息交换的表示方法*

[2] ISO/IEC8859（全部部分），***信息技术——****8位单字节编码图形字符集*

[3] ISO/IEC 10646，*信息技术——通用编码字符集（UCS）*

[4] ISO/IEEE11073（全部部分），*健康信息学——设备互操作性*

[5] ISO 12052，*健康信息学——医学数字****成像与通信（DICOM），包括****工作流程与数据管理*

[6] ISO 13131，*健康信息学——远程医疗服务——质量规划指南*

[7] ISO 13940:2015，*《健康信息学——支持连续性医疗的概念体系》*

[8] ISO/TS 14265*健康信息学——个人健康信息处理目的的分类*

[9] ISO/TS 14441:2013*健康信息学——用于符合性评估的EHR系统的安全与隐私要求*

[10] ISO 17090-3*健康信息学——公钥基础设施——第3部分：认证机构的策略管理*

[11] ISO/TS 17975:2022*健康信息学——P：个人健康信息收集、使用或披露过程中知情同意的原则与数据要求*

[12] ISO*/TS 21089，《健康信息学——可信的端到端信息流》*

[13] ISO 21298，健康信息学*——功能与结构作用*

[14] ISO/TR 21332，*健康信息学——健康信息系统安全与隐私的云计算考量*

[15] ISO 22600（所有部分），*健康信息学——权限管理与访问控制*

[16] ISO 22857：健康信息学——促进个人健康数据跨境流动的数据保护指南

[17] ISO/TS 23535，*《健康信息学——面向客户的健康云服务协议的****要求****》*

[18] ISO 25237，健康信息学——P匿名化

[19] ISO/IEC 27001:2022，《信息安全》、*网络安全与隐私保护——信息安全****管理体系——要求***

[20] ISO/IEC 27005*信息安全、网络安全与隐私保护——信息安全风险管理指南*

[21] ISO/IEC 27701，*信息安全、网络安全与隐私保护——隐私信息管理系统——要求与指南*

[22] ISO 27789:2021*健康信息学——电子健康记录的审计追踪*

[23] ISO/HL727931*数据交换标准——Health Level Seven 第2.5版——医疗保健环境中电子数据交换的应用协议*

[24] IEC/TS 81001-2-2:2025，《健康软件与健康信息技术系统的安全性、有效性和安全性 一 》*第2-2部分：关于安全需求、风险及控制措施的实施、披露与沟通指南*

[25] FHIR . 快速医疗互操作性资源。可在https://h17.org/fhir/获取

[26] IHE . 整合医疗保健企业。网址：https://www.ihe.net

[27] 世界卫生组织（WHO）。WHO/HSS/EHT/DIM/11.03，《核心医疗设备》。可获取地址：https://iris.who.int/handle/10665/95788

ICS 35.030;35.240.80
基于72页内容

iso.org

International Standard

ISO 27799

Health informatics — Information security controls in health based on ISO/IEC 27002

Informatique de santé — Contrôles de sécurité de l'information dans le domaine de la santé basés sur l'ISO/IEC 27002

Third edition
2025-12

Reference number
ISO 27799:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This third edition cancels and replaces ISO 27799:2016 and ISO/TS 14441:2013, which have been technically revised.

The main changes are as follows:

— alignment with the new structure of ISO/IEC 27002:2022 and other changes to that standard from the previous version;

— revision and addition of controls specific to health;

— removal of material that was originally only in the second edition of this document but was subsequently included in ISO/IEC 27002:2022;

— addition of informative Annexes providing supplementary guidance on cybersecurity in health organizations and, based on ISO/TS 14441:2013, 5.3, updated example security and privacy requirements for health information systems.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

This document contains a set of information security controls for health organizations. It considers all the controls in ISO/IEC 27002:2022 and, in some cases, supplements the controls or provides guidance on their application in health. There are also some additional controls specific to health which are not derived from any in ISO/IEC 27002:2022.

0.2 Context and background

Factors that affect information security in healthcare include the following:

a) Use of equipment that relies on digital technologies for its operation and is deployed exclusively or predominantly in the healthcare domain. Medical devices incorporating health software are the prime example.

b) The need to balance clinical safety and effectiveness with information security.

c) Maintaining the privacy of subjects of care while ensuring access to relevant personal health information for diagnosis and treatment.

d) The distributed nature of personal health information both within and between organizations (possibly in different jurisdictions) resulting in the need for high levels of interoperability between diverse systems, applications and devices.

e) Users of many different kinds including doctors, nurses, other clinicians, trainees, students, healthcare assistants, technicians, administrative staff and volunteers as well as subjects of care and their proxies.

f) The multiple interdependencies and information flows between and within organizations responsible for one or more of: healthcare, clinical research, teaching, education and training.

g) The need for some healthcare services to be available on a continuous basis (24 hours a day every day) under normal circumstances. In addition, natural disasters and other unusual events that can lead to surges in demand for healthcare services.

h) Organizations providing health services as well as manufacturers or suppliers of systems, devices and equipment are all subject to a wide range of legal, statutory, regulatory and contractual requirements which can vary between jurisdictions.

i) Overlapping or incomplete requirements for accountability and professional responsibility between different professions (such as ICT and medical devices staff) for ensuring security and safety of systems, devices and equipment.

Given this overall context, healthcare has a number of sector-specific, if not unique, information security requirements. However, the controls in ISO/IEC 27002:2022 are intentionally generic, hence the need for this document.

0.3 Audience and uses

This document is targeted at organizations that:

— provide healthcare services or are custodians of personal health information for other reasons;

— supply software, systems, devices, equipment or services that are used to process personal health information;

— are responsible for healthcare regulation, accreditation, inspection, assurance or similar.

Individuals for whom this document is particularly relevant include:

— ICT and medical devices or equipment professionals working in the types of organizations listed above;

— information security professionals (particularly those unfamiliar with the health domain): these professionals can include consultants, penetration testers, auditors and those working for bodies that provide accreditation, inspection, assurance or certification services for information security.

Appropriate implementation of the controls in this document can provide assurance to individuals, including subjects of care, their proxies and members of an organization's workforce. Appropriate implementation can also provide assurance to a wide range of stakeholder bodies including management and governance boards of healthcare organizations, other healthcare organizations with which information is exchanged or shared, public authorities, regulators, auditors, and organizations that finance, insure, accredit or inspect healthcare services.

This document can be used in healthcare settings when determining and implementing controls for an information security management system (ISMS) conformant to ISO/IEC 27001.

Health informatics — Information security controls in health based on ISO/IEC 27002

1 Scope

This document provides information security controls, including implementation guidance, for health organizations. It is based on ISO/IEC 27002:2022

In addition to generic ICT equipment and software used in many other environments, the scope of this document includes software and systems specifically for healthcare, such as electronic health record systems and medical devices incorporating health software. Such medical devices can be programmed or programmable and can contain software, firmware or both.

Other digital equipment (such as that for environmental and infection control, building management, and physical security), which can be used in premises where healthcare is provided, is also in scope.

This document applies to information in all its aspects, whatever form the information takes (including text and numbers, sound recordings, drawings, images and video), by whatever means it has been acquired or captured, whatever means are used to store it (such as printing or writing on paper or storage electronically), and whatever means are used to transfer or exchange it (orally, by hand, by post, movement of storage media, direct links or networking).

This document is for organizations of all types and sizes that provide healthcare or are custodians of personal health information for other reasons. The information that they are responsible for can be stored and processed in many possible ways and locations, including on premises or in the cloud, but remains in scope.

This document applies to all physical settings where healthcare is intended to be delivered, such as hospitals, clinics and other locations or facilities designated for healthcare purposes such as ambulances and mobile imaging or diagnostic units. It also applies to care provided elsewhere, such as in residential premises. In addition to the range of settings, this document applies to all methods of service provision including remote or virtual healthcare.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

ISO 81001-1, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 27002:2022, ISO 81001-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms and definitions

3.1.1
health
complete physical, mental and social well-being

Note 1 to entry: Health is not merely the absence of disease or infirmity.

Note 2 to entry: Adapted from World Health Organization[1)].

3.1.2
health software
software intended to be used specifically for managing, maintaining, or improving *health* (3.1.1) of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device

Note 1 to entry: Health software fully includes what is considered software as a medical device.

[SOURCE: ISO 81001-1:2021, 3.3.9]

3.1.3
healthcare
care activities, services, management or supplies related to the *health* (3.1.1) of an individual

3.1.4
personal health information
information about an identifiable person that relates to the physical or mental *health* (3.1.1) of the individual or to provision of health services to the individual

Note 1 to entry: Personal health information can include the following:

a) information about the registration of the individual for the provision of health services;

b) information about payments or eligibility for healthcare 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;

f) identification of a person (for instance a health professional) as a provider of healthcare to the individual.

Note 2 to entry: Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymised.

Note 3 to entry: Personal health information is a subset of personally identifiable information (PII).

[SOURCE: ISO/TS 17975:2022, 3.21, modified — Note 3 to entry was added.]

3.1.5
proxy
subject of care proxy
person with the right to take decisions on behalf of the *subject of care* (3.1.6)

EXAMPLE 1 Parents of children who are not yet adults.

EXAMPLE 2 Guardians of adults with learning disabilities or lacking mental capacity.

Note 1 to entry: Adapted from ISO 13940:2015, 5.2.4.3.

1) https://www.who.int/about/governance/constitution.

3.1.6
subject of care
person who seeks to receive, is receiving, or has received *healthcare* (3.1.3)

Note 1 to entry: Adapted from ISO 13940:2015, 5.2.1.

3.2 Abbreviated terms

HLT health

ICT information and communication technology

ISMS information security management system

PII personally identifiable information

4 General

4.1 Structure of this document

This document adopts the structure of ISO/IEC 27002:2022, Clauses 5 to 8 and lists all the control titles in that standard. Using that framework, this document:

a) indicates which controls (including their purposes, guidance and any other information) in ISO/IEC 27002:2022 apply unchanged in health;

b) for certain controls in ISO/IEC 27002:2022, provides guidance, other information, or both on how to apply the controls in health;

c) for the remaining controls in ISO/IEC 27002:2022, supplements what each control is, its purpose and guidance. Other information for health is also provided in some of these instances;

d) specifies controls that are specific to health and that are not based on any existing controls in ISO/IEC 27002:2022. These additional controls have the same layout as the controls in ISO/IEC 27002 and the control titles are prefixed with "HLT" (for HeaLTh).

In relation to ISO/IEC 27002:2022, controls in c) and d) are supplementary and additional respectively.

This document contains 4 Annexes:

— Annex A is a reference list of the controls specific to health, namely those under c) and d). Annex A also complements ISO/IEC 27001:2022, Annex A.

— Annex B provides a mapping table showing the correspondence of the HLT controls in this document with controls in ISO 27799:2016. It provides support for the transition between the two editions and complements ISO/IEC 27002:2022, Annex B.

— Annex C provides information on aspects of healthcare that are of particular importance in the context of information security.

— Annex D provides example requirements for the development and acquisition of health IT systems and a mapping to MDS2 (manufacturer disclosure statement for medical device security).

4.2 Safety

Security, safety and health information system effectiveness are interdependent. This should always be taken into account when assessing and managing risks and their risk control measures. For example, a risk that systems or data will not be available at the point-of-care is not just a security risk; it can have significant impact on safety if decision making about care is compromised. In turn, this can impact the effectiveness of the health system.

A consequence of the interdependence of security, safety and effectiveness is that well-intended risk control measures can, in some instances, adversely impact one or both of the other properties. For instance, adding controls to reduce the risk resulting from unauthorized access can impact system usability and availability and hence compromise system effectiveness. It can also result in system workarounds that adversely impact safety.

Safety should be taken into account in all aspects of information security management in health, including the selection and application of controls. Accordingly, any impacts on safety should be considered when implementing controls in this document.

4.3 Selecting and applying controls

4.3.1 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

Health organizations should select information security controls from this document and ISO/IEC 27002 as appropriate. In addition, new information security controls can be designed to meet specific needs as necessary.

4.3.2 Application of guidance

Where healthcare-specific guidance for a control is provided in this document and the control is being implemented, that guidance should either be followed or the reason for not following it should be documented along with an explanation of how the control's purpose will be met ("comply or explain").

Within the guidance for some controls, there are cross references to other controls in this document or to other standards, or both. Such cross-references are for information.

4.3.3 Use with ISO/IEC 27001:2022

The supplementary and additional controls, as listed in Annex A, can be used when determining and implementing controls in health settings for an information security management system (ISMS) that is conformant to ISO/IEC 27001.

It is a requirement of ISO/IEC 27001:2022, 6.1.3 that organizations produce a Statement of Applicability. The controls in Annex A can also be used in this connection.

5 Organizational controls

5.1 Policies for information security

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.1 apply.

Control for health (supplementary)

The information security policy should set out the approach to managing information security and be approved by the highest management level, then reviewed at least annually and after the occurrence of any serious security incident.

Purpose for health (supplementary)

To ensure top-management commitment to information security, that is kept up to date.

Guidance for health

The information security policy should contain statements on:

a) the need for health information security;

b) the goals of health information security;

c) compliance scope;

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 importance of reporting actual or suspected incidents including near misses as soon as possible so that any incidents that do occur can be dealt with at the earliest opportunity and do not become more serious;

g) the identification of processes and systems that are vital in healthcare (that is failure can lead to adverse effects in care or to reduced patient safety).

Revision of the policy's contents should be driven by the findings of a risk assessment.

In creating and maintaining the information security policy and topic specific policies, the following factors should be considered:

a) the breadth of health information;

b) the rights and responsibilities of staff, which include legal and ethical requirements, standards set by professional bodies, and any local requirements;

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

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

e) multiple organisations (which can be in different jurisdictions from each other) providing healthcare or supporting services, as well as individuals (including the subjects of care themselves and their relatives or close companions) who can be involved in the current or past delivery, determination, administration or funding of a subject's health and social care (see Annex C);

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

g) the arrangements for and access limits of:

   1) personnel involved in the delivery of care, including permanent and temporary or visiting staff such as locums, trainees, students and "on-call" or agency staff (see Annex C for further information);

   2) personnel who are supporting direct care, including administrative and support staff as well as clergy, charity workers and other volunteers (see Annex C for further information);

   3) personnel from regulatory and inspection bodies, financial and other auditors, health professionals and others investigating clinical or other incidents involving care provisioning;

h) situations where information about a subject must be provided externally or is requested by authorities or other third parties: such situations can include where someone has been harmed during a crime, when there is suspected abuse or inadequate care of children, women, elderly, persons with learning disabilities or other vulnerable subjects of care;

i) the implications of security measures on patient safety;

j) the implications of information security measures on the functionality and performance of health information systems.

Where support from or collaboration with third parties is obtained, and especially where it receives services from other jurisdictions, the policy framework should include documented policy and procedures that cover such interactions and specify the responsibilities of all parties.

Where applicable, reviews of policies should address:

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

b) the changes made to the ICT architecture or infrastructure, or both, and the concomitant changes these bring to the risk profile;

c) the changes identified in the external environment that similarly impact the 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 supervisory authorities in the field of protection of PII (see also 5.34);

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 caregivers, researchers and governments (e.g. supervisory authorities in the field of protection of PII);

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

5.2 Information security roles and responsibilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.2 apply.

Control for health (supplementary)

There should be at least one individual responsible for information security.

Purpose (supplementary)

To ensure that there is clear direction, visible management support for activities involving the security of health information and adequate technical expertise.

Guidance for health

Accountability and coordination of information security can only be maintained over the long term if the organization has an explicit information security management infrastructure.

An important element in roles and responsibilities with regard to information security is the presence of, or access to, an information security officer, who is responsible for the coordination of information security. Of paramount importance is the accountability of top management for all things related to information security.

Many organizations and particularly larger ones (for example, with a workforce of more than 500 or a client base of more than 10 000) should have an information security advisory group. Such groups are sometimes termed committees or boards.

The group's purpose is to ensure that there is clear direction and visible management support for ensuring the security of health information. The group should meet regularly, typically on a monthly basis, to "stay on top of things" and keep up-to-date.

In addition to the information security officer, the group should include representatives from the organization who:

— use health IT systems or other ICT infrastructure and services (for example, doctors, nurses, other clinicians, managers, administrators);

— have professional responsibility or accountability within the organization for the operation of the systems and services (for example, ICT staff, medical device and hospital engineering professionals).

Other information for health

See Annex C for further information on information security advisory groups.

5.3 Segregation of duties

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.3 apply.

Guidance for health

In very small organizations, it is sometimes not possible to segregate all conflicting duties and areas of responsibility. In such cases, duties and areas of responsibility should be segregated where feasible. Additionally, measures should be considered where problematic conflicts remain. The remaining areas of conflict should be documented along with the compensatory measures.

Many staff in healthcare, such as professionals and researchers, switch roles continuously. What isn't a conflicting duty or area of responsibility, can easily become one in an instant. For example, a physician is at one moment supervising a doctor in training and at the next moment administering care. Special consideration should be given to segregation of duties and areas of responsibility where roles change frequently.

5.4 Management responsibilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.4 apply.

5.5 Contact with authorities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.5 apply.

5.6 Contact with special interest groups

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.6 apply.

Guidance for health

Privacy requirements can have significant implications for security. Because of the special considerations that apply in healthcare, involvement with groups, forums and professionals' associations that have a specific focus on the privacy and security of health information should be considered.

5.7 Threat intelligence

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.7 apply.

Guidance for health

In health, there is a wide range of threats that should be taken into account and for which intelligence should be maintained. Factors that are particularly relevant include the following:

a) In addition to generic ICT and Internet-of-Things devices, there is equipment specific to health, including many different types and models of medical devices.

b) On generic ICT equipment, security measures include updating software, applying patches and using software that protects against malware. For clinical safety and other reasons, there can be restrictions on taking measures such as these on some medical devices incorporating health software.

c) Many health organizations use hardware and software that is obsolete, inappropriately configured, or both.

d) There can be particular challenges with maintaining accurate inventories and controlling assets.

Other information for health

See Annex C for further information.

5.8 Information security in project management

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.8 apply.

Guidance for health

Safety and privacy should be considered in project management.

Other information for health

See also 5.38 which considers analysis and specification. See also 5.34 which address privacy.

ISO 81001-1 provides extensive guidance on the interdependency of safety, effectiveness and security including project management issues. ISO 81001-1 also provides information on other relevant standards, particularly for medical devices.

5.9 Inventory of information and other associated assets

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.9 apply.

Control for health (supplementary)

All information flows (both within and between organizations) and their interfaces (including integration platforms), should be included in the inventory.

Purpose for health (supplementary)

To ensure that information flows and their interfaces are identified in order to preserve their information security and assign appropriate ownership.

Guidance for health

Besides assets such as equipment, devices and software components, health organizations increasingly become dependent on structural information flows (between areas within the organization's IT-landscape but also with outside parties) and associated interfaces, especially integration platforms.

Ownership can, at times, be difficult to determine in client-supplier situations. In such cases, the (contractual) agreement between parties can offer help; this also assists in establishing owner duties.

Other information for health

See Annex C for further information on asset ownership as well as the different types and uses of assets.

5.10 Acceptable use of information and other associated assets

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.10 apply.

5.11 Return of assets

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.11 apply.

Control for health (supplementary)

There should be a policy that requires written confirmation from individuals that all assets in their possession in all formats have been securely returned or deleted as appropriate.

Purpose for health (supplementary)

To protect personal health information as part of the process of changing or terminating employment, contract or agreement.

Guidance for health

The policy should include measures that can be taken against individuals if it is found, during or subsequent to change or termination of employment, contract or agreement, that not all assets have been returned or deleted as appropriate.

The written confirmation required by the policy should include all information that does not belong to an individual and that is held on their own personal equipment or held on the individual's behalf elsewhere (for example, storage and other services, including email, provided by cloud providers).

In cases where returning information held by an individual or on their behalf would result in unnecessary duplication, the policy may allow the individual to delete the information securely without returning it. The policy should stipulate the techniques to be followed to ensure secure deletion.

5.12 Classification of information

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.12 apply.

Control for health (supplementary)

Personal health information should be classified as confidential at a minimum.

Purpose for health (supplementary)

To ensure the proper classification of personal health information under all circumstances.

Guidance for health

Classification in healthcare can be challenging. The following factors should be taken into consideration.

— Legal, statutory, regulatory, contractual and local policy requirements for medical records and other personal health information vary significantly. In some cases, the requirements are based on rules for paper records and do not take sufficient account of information being held electronically. Other potential issues are unclear or inconsistent requirements. This often happens because requirements are constantly evolving and because there can be multiple sources of requirements. For example, personal health information, as a subset of PII, can be governed by overarching general data protection legislation as well as other requirements that are not specific to health.

— Within the realm of personal health information, it can be necessary to have a range of classifications. For example, information on a broken leg is clearly of a different degree than that regarding sexually transmitted diseases. There can be varying degrees between personal health information of a high-profile person with respect to that of other persons. Other degrees can evolve over time: some personal data can be less sensitive (for example, the difference between a mental health episode 10 years ago compared with a current one), while others can become more sensitive. Personal information can also become enriched with data from other sources, changing its classification. In addition, some personal health information can point to other persons: for example, family members with regard to genetics, or people with regard to harm they have inflicted (for example, in cases of child abuse).

Personal health information, all of which should be classified, can also come from wearable technology, implants and other medical devices. Special consideration should be given to genetic and biometric data particularly if legal, statutory, regulatory, contractual and local policy requirements on the topics are not sufficiently detailed or specific.

5.13 Labelling of information

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.13 apply.

Guidance for health

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 contain or constitute personal health information.

Consideration should be given to informing users, e.g. at each start up or log in. However, it can be sufficient to provide such information only the first time a particular user accesses a system.

5.14 Information transfer

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.14 apply.

Control for health (supplementary)

Rules, procedures and agreements should be in place prior to any transfer taking place.

Purpose for health (supplementary)

To ensure security of information transfer over its full life cycle.

Guidance for health

Organizations should ensure that the security of information exchange is the subject of policy development and compliance audit (see 5.36). Cryptographic techniques should be used appropriately.

The security of information exchanges can be greatly assisted by the use of information exchange agreements that specify the minimum set of controls to be implemented. Such agreements are binding on both (or more) information exchanging parties, whereas rules and procedures are generally only applicable within a single organization.

Policies should be in place to ensure that personal health and other confidential information exchanged over e-mail, instant messaging or in other forms is secure. If sufficient security cannot be achieved, such information should not be exchanged through these channels at all.

Other information for health

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

5.15 Access control

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.15 apply.

Control for health (supplementary)

Access to personal health information should be governed by a suitable policy such as role-based access control.

Purpose for health (supplementary)

To ensure access to personal health information is properly controlled.

Guidance for health

Control of access to personal health information

Access to personal health information should be controlled. In general, users of health information systems should only access personal health information:

a) when the user is part of the care team of the data subject (the subject of care whose personal health information is being accessed);

b) when the user is carrying out an activity on behalf of the data subject;

c) when there is a need for specific data to support this activity.

In order to prevent healthcare delivery being delayed or otherwise adversely affected, a clear policy and process, with associated authorization, to override the "normal" access control rules in emergency situations (sometimes referred to as "break the glass") can be necessary.

Control models

The organization should establish access policies using an appropriate control model in order to:

a) address the needs of predefined roles with associated authorities that are consistent with, but limited to, the needs of that role;

b) reflect professional, ethical, legal and subject-of-care-related requirements;

c) enable the tasks performed by health professionals or other authorized personnel and the tasks workflow.

Other information for health

Role-based access control (RBAC) and attribute-based access control (ABAC) are possible control models and are sometimes used in combination.

See also 5.34 on additional privacy considerations that can restrict access to personal health information and should be included as appropriate in the access control policy.

The ISO 22600 series provide further information on access control in health informatics.

5.16 Identity management

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.16 apply.

Control for health (supplementary)

Users who are to have access to personal health and other confidential information should be subject to a formal registration process.

Purpose for health (supplementary)

To ensure that each individual is allocated a correct user identity.

Guidance for health

The registration process should include rigorous checks to ensure that the identities allocated to users will be subject to appropriate authentication and that their access rights are consistent with their roles.

The registration process should, where applicable, include all of the following:

a) checking that the individual is who they claim to be;

b) verification of the individual's professional credentials, including whether they are currently valid;

c) accurate capture of the information associated with the individual;

d) assignment of a unique and unambiguous user identity.

For personnel who are new to an organization, the personal details – such as name, date of birth – should be checked against a suitable document such as a passport unless this has been done as part of the screening process (see 6.1 for further information).

Professional credentials should be verified with relevant registration, regulatory or professional bodies. Some professional credentials can be verified with digital certificates.

The registration process should accommodate varying types of users including health professionals, ICT staff with elevated rights as well as subjects of care and their support companions. All of these have different registration prerequisites.

Other information for health

It can be beneficial to coordinate identity management with activities relating to physical security. An example is the allocation of security passes that control access to rooms or locations. Another example is the allocation of identity badges or passes.

5.17 Authentication information

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.17 apply.

Guidance for health

Time pressures found in health delivery situations can make effective use of passwords difficult to employ. Health organizations should in such cases consider the adoption of alternative authentication technologies to address this problem.

Other information for health

See also 8.5.

5.18 Access rights

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.18 apply.

Guidance for health

Especially in large hospitals, significant numbers of staff will typically have short-term access to personal health information. The termination of the access rights of such staff needs to be carefully managed. Examples of such staff include students, interns, trainees and locums. Other examples include agency or equivalent staff, as well as permanent employees providing cover for other people's roles or shifts.

Another issue is that many transactions take place sometime after care events (for example, the sign-off of medical transcriptions) and in some cases the transactions take place a considerable time later. This can significantly complicate the process of removing access rights in a timely fashion and these transactions should be taken into account when designing and implementing procedures on the removal of access rights.

Immediate termination of access rights following the supply of a resignation notice, notice of dismissal, etc. should be considered, wherever an increased risk is perceived from the continuation of such access.

5.19 Information security in supplier relationships

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.19 apply.

Control for health (supplementary)

The risks associated with access by external parties to systems or the data they contain should be assessed, and controls that are appropriate to the assessed risk should be implemented.

Purpose for health (supplementary)

To manage and protect the external access of suppliers to systems and data.

Guidance for health

Risk assessment is essential for effectively managing third-party access to systems containing health information, especially personal health information.

Rights of subjects of care should be protected, even when a third party with potential access to personal health information is located in a jurisdiction different than the one governing the subject of care or health organization.

All personal health and other confidential information that could be accessed by suppliers for whatever reason, including provision of cloud services, processing, support, training or testing, should be encrypted.

There should be policies together with processes and procedures to ensure this is achieved and monitored. In some cases, for example certain medical devices, it is not possible to encrypt data and compensating controls based on a risk assessment should be implemented instead.

Other information for health

Depending on the systems, services and suppliers, information can potentially be accessed in many ways including use of application programs or utilities and tools that operate, for example, on databases, file systems or networks. Suppliers and their subcontractors can have administrative or other rights as well as diagnostic or privileged utilities that could enable or provide access to confidential information. It is difficult, if not impossible, for clients of suppliers to know the full extent of suppliers' capabilities. These factors should be taken into account when assessing risks with supplier relationships.

5.20 Addressing information security within supplier agreements

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.20 apply.

5.21 Managing information security in the ICT supply chain

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.21 apply.

Guidance for health

For medical devices incorporating health software the information that should be provided by manufacturers includes a disclosure statement for Medical Device Security (MDS2), configuration requirements, vulnerability assessments and a software bill of materials (SBOM).

Other information for health

See Annex D and ISO 81001-1.

5.22 Monitoring, review and change management of supplier services

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.22 apply.

5.23 Information security for use of cloud services

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.23 apply.

Other information for health

ISO/TS 23535 and ISO/TR 21332 provide information on security and privacy for cloud services used in health.

5.24 Information security incident management planning and preparation

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.24 apply.

Guidance for health

Information security incidents should not be assessed in isolation from other types of incidents, both in handling and in reporting. All types of incidents should be included in the information security incident management process. After all, a break-in could have led to theft of ICT hardware (leading to a confidentiality breach), or a fire could have been set to disguise misuse of ICT equipment, or an identified misuse or erroneous use of the system could have had clinical consequences, etc.

5.25 Assessment and decision on information security events

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.25 apply.

Guidance for health

The categorization and prioritization scheme should consider whether events involved either or both:

a) personal health information;

b) medical devices incorporating health software.

The scheme should also consider whether clinical activities were (potentially) affected.

5.26 Response to information security incidents

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.26 apply.

5.27 Learning from information security incidents

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.27 apply.

5.28 Collection of evidence

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.28 apply.

Guidance for health

Health organizations should consider the implications of collecting evidence for purposes of investigating clinical incidents.

5.29 Information security during disruption

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.29 apply.

5.30 ICT readiness for business continuity

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.30 apply.

Guidance for health

Organizations should identify processes, systems and other relevant equipment that are vital in healthcare delivery.

Contingency plans should include fall-back procedures as necessary in order to counter failure in processes, systems and other relevant equipment that are vital in healthcare delivery.

Reflecting the rigorous availability requirements in healthcare, particular attention should be paid to resilience and redundancy arrangements, both for technology as well as for personnel.

ICT continuity planning in healthcare should be suitably integrated within business continuity planning (e.g. plans for handling power failures, implementing infection control and dealing with other clinical emergencies).

The safety of subjects of care can depend upon access to their data and this should be taken into account during planning. Catastrophes and force majeure crises that would disable ICT systems in industrial and other sectors are the very events that can precipitate a health crisis in which timely access to health information is crucial.

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

Health organizations should remain cognizant of the role that health information systems play in continuity of care. Such organizations should be prepared if/when ICT systems fail.

Depending on the nature and duration of a system outage, it can be necessary to capture by other means data about subjects of care that would be recorded in the system under normal circumstances. Backup arrangements can include, for example, use of spreadsheets or paper forms. Contingency arrangements should ensure that information captured during outages is as accurate, complete and timely as possible.

Data captured during an outage will often need to be transferred or entered manually into systems once they are running again after the outage. Additional checks for accuracy, completeness and data integrity should be performed as part of the update processes.

5.31 Legal, statutory, regulatory and contractual requirements

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.31 apply.

5.32 Intellectual property rights

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.32 apply.

5.33 Protection of records

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.33 apply.

5.34 Privacy and protection of PII

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.34 apply.

Guidance for health

Access to personal health information should only be permitted where the user has a legitimate need to access a subject of care's records.

Where the user has a legitimate need, this does not necessarily mean the user is entitled to access all the subject of care's personal health information because legal, regulatory, professional, local policy or other requirements can result in additional access restrictions. For example:

a) access to personal health information concerned, for instance, with a subject of care's sexual health, mental health, contraception, any current pregnancy or the outcomes of any previous pregnancies can be restricted to the clinicians treating the specific conditions;

b) subjects of care can have rights to specify which of their health records are either accessible or not to particular users or groups of users;

c) subjects of care can have rights to access their own records but there can be requirements to withhold some information from them; this can apply to some mental health conditions or where there is information in a subject of care's health records about other individuals, such as relatives with related conditions or diagnoses, whose privacy has to be protected;

d) when certain health matters such as those listed in a) are being recorded, subjects of care can be given records under aliases or special identifiers and access to their true identification information is restricted;

e) certain subjects of care can be given aliases or special identifiers for all their records to prevent access to their true identities; this can apply, for example, to "very important persons" (VIPs), members of the security forces and victims of crime.

Additional considerations apply to access to records of children or adults who have proxies.

In cases where subjects of care or their proxies have rights to specify whether access to particular records should be granted or denied, suitable logs should be maintained. These logs should include details of advice given to subjects of care or their proxies and the decisions they subsequently take.

There are options for when access to part of a subject of care's records is denied. For example:

a) the information in question can be hidden altogether, so that the user is not shown that it is there at all;

b) the information can be obscured, or it can be replaced with text informing the user that certain information is restricted.

Legal, regulatory or local policy requirements can apply in situations where access is to be denied. Methods for denying access are considered in 8.11.

As noted in 5.15, it can be necessary to override certain access controls or restrictions in emergencies.

Special emphasis should 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. 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 should address these concerns.

All access to personal health information, including overrides of access restrictions (for example for emergency access), should be logged (see 8.15 and, for the rights of subjects of care, ISO 27789:2021, 5.2.2). Unauthorized access attempts or suspicious patterns (such as excessive record views) should generate alerts for immediate investigation.

Other information for health

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

ISO/IEC 27701 is an extension to ISO/IEC 27001 and ISO/IEC 27002 that provides requirements and guidelines for privacy information management. Many of the controls can be applied in health.

See also Annex D.

5.35 Independent review of information security

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.35 apply.

Guidance for health

Because of the specialized nature of healthcare, including the interdependencies between safety and information security, the use of independent reviewers with an understanding of the sector should be considered.

Although not necessarily performed by relevant experts and not strictly independent, assessment by colleagues from a peer organization can act as a useful supplement to formal independent reviews.

5.36 Conformance with policies, rules and standards for information security

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.36 apply.

Guidance for health

A compliance auditing programme should be in place that addresses the full life cycle of operations, to

a) identify issues,

b) review outcomes, and

c) decide on updates to the ISMS.

The audit programme should be formally structured within a 12-month to 18-month cycle, to cover

a) all elements of this document,

b) all areas of risk, and

c) all implemented controls.

Where applicable, the information security advisory group (see 5.2) should set itself the objective of establishing a graduated compliance auditing framework, whose bottom layer is self-audit by the process operators and managers. Thereafter, the auditing of the ISMS, on behalf of the information security advisory group, internal auditing, controls assurance assessments and finally external audits, should be defined in a manner that allows each layer to draw confidence from all of the layers below it.

5.37 Documented operating procedures

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 5.37 apply.

5.38 HLT – Information security requirements analysis and specification

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

The information security-related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Purpose

To ensure information security risks related to the development or acquisition, or both, of information systems are effectively addressed throughout the information system life cycle.

Guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the value of the information involved (see 5.12 and 5.13) and the potential negative impact that can result from lack of adequate security. The implications for safety should also be considered.

Identification and management of information security requirements and associated processes should be integrated in the early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage, can lead to more effective and cost-efficient solutions.

Information security requirements should also consider:

a) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

b) access provisioning and authorization processes, for all types of users including privileged or technical users;

c) informing users and operators of their duties and responsibilities;

d) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

e) requirements derived from operational processes, such as transaction logging and monitoring, nonrepudiation requirements;

f) requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated control 8.26 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software or service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined (for example, in terms of their functionality), which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Other information

See Annex D.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

5.39 HLT – Uniquely identifying subjects of care

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

There should be policies and procedures to ensure there is a single unique identifier for each subject of care, and functionality to merge duplicate or multiple records in cases where they exist for the same subject of care.

Purpose

To prevent incomplete or inconsistent information and records about subjects of care.

Guidance

Emergency care and other situations in which adequate identification of a subject of care has not been possible can result in instances of multiple records for the same subject of care. In addition, subjects of care can have multiple records for administrative reasons such as the merger or takeover of previously separate health organizations at which they have been treated.

Health information systems should have the facility to merge multiple records for a subject of care into a single record. Merging requires great care, trained personnel and appropriate technical tools to facilitate the integration of information from the original records into a unified whole.

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

5.40 HLT – Validation of displayed/printed data

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

When any of an individual's personal health information is displayed or printed, information that identifies the subject of care should be included.

Purpose

To enable confirmation that information is for the correct subject of care and to prevent use of information that relates to someone else.

Guidance

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

Health information systems should make it possible to check that hardcopy print-outs are complete (for example, "page 3 of 5").

5.41 HLT – Publicly available health information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Integrity	#Protect	#Governance, #Asset_management, #Information_protection, #Legal_and_compliance	#Protection, #Defence

Control

Publicly available health information should be protected, traceable, preserved and managed throughout its life cycle.

Purpose

To ensure publicly available health information is available when required, its integrity is maintained, its provenance is recorded, there is an audit trail, and historical information is retrievable.

Guidance

Publicly available health information (as distinct from personal health information) can be found at websites and, for instance, in portals. It can often take the form of medical advice. For instance, information on when to make an appointment with a doctor, midwife or other clinician, as opposed to visiting the emergency

department immediately. Information, including side-effects, on prescription and other medications is also often publicly available along with explanations of the diagnosis and treatment of many conditions.

Important decisions can be made by subjects of care, their companions or proxies based on publicly available health information. Health professionals can also rely on such information. It is therefore considered essential that publicly available health information is reliable, accurate and up-to-date. To ensure this:

a) the integrity and availability of the information should be protected;

b) the origin of the information should be stated and its provenance should be checked before it is made available;

c) there should be a full audit trail so it is evident which personnel created, amended, deleted or performed other actions on the information;

d) a comprehensive archive of the information should be maintained and there should be a facility to access the historical information in order to establish what content was available at any particular time.

Other information

Similar principles should be applied for information on intranets, internal knowledge bases and similar resources that are only available to personnel within an organization.

5.42 HLT – Emergency communication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond, #Recover	#Governance, #Information_protection, #Human_resource_security, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Information_security_event_management, #Information_security_assurance	#Protection, #Defence, #Resilience

Control

Emergency communication channels within a health organization that function when the organization's ICT continuity has failed should be planned, implemented, maintained and tested.

Purpose

To ensure that essential communications are possible during an ICT outage.

Guidance

Interpersonal communication increasingly uses ICT, resulting in a corresponding increase in dependence on ICT. If there is an ICT failure, communication using ICT will quickly become impossible. That is not acceptable for providing care. Therefore, emergency communication that does not rely on (organizational) ICT should be planned, implemented, maintained and its effectiveness tested regularly. For instance, mobile communication can be used instead of network communication, and paper forms can be used to communicate pathology requests and results.

5.43 HLT – External incident reporting

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective, #Corrective	#Integrity, #Availability	#Respond	#Governance, #Threat_and_vulnerability_management, #Supplier_relationships_security, #Legal_and_compliance	#Governance_and_Ecosystem

Control

Legal, statutory, regulatory and contractual requirements applying to reporting information security incidents should be identified, documented and kept up to date.

Purpose

To ensure that legal, statutory, regulatory and contractual obligations regarding information security incidents are met.

Guidance

In healthcare and elsewhere, the need for reporting information security incidents to authorities or contractual partners, or both, is growing. It enables such parties to quickly uncover patterns in cybercrime. To ensure that such reporting obligations are met, an inventory of such obligations should be established. Based on this:

a) parties within the organization should be appointed who are responsible for (groups of) individual reports;

b) the scope (length and breadth) of each report should be established based on a balance between reporting requirements and the protection of personal (health) information.

Every time an external incident report has been submitted, management should be informed of this.

Other information

See also 5.31.

6 People controls

6.1 Screening

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 6.1 apply.

Guidance for health

All organizations processing personal health information should have a policy for screening personnel. As a minimum, the policy should require verification of identity, current address and previous employment.

Background checks on all candidates to become personnel should include a verification of applicable health professional qualifications and, where applicable, that they are accredited or licensed to practice. Where applicable, criminal background checks should be undertaken. All checks should be repeated regularly.

6.2 Terms and conditions of employment

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 6.2 apply.

Control for health (supplementary)

Job descriptions should state the security roles and responsibilities that apply to processing of personal health information.

Purpose for health (supplementary)

To ensure privacy of subjects of care is emphasized and understood.

Guidance for health

Organizations should ensure that personnel have a duty to report breaches of health information security or subject of care privacy.

Policies should address all types of personnel whether permanent or not, including:

a) clinicians who are temporary or visiting, such as locums, trainees, interns, students and "on-call" or agency staff;

b) personnel who are supporting direct care, including administrative and support staff as well as clergy, charity workers and other volunteers.

Other information for health

See Annex C for further information on the workforce in health organizations.

6.3 Information security awareness, education and training

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 6.3 apply.

Guidance for health

Awareness, education and training can include regular assessment or testing, or both.

Social engineering threats are a particular concern for health organizations. Examples of people who are impersonated include:

a) clinicians or other healthcare staff within the organization or external to it;

b) relatives or friends of subjects of care;

c) police, social services staff or, for children, teachers and other school staff.

Awareness, education and training should take appropriate account of social engineering. This should include encouragement of prompt reporting (see 6.8) of social engineering attempts, whether successful or otherwise.

6.4 Disciplinary process

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 6.4 apply.

Guidance for health

The disciplinary process should state (both as a deterrent and because it can be necessary) that, for serious violations, individuals will be reported to one or more external bodies.

For example, clinicians could be reported to their regulatory or registration body. Students and trainees could be reported to the academic institution they are associated with.

6.5 Responsibilities after termination or change of employment

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 6.5 apply.

Guidance for health

Many doctors, nurses and other clinicians progress through training programmes and other "rotations" where their clinical duties, and the subjects of care they are involved in the care of, can change fundamentally.

Organizations should inform the subject of care whenever personal health information has been inappropriately disclosed. In some jurisdictions, this can be required by law. In many jurisdictions there is a legal requirement to report data breaches involving PII to the data subjects whose personal information has been breached.

6.9 HLT – Management training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive, #Corrective	#Confidentiality, #Integrity #Availability	#Protect, #Respond, #Recover	#Governance, #Legal_and_compliance, #Information_security_assurance	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

Control

Management of the organization should receive appropriate training, as relevant for their roles and responsibilities with regard to information security and how it is managed.

Purpose

To ensure that management can fulfil its roles and bear its responsibilities with regard to the ISMS.

Guidance

The management of the organization is awarded various roles and responsibilities through this document, ISO/IEC 27002 and elsewhere. The specific roles and responsibilities should be inventoried. Then, a gap analysis should be performed in order to establish which training is needed.

Since the membership of the organization's management teams can change regularly, the steps above should be repeated as necessary.

Management training should include crisis response simulations for cyber incidents such as ransomware attacks and data breaches.

Other information

See also 6.3.

7 Physical controls

7.1 Physical security perimeters

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.1 apply.

Guidance for health

Many operational areas are permeated by subjects of care. At the same time, the physical safety and security of the public (subjects of care and their support companions), as well as of the data and systems that can be accessible within that environment, should be preserved. For example, a subject of care can be left unattended in an examining room (for example, to allow the subject of care to change into a gown for physical examination), despite the presence of a functioning workstation in the room. Workstation security in healthcare cannot therefore depend entirely upon the exclusion of subjects of care from a security perimeter.

In healthcare, situations can arise where subjects of care (or others) do not always act rationally. This can apply, for example, to young children, people with mental health issues, people who have recently been confronted with distressing news, neurodivergent people, people under the influence of substances such as drugs or alcohol, and so on. Physical security measures should reflect this appropriately.

Consideration should be given to the security of ICT equipment (including mobile phones) belonging to subjects of care while they are unable to provide for security themselves.

Physical security measures for data and systems should be coordinated with more general physical security and safety measures.

7.2 Physical entry

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.2 apply.

Guidance for health

The provision of healthcare includes distinct circumstances where the public (subjects of care and their support companions) are physically admitted into areas where sensitive information is being processed. Physical areas where health information is gathered and/or that contain systems where data are viewed on screen should therefore be subject to additional precautions.

In certain cases, personal health information is displayed on screens and is visible to people who are not entitled to see it. An example is the screen that is presented to a subject of care during the administrative phase of admission and possibly can be read by the next in line. Another example is large informational displays (screens or whiteboards) showing the room or bed allocation on a ward. These displays are intended for use only by clinical and other personnel but can be read by all visitors to the ward. In such cases, information disclosure to unauthorised persons should be prevented, for instance, by changing the location or placement of said displays.

7.3 Securing offices, rooms and facilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.3 apply.

7.4 Physical security monitoring

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.4 apply.

7.5 Protecting against physical and environmental threats

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.5 apply.

7.6 Working in secure areas

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.6 apply.

7.7 Clear desk and clear screen

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.7 apply.

Guidance for health

In cases where the facilities are provided, care should be taken to ensure that timeout and automatic logout features are appropriately configured.

Particular care is needed in certain areas such as operating theatres and intensive care units where it can be necessary to disable timeouts and automatic logouts for safety reasons. In such cases, appropriate procedures should be in place to prevent unauthorized viewing or other activities when use of items of equipment or

devices is definitely not required. However, caution is necessary because devices and equipment can be in use even if unattended or displays are not viewed for prolonged periods.

7.8 Equipment siting and protection

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.8 apply.

Guidance for health

ICT equipment and medical devices incorporating health software can require special security considerations about the environment in which they operate and to the electromagnetic emissions that occur during their operation. Health organizations, especially hospitals, should ensure that siting and protection of such equipment and devices minimises exposure to such emissions.

7.9 Security of assets off-premises

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.9 apply.

Guidance for health

Organizations should ensure that any use, outside their premises, of medical devices incorporating health software has been authorized. This includes equipment used by remote workers, even where such usage is for an indefinite period (i.e. where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, etc.), and equipment used by subjects of care.

7.10 Storage media

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.10 apply.

Control for health (supplementary)

All personal health information stored on removable media should be encrypted.

Purpose for health (supplementary)

To prevent misuse of personal health information including unauthorized access, disclosure or modification.

Guidance for health

The most commonly recognized types of removable storage media are secure digital (SD) cards and universal serial bus (USB) drives.

Subscriber identity module (SIM) cards are also removable in many cases and often hold confidential information. In addition to mobile phones, devices, including tablets and laptops can incorporate SIMs. SIMs are used in many other circumstances including, for example, remote monitoring systems for building and facilities management, building security alarms, and motor vehicles.

Many items of equipment can include in-built storage including hard drives, solid-state drives (SSDs) and non-volatile memory. However, the presence of such storage is not always documented, evident or expected. Examples include printers (particularly those intended for more than one computer or user and that are networked), stand-alone copiers, and medical devices incorporating health software.

Maintenance, repair and disposal of any equipment containing storage requires additional precautions.

Other information for health

Regarding equipment maintenance see 7.13, regarding secure disposal of re-use of equipment see 7.14 and regarding encryption see 8.24.

7.11 Supporting utilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.11 apply.

Guidance for health

Electrical power is essential for many aspects of healthcare and loss of power, particularly to certain medical devices, can result in serious harm to subjects of care. For this reason, many hospitals and other healthcare premises have emergency electrical supplies, which continue to provide power (often through specially designated outlets) to essential medical or ICT equipment and devices in the event of a major supply failure.

Emergency power can be provided in different ways, but the quality is not always the same as a normal supply. For example, there can be voltage and frequency fluctuations or other variations. This is also the case when switching (in either direction) between the normal and emergency power supplies takes place. Therefore, even if equipment is protected by connection to an emergency supply, additional measures (such as dedicated uninterruptible power supplies) can be necessary in certain circumstances. There is considerable evidence that, when needed, emergency supplies do not always operate as intended, for example because stand-by generators fail or emergency supplies are overloaded. Therefore, appropriate contingency measures for such events should be considered.

7.12 Cabling security

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.12 apply.

Guidance for health

Measures should be taken to prevent unauthorized access through network outlets in publicly accessible and other areas. The following should be considered:

— disabling ports that are not in use (either physically at patch panels for example or, if available, with suitable network administration tools);

— disabling any form of access (including traffic monitoring) to devices that have not been previously authorized;

— use of intrusion detection tools;

— monitoring unexpected physical disconnection of devices – this can indicate a network cable has been unplugged to enable connection of an unauthorized device instead.

Network outlets are also vulnerable to physical damage. Children and some adults can be destructive, whether accidentally or intentionally. Precautions should be taken to prevent the insertion of objects or substances into outlets by young children, particularly in wards dedicated to them.

Other information for health

See 7.1 for other physical security considerations.

7.13 Equipment maintenance

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.13 apply.

Guidance for health

Patient safety should be taken into account both when preparing for and when undertaking all equipment maintenance activities.

Policies should be in place for safe and secure equipment maintenance. A maintenance plan, including both an up-to-date risk assessment and contingency arrangements, should be developed in accordance with the

relevant policies. Before maintenance takes place, the completed plan should be approved in writing by senior management.

In all cases, steps should be taken to ensure that there are no unexpected events, particularly outages (such as loss of network connectivity), that affect systems and devices dependent on the equipment being maintained. Special care should be used when maintenance is being undertaken remotely or by a third party.

7.14 Secure disposal or re-use of equipment

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 7.14 apply.

Guidance for health

Almost all digital equipment has some form of non-volatile storage, whether or not the equipment has internal (solid-state or hard) disks or ports for removable storage media. This includes medical devices incorporating health software. In addition, non-medical devices, such as printers, and network equipment can log or store health or other confidential information (such as network configurations).

Medical devices and equipment can have specific disposal protocols. For example, decontamination as well as other processes can be required to avoid subsequent risk to health. Organizations should ensure that arrangements for disposing of medical devices and equipment include checks for any storage media.

Other information for health

See 7.10 for further information on storage media.

8 Technological controls

8.1 User endpoint devices

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.1 apply.

Other information for health

User endpoint devices can include mobile devices such as smartphones, portable medical devices and wearables.

8.2 Privileged access rights

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.2 apply.

Other information for health

Guidance on privilege management in healthcare can be found in the ISO 22600 series.

8.3 Information access restriction

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.3 apply.

8.4 Access to source code

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.4 apply.

8.5 Secure authentication

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.5 apply.

Control for health (supplementary)

At least two factor authentication should be used for systems that process personal health information.

Purpose for health (supplementary)

To ensure greater security for access to personal health information.

Guidance for health

Special consideration should be given to the technical measures by which subjects of care are securely authenticated when accessing all or part of their own information (in those health information systems that permit such access).

Consideration should also be given to the ease of use of such measures for subjects of care who have accessibility or other issues. Additional consideration should be given to the subject of care proxies.

8.6 Capacity management

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.6 apply.

Guidance for health

The proportion of medical devices that either can or need to be connected (whether wirelessly or by cable) to a network is increasing rapidly and capacity management should take account of this. Other factors that should be considered are the potentially high and rising levels of demand both for patient entertainment systems and on guest networks.

8.7 Protection against malware

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.7 apply.

Guidance for health

Where installation of software that protects against malware is possible in medical devices incorporating health software, that anti-malware software can interfere with the safe operation of such devices. Software that protects against malware should only be installed or updated in accordance with both the manufacturers' instructions and local policies.

In cases where the use of anti-malware software is not possible, compensating controls, based on a risk assessment, should be implemented as necessary.

8.8 Management of technical vulnerabilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.8 apply.

Guidance for health

In large-scale environments, there can be considerable exchange of data both within and between organizations. This exchange can take place across many different interfaces and can be between large numbers of systems and devices, and use a wide range of technologies. Detailed consideration of technical vulnerabilities resulting from these interfaces should be undertaken.

For some medical devices incorporating health software, it is either not possible at all or not appropriate for clinical safety reasons to take measures, such as updating software or applying patches, in the same way as on standard ICT equipment. In cases where it is not possible to update software or apply patches, compensating controls, based on a risk assessment, should be implemented as necessary.

Other information for health

See Annex C for further information.

8.9 Configuration management

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.9 apply.

Guidance for health

Configuration of connections

Health IT systems that interoperate with other systems within the organization and externally in order to enable an interoperable electronic health record are configured initially to conform to the suggested guidance. They should also be maintained in order to continue to enforce the adopted standards as the parameters of their connections change, whether those changes are due to systems changes under the control of the organization or due to changes external to the organization.

Configuring medical devices

For patient safety reasons, it is often a legal or local policy requirement that medical devices are configured and maintained by qualified or licensed clinical engineers/scientists.

Many medical devices incorporating health software can exchange information with other devices or health IT systems. Such information exchange can take place through permanent or temporary network connections or by other means such as direct connection. The relevant interfaces are typically the responsibility of ICT professionals who, in some cases, also support operating systems, system utilities, database software and anti-malware software on certain medical devices.

Accordingly, both clinical engineers/scientists and ICT professionals can have responsibilities for (different or overlapping) aspects of the same items of equipment. Configuration management should take account of these issues.

Similar considerations apply to areas other than medical devices. For example, certain items of equipment for delivering medical gases, subjects of care call systems as well as building and facilities management systems are often networked but the responsibility of qualified or licensed engineers. Engineers with such responsibilities are often not clinical engineers/scientists.

8.10 Information deletion

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.10 apply.

Guidance for health

Consideration should be given to situations where information is (temporarily) stored on devices that are not managed by the organization. Examples of such situations are "bring your own device" and access to information through personal computers that are privately owned.

Other information for health

See also 7.10 and 7.14 in connection with storage media and circumstances under which information should be deleted.

8.11 Data masking

The control, associated attribute table, purpose and other information as given in ISO/IEC 27002:2022, 8.11 apply.

Guidance for health

The guidance given in ISO/IEC 27002 applies with the exception of b) and c) of the items that "should be considered when implementing data masking techniques". For health, these issues are covered in 5.34 of this document.

Other information for health

For information on pseudonymization in health see ISO 25237.

8.12 Data leakage prevention

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.12 apply.

8.13 Information backup

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.13 apply.

Control for health (supplementary)

Personal health information should be backed up in an encrypted format.

Purpose for health (supplementary)

To protect confidentiality of personal health information.

Guidance for health

As a general precaution and specifically to avert ransomware attacks, measures such as storing backup data offline or adopting an immutable backup technology should be considered.

Other information for health

See 8.24 regarding the use of cryptography.

8.14 Redundancy of information processing facilities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.14 apply.

8.15 Logging

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.15 apply.

Other information for health

Guidance on audit trails for electronic health records can be found in ISO 27789.

8.16 Monitoring activities

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.16 apply.

8.17 Clock synchronization

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.17 apply.

8.18 Use of privileged utility programs

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.18 apply.

Guidance for health

As explained in 8.9, professionals from different disciplines can have (different or overlapping) responsibilities for aspects of particular items of equipment. Policies and procedures for use of privileged utility programs should take account of these issues.

8.19 Installation of software on operational systems

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.19 apply.

Guidance for health

The delivery of care in a healthcare organization can include hardware devices and software installations that are certified for safe operation with very specific configuration parameters. In certain cases, the certification can prohibit changing any part of the software stack, including making security patches. In such cases, the organization should record known vulnerabilities in operational systems and the mitigations employed to enable the continued safe operation of those systems.

8.20 Networks security

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.20 apply.

8.21 Security of network services

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.21 apply.

Guidance for health

The impact of loss of network service availability of the (clinical) practice should be considered. See also 5.29.

8.22 Segregation of networks

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.22 apply.

Guidance for health

Patching, software or firmware upgrades, and the use of software that protects against malware are all techniques that help to maintain security. In some cases (for example, certain medical devices incorporating health software), the use of these techniques is restricted (see Annex C) and compensating controls are necessary. One such control to protect otherwise vulnerable assets is network segregation.

Segregation of patient entertainment systems is often advisable.

Other information for health

See 8.35.

8.23 Web filtering

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.23 apply.

Guidance for health

Policies should be in place to avoid incorrect blocking of content that is relevant to healthcare. Such policies should cover handling false positives appropriately.

By default, web filtering systems often block text, images, drawings, videos and other types of content that are entirely appropriate in healthcare but unacceptable in many other contexts. There is a wide range of such content. In addition to anatomical terms and images, examples include content relating to drug use, the results of violence and self-harm, abuse of children and vulnerable adults.

False positives can affect the delivery of healthcare and should be reviewed without undue delay. Correspondingly, there are risks that it is possible to access inappropriate material, under the pretext that it is for legitimate healthcare purposes, and steps should be taken to monitor this.

8.24 Use of cryptography

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.24 apply.

Other information for health

Guidance on policy for issuing and use of digital certificates in healthcare and on the management of keys can be found in ISO 17090-3.

8.25 Secure development life cycle

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.25 apply.

8.26 Application security requirements

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.26 apply.

Guidance for health

Consideration should be given to the possibility that personal health information is not necessarily recognized as such, or at least not immediately. This can occur with information about payments or eligibility for healthcare in respect to an individual. Of special concern are circumstances in which personal health information can be derived, for example from metadata related to patient communication.

Other information for health

Annex D can be used for the evaluation of security requirements during the development or acquisition of applications.

8.27 Secure system architecture and engineering principles

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.27 apply.

8.28 Secure coding

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.28 apply.

8.29 Security testing in development and acceptance

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.29 apply.

Guidance for health

Acceptance criteria should be established for planned new information systems, upgrades and new versions. Suitable testing of such systems, upgrades and versions should be carried out prior to acceptance.

Acceptance testing of clinically relevant system features should involve clinical users.

8.30 Outsourced development

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.30 apply.

8.31 Separation of development, test and production environments

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.31 apply.

Guidance for health

Development and testing environments for systems processing health information, as well as training environments, should be separated from production environments hosting those health information systems.

Rules and authorization for the deployment of software from development to production status should be defined, documented and implemented.

Testing should not take place in production environments and should not be performed on personal health information.

8.32 Change management

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.32 apply.

Guidance for health

Inappropriate, inadequately tested or incorrect changes to the processing of personal health information can have adverse consequences for the delivery of care and patient safety.

The change process should explicitly record, assess and manage the risks of the change.

8.33 Test information

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.33 apply.

Guidance for health

Actual personal health information should not be used as test data, but steps should be taken to ensure that test data are realistic (see for instance 8.11).

8.34 Protection of information systems during audit testing

The control, associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002:2022, 8.34 apply.

8.35 HLT – Zero trust principles

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection, #System_and_network_security, #Identity_and_access_management	#Protection, #Defence

Control

Groups of information services, users and information systems that are assigned to a network segment should be kept as small as possible and should only have access to another network segment after both segments involved have authenticated each other.

Purpose

To ensure that entities connected to a network are not trusted by default.

Guidance

Zero-trust security is also known as perimeter-less security. The main concept is "never trust, always verify", which means that information services, users and information systems should not be trusted by default.

Zero-trust is implemented by:

a) establishing strong identity verification;

b) validating device compliance prior to granting access;

c) ensuring least privilege access to only explicitly authorized resources;

d) mutual authentication, including checking the identity and integrity of users and devices without respect to location;

e) providing access to information systems and information services based on system/device identity and security status in combination with appropriate authentication.

Other information for health

See 8.22.

Annex A
(informative)

Information security controls for health reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in Clauses 5 to 8 and can be used in context with ISO/IEC 27001:2022, 6.1.3.

If the control title contains "HLT", then the control is not included in ISO/IEC 27001:2022, Annex A.

If the control title does not contain "HLT", then the control is supplementary to the corresponding one in ISO/IEC 27001:2022, Annex A.

Table A.1 — Information security controls for health

Subclause	Control title	Control
5.1	Policies for information security	The information security policy should set out the approach to managing information security and be approved by the highest management level, then reviewed at least annually and after the occurrence of any serious security incident.
5.2	Information security roles and responsibilities	There should be at least one individual responsible for information security.
5.9	Inventory of information and other associated assets	All information flows (both within and between organizations) and their interfaces (including integration platforms) should be included in the inventory.
5.11	Return of assets	There should be a policy that requires written confirmation from individuals that all assets in their possession in all formats have been securely returned or deleted as appropriate.
5.12	Classification of information	Personal health information should be classified as confidential at a minimum.
5.14	Information transfer	Rules, procedures and agreements should be in place prior to any transfer taking place.
5.15	Access control	Access to personal health information should be governed by a suitable policy such as role-based access control.
5.16	Identity management	Users who are to have access to personal health and other confidential information should be subject to a formal registration process.
5.19	Information security in supplier relationships	The risks associated with access by external parties to systems or the data they contain should be assessed, and controls that are appropriate to the assessed risk should be implemented.
5.38	HLT – Information security requirements analysis and specification	The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.
5.39	HLT – Uniquely identifying subjects of care	There should be policies and procedures to ensure there is a single unique identifier for each subject of care, and functionality to merge duplicate or multiple records in cases where they exist for the same subject of care.
5.40	HLT – Validation of displayed/printed data	When any of an individual's personal health information is displayed or printed, information that safely identifies the subject of care should be included.
5.41	HLT – Publicly available health information	Publicly available health information should be protected, traceable, preserved and managed throughout its life cycle.

Table A.1 *(continued)*

Subclause	Control title	Control
5.42	HLT – Emergency communication	Emergency communication within a health organization that functions when ICT continuity has failed should be planned, implemented, maintained and tested.
5.43	HLT – External incident reporting	Legal, statutory, regulatory and contractual requirements applying to reporting information security incidents should be identified, documented and kept up to date.
6.2	Terms and conditions of employment	Job descriptions should state the security roles and responsibilities that apply to processing of personal health information.
6.6	Confidentiality or non-disclosure agreements	All personnel authorized to access personal health information should be formally bound to treat such information confidentially.
6.9	HLT – Management training	Management of the organization should receive appropriate training, as relevant for their roles and responsibilities with regard to information security and how it is managed.
7.10	Storage media	All personal health information stored on removable media should be encrypted.
8.5	Secure authentication	At least two factor authentication should be used for systems that process personal health information.
8.13	Information backup	Personal health information should be backed up in an encrypted format.
8.35	HLT – Zero trust principles	Groups of information services, users and information systems that are assigned to a network segment should be kept as small as possible and should only have access to another network segment after both segments involved have authenticated each other.

Annex B
(informative)

Correspondence of this document with ISO 27799:2016

The purpose of this annex is to provide backwards compatibility with ISO 27799:2016 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls for health specified in Clauses 5 to 8 of this document with those in ISO 27799:2016, and should be used in conjunction with ISO/IEC 27002:2022, Annex B.

Table B.1 — Correspondence between HLT-controls for health in this document and in ISO 27799:2016

ISO 27799:2025 control identifier	ISO 27799:2016 control identifier	Control name
5.38	14.1.1	HLT – Information security requirements analysis and specification
5.39	14.1.1.1	HLT – Uniquely identifying subjects of care
5.40	14.1.1.2	HLT – Validation of displayed/printed data
5.41	14.1.3.1	HLT – Publicly available health information
5.42	New	HLT – Emergency communication
5.43	New	HLT – External incident reporting
6.9	New	HLT – Management training
8.35	New	HLT – Zero trust principles

Annex C
(informative)

Information security in health organizations

C.1 Introduction

This Annex provides an outline of certain information security considerations in healthcare. It is intended principally for:

— information security experts including penetration testers and other professionals, such as auditors, with ICT expertise but who are unfamiliar with the health domain;

— medical device, engineering and ICT professionals who work in health organizations and, as such, can have responsibilities for equipment, systems or services that rely on digital technology.

The important subject of the interdependency of security, safety and effectiveness throughout the life cycle of health software and health IT systems is covered briefly in the Introduction of this document. It is not explored further here but is comprehensively addressed in ISO 81001-1 and related IEC standards.

C.2 Safety of medical devices and equipment

C.2.1 Context

Medical devices and other items of medical equipment that do not perform as intended have the potential to harm patients or other subjects of care.

Depending on the circumstances, harm can be apparent immediately or there can be a delay before harm manifests itself. Some incidents of harm only affect one individual whereas others can affect many people.

In the worst cases, incidents are fatal. However, it can also be devastating for individuals and others, such as family members, when incidents lead to consequences such as irrecoverable and lifelong suffering. In addition, if the results of such harm include the need for 24 hour a day care, the financial consequences are extreme.

In order to minimize the risk of harm, the entire life-cycle of all types of medical device (many of which do not rely on digital technology) and related equipment is heavily standardised and strictly regulated.

C.2.2 Professional responsibility and accountability

Once deployed in health organizations, the safety of all types of medical devices has to be maintained. This is usually the responsibility of professionals such as clinical engineers, clinical scientists, bio-engineers or (particularly when ionizing radiation is involved) medical physicists. The precise naming and nature of these roles, as well as the division of responsibilities between them, depends on the devices in question, jurisdictional requirements and local policies. Collectively, however, the individuals performing the roles are termed medical device professionals here.

Similarly, in health organizations, building facilities and building management systems are frequently the responsibility of engineering professionals, often known as hospital engineers. That term is also used here. In some health organizations, hospital engineers also have responsibility for all medical devices.

In many sectors other than health, professionals in ICT or similar departments typically have responsibility for assets that rely on digital technology and this responsibility can include information security.

However, the responsibilities of medical device professionals and hospital engineers can extend to many aspects of information security. Their departments will normally be provided with instructions by the manufacturers of assets that depend on digital technology, on relevant information security measures and tasks or activities that need to be undertaken.

Depending on the type of asset, these tasks can include: patch installation, software or firmware upgrades, configuration changes, updating software that protects against malware and so on. The assets typically have to be (taken safely) out of service before such tasks can be undertaken. Afterwards, the assets have to be put back into service. This can involve testing, recalibration or other activities that only the relevant professionals are permitted to undertake.

Many of the assets that are the responsibility of medical device or hospital engineering professionals rely on (cabled or wireless) networking or are accessed from end-user equipment such as PCs, laptops or other mobile devices. In addition, manufacturers of medical devices incorporating health software can require networks and end-user equipment (including apps running on it) to be configured in particular ways to support medical device operation or for information security reasons.

However, the networking and end-user equipment is often the responsibility of ICT professionals. It is therefore possible for information security responsibilities to overlap, and it is essential that all the professional groups coordinate their activities. Such coordination is also essential to ensure, for certain devices and systems, that information security activities are not overlooked on the assumption that another professional group is attending to them.

C.3 Asset ownership and organizational obligations

C.3.1 General

Identification of all assets that use digital technology and that a health organization utilizes or is dependent on is critically important. Establishing responsibility and accountability for all assets that use digital technology is also essential.

Particularly in large health organizations, maintaining inventories can be complicated because of the large number of assets and frequent movement or other changes.

Some relevant factors are outlined in following subsections.

C.3.2 ICT and medical devices

C.3.2.1 Asset sources and acquisition

Depending on the nature of the health organization, assets that use digital technology can enter it by various means. Some of these means can be unofficial.

Assets that use digital technology and that are deployed in a health organization can be:

— purchased by it;

— hired, leased or rented by it;

— provided to it as part of a contracted service;

— loaned to it – for example from medical device manufacturers or pharmaceutical companies providing items for direct evaluation or to support clinical trials;

— donated to it – for example by charitable foundations;

— imposed on it;

— developed, built or constructed within it;

— shared.

In addition, some parts or units of health organizations can have considerable autonomy. This can apply to organizations that are geographically dispersed. It can also apply for example, in large health organizations in which (groups of) departments or clinical specialties are authorized to acquire and implement at least some assets that use digital technology without needing approval or oversight from any central or corporate functions in the organization.

C.3.2.2 Asset sharing and other types of organization

A health organization can be associated with other health-related organizations (or departments within them) including:

— medical schools and other bodies that provide education and training to existing and aspiring (i.e. students, trainees and so on) health professionals;

— clinical research units and institutions;

— other academic bodies undertaking clinical, medical or health-related research;

— university departments (such as engineering, physics and computer science) researching or developing one or more of: techniques, devices, equipment and software to improve digital solutions for health and medicine.

Assets that use digital technology and which are owned or under the control of these other organizations are, in some circumstances, shared with the health organization. In some cases, such assets are used exclusively by the health organization.

Correspondingly, some of the health organization's assets that use digital technology can be shared with the other organizations or their departments.

Although it can be more challenging, maintaining the information security of the assets in all these shared situations is essential and ensuring that there is no doubt about which organization retains that responsibility is a critical factor.

C.3.2.3 Other asset flows

Particularly if they need more specialist care elsewhere, subjects of care can be transferred urgently between health organizations. It is possible for some equipment, including medical devices incorporating health software, to be transferred with the subject of care in such circumstances.

In other cases, subjects of care may be provided, temporality or permanently, with medical devices incorporating health software for use when they are no longer on a health organization's premises. This can apply for example to monitoring equipment or implanted devices.

C.3.2.4 Assets owned by the workforce or subjects of care

Depending on their use, some assets owned by members of the workforce or subjects of care need to be included in inventories. This applies, for example, if software licensing rules have to be enforced or it is necessary to be able to remotely wipe equipment.

C.3.3 Building and facilities management systems

Health organizations can operate from a variety of premises. Some premises are owned or under the control of the health organizations that are based in them, but this is not always the case. For instance, health organizations can operate from buildings with multiple purposes (including offices, retail, or both) or share premises, such as outpatient clinics, with other health organizations.

In premises that are not wholly under the control of the health organization, it is important that necessary information security activities are performed on the facilities and building management systems and to identify which parties are responsible for overseeing or performing them.

This can be complicated particularly in premises where building management has been contracted by an owner or landlord to one or more third parties who can, in turn, subcontract further. Complications can also arise if the building has been equipped by several different parties such as the owner or landlord, managing agents, tenants or other occupiers.

C.4 People

C.4.1 System and information users

C.4.1.1 General

There are a number of factors in connection with:

— identity management, authentication information and role-based access control;

— development of policies and procedures;

— communication and enforcement of policies and procedures;

— awareness, education and training;

— risk assessment and management.

Some the factors are outlined in following subsections.

C.4.1.2 Health workforce

There are many roles in the health workforce. These include:

— doctors, dentists, pharmacists, nurses, midwives, physiotherapists, paramedics;

— healthcare assistants, technicians, medical secretaries, clinical coders;

— administrative, finance, clerical and support staff;

— volunteers, clergy, charity workers.

Members of the work force in a health organization can be one or more of:

— managers or supervisors;

— full-time or part-time;

— in more than one role (for example as a doctor and, separately, as an academic researcher or educator);

— employed or working in other health organisations (regularly or on an ad hoc basis).

Examples of the basis on which individuals can be on the workforce include:

— permanent contract;

— short-term or temporary contract;

— secondment or placement;

— locum;

— agency staff (provided by an outside organization);

— bank staff (from a pool within the organization);

— visiting (sometimes for providing a “second opinion”) specialist or advisor.

Before achieving full professional status, individuals can be on the workforce as students, trainees or interns.

Some individuals are only at work outside standard office hours. To cover for unexpected absences, some individuals can end up working in a different ward or department for just a few shifts or even only one.

While many health care staff work only at fixed locations such as hospitals, a substantial number of clinicians work in the community and provide care to people in their own homes or other accommodation, such as nursing homes and care homes, where they reside.

All these workforce factors have multiple implications, including ensuring that:

— personal health information of individuals is only available to those members of the workforce who have a legitimate need to access it;

— access rights to systems are correctly managed.

Some compromises can be necessary in order to avoid unmanageably complex approaches.

ISO 21298 considers some of these factors further and also provides lists of regulated professional roles in health.

C.4.1.3 Subjects of care and their proxies

Subjects of care (and their proxies) can be given access to their personal health information. In some cases, users have direct access to health information systems but, in other instances, their personal health information is accessed through an app.

Issues include:

— ensuring that information retrieved or downloaded remains secure on the device used;

— implications of providing users with the ability to update their personal health information not only by direct entry of information but also by upload from:

  — health, well-being or fitness devices (that can belong to the health organization or the user) or apps;

  — records from other health organizations where the subject of care has been treated;

— subjects of care who: are children, have accessibility issues or have learning difficulties;

— any restrictions on the information in their own records that subjects of care are allowed to see;

— restrictions that subjects of care wish to place on what any proxies they have can access and how these restrictions are managed;

— how the authorization of proxies as users is managed and the extent to which, or not, this can be controlled by the subjects of care.

C.4.1.4 Other users

Examples of other users who can need or be entitled to access personal health or other confidential information, as well as systems holding such information, include personnel from regulatory and inspection bodies, insurers, financial and other auditors, health professionals and others investigating clinical or other incidents. To investigate crime, police and other law enforcement organizations can also be given access to personal health information.

Even if these other types of users claim otherwise, it is not always appropriate for them to be granted unrestricted access to information about particular subjects of care or other individuals (such as members of the workforce).

C.4.2 Information security advisory group

C.4.2.1 Aims

Because information security has such widespread implications for a health organization, it can be beneficial for it to have an information security advisory group (such a group can also be called, for instance, a board, committee or forum).

Aims of the group can include:

— ensuring that there is clear direction and visible management support for ensuring information security;

— keeping users up-to-date about information security issues which they need to be aware of (such as new phishing techniques or malware threats);

— learning lessons from information security incidents and near misses both within the organization and elsewhere;

— coordinating awareness raising, education and training for the workforce – not only for new joiners but also as a refresher for others;

— consulting on proposed changes as these can affect clinical practice, business processes or both; for example, shortening session inactivity timeouts or resetting large numbers of passwords can have unintended consequences such as preventing or delaying access to systems in clinical emergencies, or causing interfaces to fail.

C.4.2.2 Membership

It is preferable to always have representation on the group from top level management and the organization's information security experts. Stakeholders who can be represented depend on the type and size of health of organization. They can include:

— clinicians and other members of the workforce closely involved in the direct care of patients;

— academic, teaching and research staff;

— other non-clinical staff who use different systems, typically from departments such as: finance, human resources, procurement/supplies, press and communications.

Clinical and business processes, as well as systems used, can vary substantially between clinical specialties. Accordingly, to give a more balanced view in large organizations, it helps to have attendees from several clinical specialties on the group. It can also be helpful to have some junior staff, trainees or students involved in the group. This is because their experiences, as well as their exposure to different information and systems, can vary considerably from those of senior staff or management.

C.4.3 Technical roles and coordination

As previously noted, medical device, hospital engineering and ICT professionals can have responsibility for various aspects of information security and therefore need to coordinate their activities.

However, there can be individuals in other groups or professions who have technical information security responsibilities such as installing patches and updating software. These individuals are typically system managers or system administrators of specialist clinical or departmental systems. As such their day-to-day duties can include authorizing users of the systems, running backups and so on. Examples are the following:

— Pathology laboratory analysers and related equipment can be supplied with a laboratory information system. Such systems typically export results through interfaces and it is only laboratory staff who access the systems directly. The system manager is usually a member of the relevant department and could be a pathologist or a laboratory manager.

— An individual in a department that ensures physical security in a hospital can be responsible for systems such as those for identity cards and security passes, door entry systems, intrusion alarms and surveillance.

It is therefore important for there to be coordination between departmental system managers, or others who can perform technical information security tasks, and the organization's overall information security professionals.

Another area affecting ICT and hospital engineering departments, in which there can be overlapping responsibilities or, conversely, (usually inadvertent) gaps in coverage, is the building infrastructure that supports ICT. This infrastructure includes network cabling, patch panels, network outlets, communications and computer rooms, and uninterruptible power supplies.

C.5 Asset types and uses

C.5.1 General

The following sub-sections provide examples of various types of asset that use digital technology. Because of the very wide range of such assets, the examples cannot be comprehensive. The purpose of the examples is to provide outline checklists and to highlight that a rigorous approach avoids omission of any assets from inventories.

C.5.2 ICT and IoT

C.5.2.1 Generic equipment and services

As in many other sectors, much generic ICT and, increasingly, IoT (Internet of Things) technology is used in health.

One area of note is patient entertainment systems which provide TV and streaming services to the bedside. These systems can routinely place very large loads, which exceed all other traffic combined, on hospital networks. In addition, demands on these systems can peak dramatically if large numbers of users all want to access the same broadcast at the same time; this can happen when there are high-profile news or sporting events.

C.5.3 Medical devices

Medical devices can be classified or categorized in many different ways. The grouping and order of the medical devices incorporating health software in the list that follows are of no particular significance:

— implantable devices such as pacemakers and defibrillators;

— imaging equipment: digital radiography (DR) and other X-ray based devices, CT (computed tomography) scanners, MRI (magnetic resonance imaging) scanners, ultrasound scanners, endoscopy equipment;

— anaesthetic machines;

— haemodialysis machines;

— radiotherapy equipment;

— surgical robots;

— ventilators;

— external defibrillators;

— clinical/pathology laboratory analysers;

— infusion pumps, syringe drivers;

— point of care testing devices;

— monitoring and diagnostic devices including those for: temperature, heart rate, respiratory rate, blood pressure, oxygen saturation, blood glucose level, electrocardiography, electroencephalography.

Many of the devices listed are normally only found in premises or locations (such as hospitals, clinics, diagnostic centres, hospices and nursing homes) that are specifically for health care. However, some medical devices incorporating health software can also be found in mobile trailer units (this applies particularly to certain types imaging equipment) and ships. Ambulances and other means of transport (such as helicopters) used by emergency services also use certain medical devices incorporating health software.

C.5.4 Building and facilities management

C.5.4.1 Generic equipment and services

Premises in which health services are delivered typically have systems, plant and machinery which are deployed in many types of buildings and are generic. These generic items provide, for example:

— HVAC (heating, ventilation, and air conditioning) and environmental controls;

— fire detection and suppression;

— lighting control, including for example occupancy sensing;

— energy management;

— electronic signage and public address facilities.

C.5.4.2 Physical security systems

There can be generic security systems in health premises such as:

— access control and door entry systems;

— surveillance systems including security cameras;

— intrusion detection and alarm systems;

— personal alarms and body-worn cameras for members of the workforce.

C.5.4.3 Health-specific equipment

Health-specific items of equipment (some of which are classed as medical devices) and related systems specific to health buildings include:

— medical gases and vacuum including monitors and alarms;

— refrigeration and temperature-controlled storage (of blood products, drugs, pathology samples, and so on);

— permanently installed sterilizers (also known as autoclaves);

— nurse call and similar alerting systems as well as other bedhead services.

C.5.5 Uses of personal health information

C.5.5.1 General

Reviewing all the ways in which personal health information is being used or processed in a health organization can assist in both identifying assets that use digital technology and confirming completeness of inventories.

C.5.5.2 Classification of purposes for processing personal health information

ISO/TS 14265 provides a detailed classification of purposes for processing personal health information. The main entries at the topmost level of the classification are as follows:

a) person centred care – processing that directly or indirectly contributes to the health and care of an individual;

b) health service management and quality assurance – processing that utilizes the personal data of an individual in order to monitor and improve the quality, safety and equity of health and care provision to a broad range of individuals;

c) population and public health – processing personal health data to track public health concerns, manage public health risks to individuals and populations, and develop effective strategies;

d) clinical research – the design and conduct of clinical trials, real world data studies and other forms of knowledge generation that involve the processing of personal health data;

e) education and training – processing personal health data to develop education and training materials, to deliver teaching or to evaluate learning;

f) compliance with legal obligations – disclosing or processing personal data in compliance with laws or judicial instructions.

C.5.5.3 Record life cycle events

In addition to considering overall purposes for processing personal health information, possible actions on records can be reviewed in order to identify assets that use digital technology and confirm completeness of inventories.

ISO/TR 21089 specifies the following set of record life cycle events: access/view, add legal hold, amend (update), archive, attest, decrypt, de-identify (anonymize), deprecate, destroy/delete, disclose, encrypt, extract, link, merge, originate/retain, pseudonymize, re-activate, receive/retain, re-identify, remove legal hold, report (output), restore, transform/translate, transmit, unlink, unmerge, verify.

These events are also those that ISO 27789 specifies for inclusion in audit logs.

C.5.6 Health and other applications

C.5.6.1 Health organizations

Hospitals and other premises where health services are provided can have a range of health IT systems (the names of which can vary) principally for direct care purposes including:

— electronic patient record (EPR) systems;

— patient administration systems (PAS);

— picture archiving and communication systems (PACS);

— laboratory information management systems;

— radiology information system (RIS);

— pharmacy/dispensing systems;

— clinical systems for particular specialties (of which there can be plenty in large organisations) such as maternity, cardiology or ophthalmology;

— departmental systems, for example theatres, sterile supplies or infection control;

— interface engines.

These systems can provide a variety of functions including: holding health records, clinical decision support, and scheduling and booking of appointments, consultations and operations.

As can be inferred from the classification of purposes in ISO/TS 14265, there can be many other systems processing personal health information. There can also be document and content management systems, websites, intranets and so on as well as systems for administrative, financial, workforce rostering, education and training (including learning management systems and virtual learning environments), retail (such as for staff and visitor refreshments) and other purposes.

The key point is that, depending on the organization, there can be an unexpectedly large number of systems and databases, many of which contain personal health or other confidential information. In large teaching hospitals, in particular, the evidence is that there can be hundreds.

For the future, significant increases in the use of systems that use artificial intelligence (AI), genomic information, or both are inevitable.

C.5.6.2 Asset and personnel tracking

Asset tracking and motoring systems using RFID (radio-frequency identification) tags, bar codes or other technologies can be used for many purposes including locating medical devices, when dispensing drugs, and managing stocks of consumables, blood products or surgical instruments. The use of bar codes for pathology samples is very common.

Certain health organizations track the locations of some of their workforce. This can be for various reasons including, for example, business process analysis and improvement. Clinicians who work in the community can be tracked for their physical safety.

Hospital inpatients usually have identity bands. These can have barcodes. Some health organizations use tracking technology for certain subjects of care. Examples include:

— individuals who can become lost or disoriented because they suffer from dementia or other conditions;

— new-born babies (if they are moved from designated areas, alarms are sounded to prevent abductions).

C.5.6.3 Apps

Health, well-being and fitness apps are increasingly common. Some are developed specifically for use with other products such as portable medical devices, fitness monitors, wearables and so on.

Some health organizations develop or license apps for subjects of care or their workforce. However, many health-related apps are sourced (usually from "app stores") in the same way as apps of any other type.

Some health-related apps can be beneficial. However, many health-related apps are associated with safety, privacy or security risks, frequently in combination.

C.5.7 Interfaces

Information on subjects of care is often captured or stored in interconnected health IT systems (that can consist of medical devices incorporating health software, middleware, multiple databases, and so on). Much of this information has to be shared or exchanged for care or other purposes; interfaces are commonly used to transfer the relevant data.

Interfaces both within and between organizations can present many different types of security and privacy risks. As such it is essential that they are all included in asset inventories.

Some interfaces use proprietary protocols and data formats. However, the heterogeneous nature of health IT systems and medical devices incorporating health software is such that interfaces, particularly between different manufacturers' products, often exploit standards for exchanging health information.

The most commonly specified and used standards for exchanging health information are as follows:

— HL7 Version 2.5 as specified in ISO/HL7 27931;

— HL7 FHIR (Fast Healthcare Interoperability Resources);

— DICOM (Digital Imaging and Communication in Medicine) as specified in ISO 12052;

— ISO/IEEE 11073 series.

Profiles of DICOM and HL7 standards developed by IHE (Integrating the Healthcare Enterprise) are also common.

Annex D
(informative)

Example security and privacy requirements for health information systems and their mapping to the ISO 27799 controls and IEC/TS 81001-2-2 security capabilities

D.1 Purpose

This annex provides example security and privacy requirements that can:

— inform the procurement, enhancement and evaluation of health software products and information systems from a security and privacy perspective;

— assist organizations implementing this document's controls and guidance in shaping information privacy and security policies, regulations, guidelines, protocols and procedures;

— foster implementation of security controls in the health IT system life cycle.

The example security and privacy requirements are derived from ISO/TS 14441:2013 which has been superseded by this document and withdrawn. The numbering of the example requirements in this document is the same as in ISO/TS 14441:2013 but the requirements themselves have been revised and updated.

The organization using this annex as the basis for its own evaluation can modify the suggested requirements as needed for the specific circumstances of the organization's process. In addition, this annex presents the relationships between these example security and privacy requirements for health information systems and the controls of this document. A mapping to the security capabilities identified in IEC/TS 81001-2-2:2025 is also included.

IEC/TS 81001-2-2:2025 presents an informative set of common, high-level security-related capabilities to be used across the entire life cycle of health software and health IT systems for information exchange between the medical device manufacturers, health software manufacturers, health delivery organizations and/or other stakeholders. These security capabilities are referenced in Table D.1.

Table D.1 — Security capabilities described in IEC/TS 81001-2-2:2025, Clause 5

Subclause	Capability	Acronym
5.2	Automatic logoff	ALOF
5.3	Audit controls	AUDT
5.4	Authorization	AUTH
5.5	Cybersecurity product upgrades	CSUP
5.6	Health data de-identification	DIDT
5.7	Data backup and disaster recovery	DTBK
5.8	Emergency access	EMRG
5.9	Health data integrity and authenticity	IGAU
5.10	Malware detection / protection	MLDP
5.11	Node authentication	NAUT
5.12	Person authentication	PAUT
5.13	Physical locks on product	PLOK
5.14	Third-party components in product life cycle roadmaps	RDMP
5.15	System and application hardening	SAHD
5.16	Health data storage confidentiality	STCF
5.17	Transmission confidentiality	TXCF
5.18	Transmission integrity	TXIG

D.2 Audience

Organizations and individuals that would particularly benefit from the information in this annex include those that are:

— involved in supply, procurement, configuration, integration and implementation of health software and health IT systems;

— responsible for planning, adoption and testing of health IT systems, from privacy and security perspectives.

D.3 Mapping tables

The relationships between the example security and privacy requirements and this document's controls are many-to-many. To simplify the use of the mapping, the relationships have been represented in two tables, each of which represents a set of one-to-many relationships:

— Table D.2: Relationships between the example security and privacy requirements and the controls in this document as well as an additional mapping to the security capabilities in IEC/TS 81001-2-2:2025. Manufacturers should also see IEC/TS 81001-2-2:2025, Annex A for an example of how a medical device manufacturer can benefit from this mapping. That informative annex consists of a sample scenario showing the exchange of security information and is two parts: an introduction and an example Manufacturer Disclosure Statement for Medical Device Security (MDS2).

— Table D.3: Relationships between the controls in this document and the example security and privacy requirements.

Table D.2 — Relationships between the example security and privacy requirements, the security capabilities in IEC/TS 81001-2-2:2025, Clause 5, and this document's controls

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Data subject's consent to collect, use or disclose personal health information		
R1 Recording consent: where data subjects have a right, by law or custom, to withhold or revoke their consent to collect, use or disclosure of their personal health information, health information systems: a) shall provide a facility to record a data subject's consent directives, including the withholding or revocation of consent; b) shall be able to accomplish this in a way that allows each organization to comply with its own legal or policy requirements on consent; **R2 Minimum data recorded:** where health information systems record a data subject's consent directives, the characteristics of the directive shall be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the type of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus expressed consent) and the date on which the directive was given. **R3 Directives follow the data:** where data subjects have a right, by law or custom, to withhold or revoke their consent to the collection, use or disclosure of their personal health information, health information systems should provide a facility to transmit restrictions on further (i.e. onward) disclosure along with the data disclosed if the recipients of the disclosure could not otherwise be aware of and honour the data subject's consent directives. The health information system should be able to accomplish this in a way that allows the sending and receiving jurisdictions to comply with their own legal requirements or policies on consent. **R4 Emergency access:** emergency medical care (such as that given to an unconscious subject of care) or other special situations permitted by law or policy (such as public health investigations during communicable disease outbreaks) may necessitate access to patient records stored in a health information system with partial compliance allowed by law or policy with previously recorded consent directives. Such emergency access capability shall only be provided to authorized users and its invocation (along with a reason the user is overriding the consent directive) shall be recorded in an audit log. Except where partial overriding of consent directives is allowed by law or policy, and to eliminate uncertainty as to whether a user intended to override subject of care consent directives, the system should either allow the user to expressly invoke emergency access or else the system should inform the accessing user, prior to granting access, that the access will constitute emergency access. **R5 Logging emergency access:** health information systems shall be able to: a) log when the processing of consent directives prohibits the disclosure of data; b) log the identity of any user who overrides a data subject's consent directives, the reason for the emergency access, a unique identifier that can be later used to identify the data subject, the date and time when the emergency access occurred; c) provide notification of emergency access to individuals accountable for facilitating privacy compliance. **R6 Consent given by a legally authorized representative**: where a consent directive is given on behalf of a subject of care by a legally authorized representative, the health information systems should be able to record the identity of this representative and the representative's relationship to the subject of care. **R7 Reporting changes to consent**: for any given subject of care, health information systems recording consent directives shall be able to indicate which consent directives, if any, were in force at any given point in time and when any changes were made.	AUDT AUTH DIDT EMRG IGAU NAUT PAUT STCF TXCF TXIG	5.1 Policies for information security 5.2 Information security roles and responsibilities 5.15 Access control 5.20 Addressing information security within supplier agreements 5.33 Protection of records 5.34 Privacy and protection of PII 8.15 Logging 8.16 Monitoring activities

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Limiting use and disclosure		
R8 Recording and storing only that data which have an identified purpose for its collection, use or disclosure: personal health information should only be used or disclosed for purposes consistent with those for which it was collected. **R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject**: it should be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the nature of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus express consent) and the date on which the directive was given. **R10 Restricting data exports**: data transmission in electronic or printed format between health information systems should only be permitted for identified purposes such as clinical care, data backup, or transmission to the data subject (or the data subject's agent) at the subject's request.	AUDT AUTH DIDT EMRG NAUT PAUT STCF TXCF TXIG	5.1 Policy for information security 5.12 Classification of information 5.13 Labelling of information 5.15 Access control 5.20 Addressing information security within supplier agreements 5.33 Protection of records 5.39 Uniquely identifying subjects of care
Data subject access to personal health information and correction of information		
R11 Data subject access: when a data subject challenges the completeness or accuracy of information in the subject's record, and the organization disagrees with the subject's assessment of incompleteness or inaccuracy, the health information system should be capable of recording the disagreement or the reason for the refusal to update the record, or both. **R12 Accessibility**: health information systems should be capable of output or display of personal health information in formats that can be read by the subjects of care, including persons with disabilities, impairments or sensory loss.	IGAU STCF	5.12 Classification of information 5.13 Labelling of information
Data accuracy		
R13 Accuracy: health information systems shall include measures to ensure that personal health information is accurate and complete as is necessary for the purposes for which it is to be used. Examples include implementing data input validation controls and using integrity checks such as checksums and hash totals. **R14 Subject of care identification**: health information systems shall accurately identify a subject of care in the system by means of unique identifiers, searchable by users, when accessing or modifying the subject's records.	AUDT IGAU STCF TXCF TXIG	5.39 HLT - Uniquely identifying subjects of care 5.40 HLT - Output data validation
User identification and authentication		
R15 User identification: users of health information systems shall be assigned an identifier (user ID) that, perhaps in combination with other identifiers (e.g. facility identifiers, jurisdictional identifiers) if necessary, uniquely identifies each individual user and that is used in user authentication and audit logging. Where transactions extend across organizational or jurisdictional boundaries, user IDs, in combination with other user registration information (e.g. user names, addresses, facility identifiers, jurisdictional identifiers) shall: a) uniquely identify each user; b) allow access control decisions; c) allow the compilation of audit records that can unambiguously associate user identities with their audited user actions.	ALOF AUDT AUTH EMRG NAUT PAUT	5.16 Identity management 5.17 Authentication information 5.18 Access rights 5.38 Information security requirements analysis and specification

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
R16 User IDs: health information systems shall support case-insensitive user identifiers that contain characters drawn from the ISO/IEC 8859 series (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode). **R17 Secure authentication**: health information systems shall authenticate the identity of every entity (e.g. users, applications, system services) seeking access to personal health information before granting them access to data and systems resources. **R18 User authentication**: health information systems shall authenticate every user before access to personal health information or related health information system services are granted to the user. For greater clarity, this includes access granted when not connected to a network (e.g. when the health information system is available for access offline). **R19 Authentication methods**: health information systems should support multi-factor user authentication. **R20 System authentication**: health information systems shall authenticate every system entity seeking access to personal health information. Health information systems shall ensure the authenticity of remote nodes (mutual node authentication) when communicating personal health information over the Internet or other known open networks by using a secure standards-based protocol. **R21 Protecting user profiles, passwords, and other authentication tokens**: all data or parameters used in the health information system user authentication process shall be stored or transported in a secure manner and protected from unauthorized access (including viewing, modification, or deletion). Where user passwords are employed, either implement secure password salting and hashing methods or encrypt the passwords using cryptographically secure algorithms. **R22 Passwords**: **use, quality, reset, and user changes**: when passwords are used, the health information system shall implement the following: a) password strength: check password strength at the time the user sets it by ensuring, for example, that passwords are composed of a combination of a sufficient number of uppercase and lowercase letters, numbers, special characters, they do not include any users' personal information e.g. a phone number, and do not contain any consecutive letters or numbers; b) frequency of password changes: implement a function that requires users to change their password according to an adjustable maximum time period; c) password history policy: implement an administrative function that prevents users from reusing the same password a certain number of iterations e.g. the last 10 passwords; d) password reset: after a password reset, users shall be required to set a new password at their next successful logon; e) case sensitivity: support case-sensitive passwords that contain characters drawn from the ISO/IEC 8859 series (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode). **R23 Failed login attempts**: health information systems shall enforce a limit of consecutive invalid access attempts by a user to protect against further (possibly malicious) user authentication attempts. Examples of appropriate mechanisms include locking the account/node until released by an administrator, locking the account/node for a configurable time period, or delaying the next login prompt according to a configurable delay algorithm. **R24 User feedback during authentication**: health information system shall provide only limited feedback information to the user during authentication that does not assist the user in discovering user IDs and passwords.		6.7 Remote working 8.1 User endpoint devices 8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code 8.5 Secure authentication 8.11 Data masking 8.12 Data leakage prevention 8.15 Logging 8.16 Monitoring activities 8.24 Use of cryptography

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Access control		
R25 Access controls: health information systems shall verify that every authenticated person or entity seeking access to personal health information is authorized to access such information. **R26 Authorization control**: prior to carrying out a system of data function related to personal health information, health information systems shall verify that the requesting user or entity has the required access privileges. **R27 Role-based access control**: health information systems shall support role-based access control (RBAC) capable of mapping each user to one or more roles, and each role to one or more system functions or access privileges. **R28 Other forms of access control**: health information systems should additionally be capable mapping each user to access rights assigned or restricted based on a) working groups to which the user belongs, or b) the context of the transaction (for example, time-of-day, workstation-location, or emergency access). **R29 Delegation of access to the personal health information of subjects of care**: health information systems should be capable of maintaining an association between selected users and the records of subjects of care and permit access based on this association. Health information systems should be capable of granting delegated access to records based upon a user with authorized access to a subject of care's records granting access rights for those records to another user. Where implemented, such granting of access shall not a) allow a user, by system means, to grant another user access to a record if the granting user does not possess such access with respect to the record, or b) exceed the role-based access privileges of the user being granted the access. **R30 Reporting access privileges**: health information systems shall be able to report, for a given user, whether the user can access the records of a given subject of care and the privileges (viewing, modification, etc.) the user has in respect of the subject's records. **R31 Restrictions on access privileges**: where a user has been assigned more than one user role, the health information system shall allow the user to select which of the roles allocated to the user is to be applied to that user's session. **R32 Revoking access privileges**: health information systems shall support revocation of all a user's access privileges without requiring the deletion of the user account from the system. Health information systems shall prevent users whose access privileges have all been revoked from logging into the system, e.g. through changing the user account to inactive.	AUDT AUTH EMRG NAUT PAUT PLOK STCF	5.2 Information security roles and responsibilities 5.15 Access control 5.18 Access rights 5.22 Monitoring, review and change management of supplier services 5.33 Protection of records 5.34 Privacy and protection of PII 6.7 Remote working 7.14 Secure disposal or re-use of equipment 8.3 Information access restriction
Acceptable use		
R33 Notifications to users: in each user's session, either prior or immediately following user login or other periodic intervals, the health information system should display a configurable warning or login banner to remind the user of the confidentiality and appropriate use of the personal health information accessible from the system and/or applicable penalties for misuse of the system.	AUTH EMRG PAUT	5.10 Acceptable use of information and other associated assets

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Security and timeout		
R34 Workstation timeout: while a particular user's session is active at an unattended workstation, the health information system shall prevent unauthorized access by automatic timeout after a configurable period of inactivity. Examples of such protection include implementation of a screen saver or a screen timeout requiring a legitimate user to re-authenticate. **R35 Application session timeout**: health information systems shall prevent idle application sessions from being accessed by unauthorized persons by means of an automatic application timeout after a configurable period of user inactivity. Examples of such protection include implementation of application locking, requiring a legitimate user to re-authenticate. Application timeout should be preceded by a warning (at a configurable interval of time) that timeout is about to take place. When an application session has timed out, the same user should be able to return to the session by re-authenticating, or another user should be able to end the previous session (without reactivating it) in order to be able to proceed with a new session. **R36 Connection timeout**: health information systems should have facilities to restrict connection durations where required to a configurable period of time and to force a reconnect when the periods have been exceeded. **R37 Session security**: health information system shall have communication session security controls to prevent the user's session from being hijacked or stolen.	ALOF AUDT AUTH EMRG MLDP NAUT PAUT PLOK SAHD TXCF TXIG	8.1 User endpoint devices 8.5 Secure authentication 8.27 Secure system architecture and engineering principles
Maintaining data availability		
R38 Backup: health information system shall support the generation of backup copies of the application data, security credentials, audit log files, as well as other data and files needed for the proper functioning of the health information system. **R39 Concurrent backup**: if the health information system is available continuously, then the system shall have ability to run a backup concurrently with the operation of the application. **R40 Restoration**: health information system data restoration shall enable a user to return the system to a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and audit files, and shall also enable validation of the integrity of the data restored. **R41 Reconstructing the content of an electronic health record at a prior point in time**: health information systems shall be capable of displaying the content any data subject's records as they existed at any previous date or time.	AUDT DTBK IGAU	5.1 Policies for information security 5.30 ICT readiness for business continuity 8.13 Information backup 8.14 Redundancy of information processing facilities 8.15 Logging 8.16 Monitoring activities
Protecting data during transmission		
R42 Encrypting data during transmission: in a health information system consisting of components distributed across multiple computers or systems, the communication between those components should, (and over the Internet or other open network, shall) offer the following security components: a) partner authentication (e.g. client and server); b) data integrity; c) data confidentiality. **R43 Confirmation of data delivery**: In order to ensure that transmitted data are received, clinical systems shall implement security controls to confirm delivery or receipt of data when data communications take place outside the physical security perimeter that protects information processing facilities.	AUDT AUTH IGAU NAUT PAUT TXCF TXIG	5.14 Information transfer 5.19 Information security in supplier relationships 8.12 Data leakage prevention 8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.24 Use of cryptography

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Protecting data in storage		
R44 Protecting operational data: health information systems shall ensure that personal information, audit logs, and security-related data, such as user profiles, are all protected from unauthorized access and modification when stored permanently (e.g. within databases or file systems) or temporarily (e.g. cached memory). **R45 Protecting data on portable or removable devices**: when storing personal health information on any media or device intended to be portable or removable (for example, flash drives, optical media, or notebook computer), health information systems shall use an industry standard encryption format. **R46 Protecting data in data repositories**: health information systems storing confidential and sensitive data including personal health information and security critical system data (e.g. user profile data and audit logs) shall protect these data from unauthorized access.	AUDT AUTH EMRG MLDP NAUT PAUT PLOK SAHD STCF TXCF TXIG	7.10 Storage media 7.14 Secure disposal or re-use of equipment 8.1 User endpoint devices 8.11 Data masking 8.12 Data leakage prevention 8.15 Logging 8.16 Monitoring activities 8.33 Test information 8.34 Protection of information systems during audit testing
Data integrity		
R47 Integrity of data inputs: data imported from anywhere (e.g. a health information system, a medical device or portable device) shall be accurately associated with a subject of care and a physician in charge, location, date and time of import, and user who imported the data. The health information system used to import the data shall display a warning regarding potential risks. **R48 Integrity of data during processing**: controls shall be in place within the health information system to ensure the integrity of data and to prevent user actions or system faults from causing data inconsistencies or integrity failures. **R49 Integrity of data outputs**: health information systems shall ensure it is possible for a reader to check that hardcopy print-outs are complete.	DIDT IGAU TXIG	5.38 HLT – Information security requirements analysis and specification 5.39 HLT – Uniquely identifying subjects of care 5.40 HLT – Output data validation 5.41 HLT – Publicly available health information
Record retention		
R50 Retention: health information systems shall be capable of storing data for configurable retention periods and support retention scheduling methods and procedures to manage different types of data as defined by law or organizational policy. When data are no longer needed, it shall be disposed using secure disposal methods, for example, erasing, cryptographic erasing, media reformatting, or rendering anonymous.	AUDT DIDT DTBK IGAU PLOK STCF	8.10 Information deletion
Data labelling		
R51 Labelling: health information systems shall be capable of informing each user of the confidential nature of personal health information they access. Examples include displaying the confidentiality label in a consistent location and manner upon user logging into the system, or when displaying personal health information.	IGAU STCF	5.12 Classification of information 5.13 Labelling of information

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
System and audit logs		
R52 System logs: health information systems shall support recording of system events and actions, e.g. system startup and shutdown, user activity, system performance, system resource usage, and system errors and warnings. **R53 Information recorded**: for each of these events, control information shall be recorded, e.g. time of event, identity and the role of the user (in those cases where a user can choose among multiple roles before commencing a user session). **R54 Protecting the audit log**: the audit log files shall have appropriate security controls to prevent alteration and unauthorized access. Examples of such controls include access controls, continuous monitoring to detect any unusual activities or breaches, encryption, and periodic or continuous backup of log files. **R55 Audit interface**: access to audit data shall be strictly controlled and itself subject to audit. Access should be by an appropriate information system that can enforce these controls, rather than directly to the audit trail itself. The audit system shall provide the capability and investigative tools to read audit information from the audit records and interrogate the audit log to a) identify all users who have accessed or modified a given data subject's records over a given period of time, or b) identify the actions of a given user (including all access to data subjects' records) over a given period of time. **R56 Audit log retention**: although the duration of retention of audit log files is a matter of organizational policy that may vary from one jurisdiction to another, the audit system shall support retention of audit log entries. **R57 Application audit logs:** health information system shall record events and actions within the system including details regarding: a) subject of care records created or accessed (e.g. displayed on-screen, printed, downloaded) or updated; b) accesses data that is locked or masked by instruction of a subject of care or person (emergency access); c) creation and modification in the consent directives of a subject of care or person; d) data queries of personal health information; e) personal health information import (reception) including data transmission, data exchange; f) personal health information export, including data transmission, data exchange and printing; g) user, role, and group management activities; h) access to audit log. Health information system audit logs should also be capable of capturing the following events: — system start and stop; — user authentication attempts and its result (successful or not); — user logout, session timeout, account lockout; — backup and restore (where initiated by the system itself); — database accesses; — node-authentication failure; — digital signature created/validated; — security administration events, including password changes; — record disposal. Health information systems should allow an authorized administrator to set the inclusion or exclusion of auditable events not included in the list above.	AUDT SAHD	8.15 Logging 8.16 Monitoring activities 8.33 Test information 8.34 Protection of information systems during audit testing

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
R58 Minimum content of information recorded: health information system audit log entries shall include the following information: a) a record of the user identity; b) a record of the identity of the authority – the person authorizing the entry of, or access to, data, if different from the user; c) the role the user is exercising (in those cases where a user can choose among multiple roles before commencing a user session); d) the organization of the accessing user (in those cases where a user accesses information on behalf of more than one organization); e) the nature of the audited event and the identity of the associated data (e.g. subject of care's ID, message ID) of the audited event; f) the function performed by the user; g) a time stamp (data and time of the event); h) in the case of emergency access to blocked or masked records or portions of records, a reason for the emergency access, as chosen by the user making the access; i) in the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker; j) end user device or access point (if available); k) in the case of password change, user whose password was changed; l) a sequence number to protect against malicious attempts to subvert the audit trail by, for example, altering the system date. **R59 Audit interface**: the health information system should support logging to a common audit engine [for example, using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile]. The system shall provide authorized administrators with the capability to read audit information from the audit records in at least one of the following ways: a) the system should provide the capability to generate reports based on date and time ranges, or b) the system should be able to export logs in such a manner as to allow correlation based on date and time (e.g. UTC synchronization). **R60 Protecting the audit logs**: health information systems shall: a) prohibit users from accessing audit log entries, except those authorized users who have been granted explicit read-access; b) prohibit users from modifying audit log entries. The system shall secure access to audit records and shall safeguard access to system audit tools and audit trails to prevent misuse or compromise, including deletion or modifications. **R61 Continuous logging**: health information system audit logging shall be enabled at all times and there shall be no means for users to disable any audit logging. **R62 Preserving the history of personal health information**: The health information system shall not make deletions to records or audit log entries or changes to data subject records that prevent the reconstruction of records of a subject of care at a prior point in time.		

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Software version control and documentation		
R63 health information system version control: all components of the health information system shall be identified and have an associated software version with a single unambiguous reference (unique ID, name, supplier, and version number). **R64 health information system documentation**: health information systems should have available documentation that addresses system requirements and capacities, installation and testing, management and operation, known security issues, user identification and authentication, privilege management and access control, secure communications, audit, software change management, time synchronization, and data backup and restoration. **R65 Changes to documentation**: documentation shall contain a history of all changes. **R66 Documentation and software versions**: all items of documentation shall clearly state at the beginning their version and the version of the software to which they apply. **R67 Software version**: health information systems shall have a functionality that allows users to view the version of its software components. **R68 Topics included in documentation**: health information systems should have available documentation that addresses all of the following: a) system requirements, including services and network protocols that are necessary for proper operation, as well as the dependencies upon other EHR components; b) system product capacities (e.g. number of users, number of subjects of care, number of records, network load) and baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity); c) system installation, start-up, and connection, including communication security setup; d) steps needed to confirm that the system installation has been properly completed and that the system is operational; e) system management and operation; f) security mechanisms and practices, including creation, modification, and deactivation of user accounts; management of roles, reset of passwords, configuration of password constraints and other aspects of privilege management; communication security, and configuration and management of audit logs; g) known issues or conflicts with security services, including antivirus, malware eradication, intrusion detection, and firewalls, and the resolution of the conflict where applicable; h) software change management and hot-fix processes; i) system time (clock) synchronization where applicable; j) system error or performance messages to users and administrators, with required actions; k) data backup procedures, including data integrity checks when a backup copy is being produced or restored. **R69 Documentation and version control**: all health information system manuals shall clearly state, at the beginning of the document, the version (or versions) to which they apply. All updated health information system manuals should provide a summary for the reader of the changes since the last major revision. **R70 Changes to documentation**: documentation shall contain a history of all changes in a user readable form, so that users can check all changes made in the latest version available.	CSUP MLDP RDMP SAHD	8.6 Capacity management 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.17 Clock synchronization 8.18 Use of privileged utility programs 8.19 Installation of software on operational systems 8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance 8.30 Outsourced development 8.31 Separation of development, test and production environments 8.32 Change management

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Time synchronization and time/date formatting		
R71 Time format: health information systems shall adopt a uniform presentation of time for control and audit. **R72 Clock synchronization**: health information systems shall perform time synchronization using an accepted standard, and use this synchronized time in all records including times. **R73 Time format in exported records**: all time data for control and audit found in exported data (other than time stamp requests to, or responses from, a Time Stamping Authority) shall be represented in the ISO 8601 format, indicating the difference between local time and UTC. **R74 Secure time source**: health information systems shall use a consistent and secure time source.	AUDT CSUP SAHD	8.17 Clock synchronization
Privacy and security incident management		
R75 Incident management: health information systems or supporting audit systems shall trigger a configurable notification to the individuals or the security system in the organization accountable or responsible for managing privacy or security incidents each time a potential incidence of system misuse is detected. **R76 Incident notification:** health information systems should provide a facility so that users can notify an accountable person of security incidents or issues.	AUDT	5.5 Contact with authorities 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 5.43 HLT – External incident reporting 6.8 Information security event reporting

Table D.2 *(continued)*

Example security and privacy requirements (see Clause D.1)	Applicable security capabilities from IEC/TS 81001-2-2	This document's controls
Digital certificates and digital signatures		
R77 Providing digital signatures for users: health information systems that provide functions where users are required to apply the electronic equivalent of a handwritten signature should allow such users to apply a digital signature. **R78 Validating digital signatures**: whenever a health information system generates and receives data containing a digital signature, the system should confirm, at generation and upon receipt, that the signature is or was valid at the time it was applied. **R79 Preserving digital signatures**: health information systems that allow users to apply a digital signature or that receive digitally signed data, should store, backup or archive the digital signature whenever the signed data are stored, backed up or archived; and transmit the digital signature whenever the signed data are transmitted. **R80 Digital signing**: all health information systems providing functions where users are required to apply the electronic equivalent of a handwritten signature shall support a suitable digital signature standard compliant with information security policies and regulations. **R81 Validating, preserving and transmitting digital signatures**: the health information system shall: a) confirm upon receipt that the signature is valid (i.e. that the associated signature certificate and all the associated chain certificates has not been revoked); b) store, backup or archive the digital signature and all related data (information about root certificates, certification chains, signatory certificates, and revocation information) whenever the signed data are stored, backed up or archived; c) transmit the digital signature together with the data or by reference whenever the signed data are transmitted; d) allow users to confirm, whenever they access signed data, that the signature is valid at the time of signing (i.e. that the associated signature certificate has not been revoked). **R82 Purpose of the signature and signatory role**: health information systems providing digital signature functionality should include the commitment-type-indication attribute and the role of the signatory (i.e. the user's role attribute).	AUDT PAUT TXCF TXIG	8.24 Use of cryptography

Table D.3 — Relationships between this document's controls and the example security and privacy requirements (see Clause D.1)

This document's control	Example security and privacy requirements (Clause D.1)
Clause 5 Organizational controls	
5.1 Policies for information security	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R50 Record retention R56 Audit log retention R62 Preserving the history of personal health information
5.2 Information security roles and responsibilities 5.3 Segregation of duties 5.4 Management responsibilities 5.5 Contact with authorities 5.6 Contact with special interest groups	R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges R75 Incident management R76 Incident notification
5.7 Threat intelligence	None
5.8 Information security in project management	None
5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets	R33 Notifications to users R62 Preserving the history of personal health information
5.12 Classification of information 5.13 Labelling of information	R14 Subject of care identification R51 Labelling
5.14 Information transfer	R10 Restricting data exports R42 Encrypting data during transmission

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
5.15 Access control	R4 Emergency access R5 Logging emergency access R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges
5.16 Identity management	R15 User identification R16 User IDs
5.17 Authentication information	R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication
5.18 Access rights	R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges
5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services	None

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence	R75 Incident management R76 Incident notification
5.29 Information security during disruption 5.30 ICT readiness for business continuity	R48 Integrity of data during processing R57 Auditable events
5.31 Legal, statutory, regulatory and contractual requirements 5.32 Intellectual property rights	R68 Topics included in documentation
5.33 Protection of records 5.34 Privacy and protection of PII	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access: R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R27 Role-based access control R29 Delegation of access to the personal health information of subjects of care R31 Restrictions on access privileges
5.35 Independent review of information security 5.36 Compliance with policies, rules and standards for information security	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access: R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R50 Record retention R56 Audit log retention R62 Preserving the history of personal health information
5.37 Documented operating procedures	R68 Topics included in documentation
5.38 HLT – Information security requirements analysis and specification	R68 Topics included in documentation
5.39 HLT – Uniquely identifying subjects of care 5.40 HLT – Output data validation	R14 Subject of care identification
5.41 HLT – Publicly available health information	None
5.42 HLT – Emergency communication	None
5.43 HLT – External incident reporting	R75 Incident management R76 Incident notification

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
Clause 6 People controls	
6.1 Screening 6.2 Terms and conditions of employment 6.3 Information security awareness, education and training 6.4 Disciplinary process 6.5 Responsibilities after termination or change of employment 6.6 Confidentiality or non-disclosure agreements	None
6.7 Remote working	R15 User authentication R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication R25 Access control R26 Authorization control R27 Role-based access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges
6.8 Information security event reporting	R75 Incident management R76 Incident notification
6.9 HLT – Management training	None
Clause 7 Physical controls	
7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.7 Clear desk and clear screen 7.8 Equipment siting and protection 7.9 Security of assets off-premises	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
7.10 Storage media	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories
7.11 Supporting utilities 7.12 Cabling security 7.13 Equipment maintenance 7.14 Secure disposal or re-use of equipment	R45 Protecting data on portable media
Clause 8 Technological controls	
8.1 User endpoint devices	R15 User identification R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R25 Access controls R34 Session security R35 User session timeout R36 Connection timeout R37 Session security R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories
8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code	R15 User identification R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges
8.5 Secure authentication	R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication R34 Session security

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
8.6 Capacity management 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management	R68 Topics included in documentation R69 Documentation and version control R70 Changes to documentation
8.10 Information deletion	R50 Retention
8.11 Data masking 8.12 Data leakage prevention	R21 Protecting user profiles, passwords, and other authentication tokens R32 Revoking access privileges R42 Encrypting data during transmission R43 Confirmation of data delivery R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositoriesR54 Protecting the audit log R58 Minimum content of information recorded
8.13 Information backup 8.14 Redundancy of information processing facilities	R38 Backup R39 Concurrent backup R40 Restoration R41 Reconstructing the content of an electronic health record at a prior point in time
8.15 Logging 8.16 Monitoring activities	R5 Logging emergency access R15 User identification R38 Backup R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories R54 Protecting the audit log
8.17 Clock synchronization	R68 Topics included in documentation-clock synchronization-related requirement R71 Time format R72 Clock synchronization R73 Time format in exported records R74 Time source
8.18 Use of privileged utility programs 8.19 Installation of software on operational systems	R64 health information system documentation R68 Topics included in documentation-software installation-related requirements
8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks	R42 Encrypting data during transmission R43 Confirmation of data delivery
8.23 Web filtering	None

Table D.3 *(continued)*

This document's control	Example security and privacy requirements (Clause D.1)
8.24 Use of cryptography	R21 Protecting user profiles, passwords, and other authentication tokens R42 Encrypting data during transmission R43 Confirmation of data delivery R77 Providing digital signatures for users R78 Validating Digital Signatures R79 Preserving digital signatures R80 Digital signing R81 Validating, preserving and transmitting digital signatures R82 Purpose of the signature and signatory role
8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance 8.30 Outsourced development 8.31 Separation of development, test and production environments 8.32 Change management	R63 health information system version control R64 health information system documentation R65 Changes to documentation R66 Documentation and software versions R67 Software version R68 Topics included in documentation R69 Documentation and version control R70 Changes to documentation
8.33 Test information 8.34 Protection of information systems during audit testing	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories R54 Protecting the audit log
8.35 HLT – Zero trust principles	None

Bibliography

[1] ISO 8601 (all parts), *Date and time — Representations for information interchange*

[2] ISO/IEC 8859 (all parts), *Information technology — 8-bit single-byte coded graphic character sets*

[3] ISO/IEC 10646, *Information technology — Universal coded character set (UCS)*

[4] ISO/IEEE 11073 (all parts), *Health informatics — Device interoperability*

[5] ISO 12052, *Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management*

[6] ISO 13131, *Health informatics — Telehealth services — Quality planning guidelines*

[7] ISO 13940:2015, *Health informatics — System of concepts to support continuity of care*

[8] ISO/TS 14265, *Health informatics — Classification of purposes for processing personal health information*

[9] ISO/TS 14441:2013, *Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment*

[10] ISO 17090-3, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

[11] ISO/TS 17975:2022, *Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information*

[12] ISO/TS 21089, *Health informatics — Trusted end-to-end information flows*

[13] ISO 21298, *Health informatics — Functional and structural roles*

[14] ISO/TR 21332, *Health informatics — Cloud computing considerations for the security and privacy of health information systems*

[15] ISO 22600 (all parts), *Health informatics — Privilege management and access control*

[16] ISO 22857, *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data*

[17] ISO/TS 23535, *Health informatics — Requirements for customer-oriented health cloud service agreements*

[18] ISO 25237, *Health informatics — Pseudonymization*

[19] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[20] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[21] ISO/IEC 27701, *Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance*

[22] ISO 27789:2021, *Health informatics — Audit trails for electronic health records*

[23] ISO/HL7 27931, *Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments*

[24] IEC/TS 81001-2-2:2025, *Health software and health IT systems safety, effectiveness and security — Part 2-2: Guidance for the implementation, disclosure and communication of security needs, risks and controls*

[25] FHIR. *Fast Healthcare Interoperability Resources*. Available at https://hl7.org/fhir/

[26] IHE. *Integrating the Healthcare Enterprise*. Available at https://www.ihe.net

[27] World Health Organization (WHO). *WHO/HSS/EHT/DIM/11.03, Core Medical Equipment*. Available at https://iris.who.int/handle/10665/95788