健康信息安全管理体系

认证技术规范

文件编号：CTS TBGL139-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

前言

本文件旨在为组织（以下简称“组织”）建立、实施、维护和持续改进健康信息安全管理体系（HISMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与 **ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》** 的高阶结构保持一致，并充分融合了 **ISO 27799:2016《健康信息学 — 基于ISO/IEC 27002的健康领域信息安全管理体系》** 的特定行业控制要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的健康信息安全控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和ISO 27799:2016要求的整合性管理体系。组织应首先建立满足ISO/IEC 27001要求的信息安全管理体系（ISMS），并在此基础上扩展健康信息安全管理要求。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 健康信息安全管理体系 的要求。本文件适用于

1) 组织建立、实施、保持和改进 健康信息安全管理体系 管理方针和目标；
2) 认证机构对组织进行健康信息安全管理体系认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- ISO/IEC 27000 信息技术 — 安全技术 — 信息安全管理体系 — 概述和词汇
- ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- ISO 27799:2016 健康信息学 — 基于ISO/IEC 27002的健康领域信息安全管理体系

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台：https://www.iso.org/obp
- IEC电子百科：https://www.electropedia.org/

3.1 个人健康信息（PHI）

与个人身体或精神健康相关的信息，包括个人健康服务提供的信息，以及可用于识别个人身份的健康相关信息。

[来源：ISO 27799:2016, 3.1]

3.2 健康信息安全管理体系（HISMS）

基于ISO/IEC 27001:2022建立、实施、维护和持续改进的，专门针对健康领域信息安全的管理体系。

3.3 健康信息

与个人健康相关的任何信息，包括但不限于：医疗记录、诊断信息、治疗信息、遗传信息、生物识别信息、健康保险信息等。

3.4 患者

接受健康服务的个人，其PHI受到保护。

3.5 健康服务提供者

提供健康服务的组织或个人，如医院、诊所、医生、护士、实验室等。

3.6 健康信息保管者

负责保管和维护PHI的组织或个人。

3.7 健康信息主体

PHI所关联的个人，通常是患者。

3.8 健康信息访问控制

基于角色、职责和最小权限原则，对PHI的访问进行授权和限制的机制。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现HISMS预期结果能力的外部和内部事项。

- **外部因素**：适用的健康信息安全法律和法规（如《网络安全法》、《数据安全法》、《个人信息保护法》、《健康医疗大数据标准、安全和服务管理办法》等）、监管机构要求（如卫健委、网信办、数据局等）、行业标准与最佳实践、PHI泄露的监管和声誉风险、患者对隐私保护的关注度、分包商所在国家的法律等。
- **内部因素**：组织的规模、治理结构、作为健康服务提供者或健康信息保管者的角色、处理的PHI类型和数量、人员健康信息安全意识与技能水平、以往PHI安全事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与HISMS有关的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过HISMS予以解决。

相关方包括但不限于：患者（健康信息主体）、健康服务提供者、监管机构（卫健委、网信办等）、员工、合作伙伴、供应商（如电子病历系统供应商）、认证机构、公众。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与HISMS相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**。**组织应将促进相关方参与所产生的输出形成文件**。

4.3 确定HISMS的范围

组织应确定HISMS的边界及其适用性，以建立其范围。在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与健康服务提供者、健康信息保管者、患者之间的接口）。

范围应形成文件化信息并可用。

4.4 健康信息安全管理体系（HISMS）

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进健康信息安全管理体系，包括所需过程及其相互作用。

组织应确定健康信息安全管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；
b) 确定这些过程的顺序和相互作用；
c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；
d) 确定这些过程所需的资源并确保其可获得；
e) 分配这些过程的职责和权限；
f) 按照 6.1 的要求应对风险和机遇；
g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
h) 改进过程和健康信息安全管理体系。
4.4.2 在必要的范围和程度上，组织应：
a) 保持成文信息以支持过程运行；
b) 保留成文信息以确信其过程按策划进行。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实其在对HISMS的领导作用和承诺：
a) 确保建立健康信息安全方针和目标，并与组织战略方向一致；
b) 确保将HISMS要求融入组织的业务过程；
c) 确保HISMS所需的资源可获得；
d) 沟通有效的健康信息安全管理的重要性；
e) 确保HISMS达成其预期结果（如PHI安全、合规、患者信任）；
f) 指导并支持相关人员为HISMS的有效性做出贡献；
g) 促进持续改进；
h) 支持其他相关管理角色在其职责范围内发挥领导作用。

5.2 方针

最高管理者应建立健康信息安全方针，该方针应：
a) 与组织的宗旨相适宜；
b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；
c) 包括对满足适用健康信息安全相关要求的承诺；
d) 包括对持续改进HISMS的承诺；
e) **特别应包括对保护PHI的保密性、完整性、可用性和可追溯性，以及遵守健康信息安全法律法规的承诺**。
健康信息安全方针应：
f) 形成文件化信息并可获取；
g) 在组织内得到沟通；
h) 适当时，可被相关方获取（如患者、监管机构）。

5.3 组织的岗位、职责和权限

最高管理者应确保与健康信息安全相关岗位、职责和权限在组织内得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如健康信息安全负责人、数据保护官），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保HISMS符合本文件的要求；

b) 向最高管理者报告HISMS绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对健康信息安全重要性的意识；

d) 协调与HISMS有关的内部和外部沟通（特别是与患者和监管机构）。

同时，最高管理者应明确**指定一个联络点**，供患者和监管机构使用，以处理与PHI处理相关的询问和投诉。

6 策划

6.1 应对风险和机会的措施

6.1.1 总则

当策划HISMS时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a) 确保HISMS可达到预期结果；

b) 预防或减少不良影响（如PHI泄露、合规处罚、患者信任丧失、医疗纠纷）；

c) 达到持续改进。

组织应策划：

d) 应对这些风险和机会的措施；

e) 如何将此措施整合到HISMS过程中并予以实现及评价其有效性。

6.1.2 健康信息安全风险评估

组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；识别与PHI处理相关的健康信息安全风险（如未经授权的访问、数据泄露、数据篡改、系统故障、医疗设备安全风险）；分析并评价风险。风险评估应特别考虑PHI泄露对患者权利和健康的影响。组织应保留有关风险评估过程的文件化信息。

6.1.3 健康信息安全风险处置

组织应定义并应用风险处置过程，以选择适当的处置方案（通过 **ISO/IEC 27001:2022附录A** 及 **ISO 27799:2016** 中的控制措施）。组织应**制定并维护一个《适用性声明》**，包含所选控制措施及删减的合理性说明，并制定正式的风险处置计划。组织应保留有关风险处置过程的文件化信息。

注： 组织应**建立并保持合规义务登记册**，以识别和跟踪与健康信息安全相关的法律法规、标准及其他要求。

6.2 健康信息安全目标及其实现的策划

组织应在相关职能和层级上建立健康信息安全目标。目标应：

a) 与健康信息安全方针一致；

b) 可测量（如PHI泄露事件数、患者投诉率、培训完成率、审计发现项关闭率、系统可用性指标）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新。

策划如何实现这些目标时，组织应确定要做什么、需要什么资源、由谁负责、何时完成、如何评价结果。

6.3 针对变更的规划

当组织确定需要对HISMS进行变更时（如引入新的电子病历系统、外包健康数据处理、法律法规重大变更、新增PHI类型），变更应系统地予以策划和实施。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进HISMS所需的资源。资源包括：具备相应能力的人员（健康信息安全专家、数据保护官等）、技术基础设施（加密工具、访问控制系统、日志审计系统、入侵检测系统、医疗设备安全工具等）、财务资源、技术资源等。

7.2 能力

组织应：确定从事会影响组织健康信息安全绩效的工作人员的必要能力（如健康信息安全法规、PHI保护技术、患者身份管理流程）；基于适当的教育、培训或经验确保其胜任；适用时采取措施获得必要能力（如健康信息安全培训、认证），并评估有效性；保留适当的文件化信息作为能力的证据（如培训记录、认证证书）。

注：**能够访问PHI的个人应承担保密义务**（根据ISO 27799:2016附录A.10.1）。

7.3 意识

在组织控制下工作的人员应了解：

a) 健康信息安全方针；

b) 其对HISMS有效性的贡献；

c) 不符合HISMS要求的潜在影响（尤其是对患者和组织的风险）。

7.4 沟通

组织应确定与HISMS相关的内部和外部沟通的需求，包括：沟通什么（如健康信息安全政策、PHI处理信息、数据泄露通知、患者权利）、何时沟通、与谁沟通、谁来沟通、怎么沟通。特别地，应建立与患者关于其PHI处理的沟通机制，以及向监管机构报告数据泄露的机制。

7.5 文件化信息

7.5.1 总则

组织的HISMS应包括：本文件要求的文件化信息（如HISMS手册、风险评估报告、风险处置计划、适用性声明、健康信息安全政策、患者同意记录、数据主体请求处理记录等）；组织

为HISMS有效性所确定的必要的文件化信息（如PHI处理活动记录、数据保护影响评估报告）。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的标识和说明、形式、载体以及评审和批准。

7.5.3 文件化信息的控制

HISMS及本文件所要求的文件化信息应得到控制，以确保：在需要的场合和时机可获得并适用；予以妥善保护（避免泄密、不当使用或缺失）。为控制文件化信息，适用时，组织应分发、访问、检索和使用；存储和防护；更改控制；保留和处置（PHI相关的文件化信息的保留期限应符合法规要求）。

8 运行

8.1 运行的策划和控制

组织应策划、实施和控制为满足要求和实施第6章所确定的措施所需的过程，包括建立过程准则，并按照准则实施控制。组织应控制计划内和计划外的变更，确保外部提供的过程、产品和服务受控。

8.2 健康信息安全风险评估

组织应考虑6.1.2a) 所建立的准则，按计划的时间间隔或当重大变更发生时（如新PHI处理活动上线、法律法规更新），执行健康信息安全风险评估。应保留风险评估结果的文件化信息。

8.3 健康信息安全风险处置

组织应实现健康信息安全风险处置计划。应保留风险处置结果的文件化信息。

8.4 健康信息安全特定控制措施（依据ISO 27799:2016）

组织应按本章节要求实施和运行特定的健康信息安全控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1 健康信息安全策略（依据ISO 27799:2016第5章）

控制

应制定和维护健康信息安全策略，以管理组织的PHI保护。

实施要求：

a) 制定并维护文件化的《健康信息安全策略》，该策略应由最高管理层批准。

b) 该策略应涵盖：PHI保护的目标和原则；PHI收集和处理的透明度；数据最小化原则；患者权利；数据保留与销毁；数据泄露响应；合规要求。

c) 该策略应定期评审和更新（至少每年一次）。

8.4.2 PHI的识别与分类（依据ISO 27799:2016第6章）

控制

应识别和分类组织处理的所有PHI。

实施要求：

a) 建立并维护**PHI处理活动记录（ROPA）**，记录所有PHI处理活动。ROPA应包含但不限于：

- **处理目的**（如诊断、治疗、研究、保险）
- **PHI类别**（如个人基本信息、医疗记录、遗传信息、生物识别信息）
- **PHI主体类别**（如患者、健康服务提供者）
- **PHI接收方或接收方类别**（如其他医疗机构、保险公司、研究机构）
- **PHI保留期限**
- **所采取的技术和组织安全措施的一般描述**

b) 对PHI进行分类（如一般PHI、敏感PHI），并根据分类实施不同的保护措施。

8.4.3 患者身份管理与访问控制（依据ISO 27799:2016第8章及附录A.10.10）

控制

应实施严格的访问控制措施，防止对PHI的未授权访问。

实施要求：

a) **患者身份管理**：建立并维护唯一的患者标识符，确保患者身份的唯一性和准确性。

b) **用户访问管理**：对所有经授权可访问PHI的用户，维护其**用户配置文件**。严格执行**最小权限原则**，确保用户仅获得执行其职责所必需的访问权限。实施**用户ID的独立使用**，每个有权访问PHI的个人应拥有唯一的用户ID。已停用或过期的用户ID不得重新分配给其他个人。

c) **基于角色的访问控制（RBAC）**：根据用户的角色（如医生、护士、行政人员）分配不同的访问权限。

d) **紧急访问**：建立紧急情况下的PHI访问程序，并记录所有紧急访问活动。

8.4.4 健康信息加密与密钥管理（依据ISO 27799:2016第10章及附录A.11.4, A.11.5）

控制

应使用加密技术保护PHI的保密性。

实施要求：

a) 应实施**静态数据加密**：对存储PHI的数据库、文件系统或存储介质进行加密。

b) 应实施**传输中数据加密**：对通过网络传输的PHI进行加密（如TLS/SSL）。

c) 应**管理加密密钥**：使用企业级密钥管理系统（KMS）；密钥生成、存储、分发、轮换和销毁应遵循安全策略。

8.4.5 健康信息安全事件管理（依据ISO 27799:2016第16章及附录A.10.1）

控制

应建立机制以管理PHI数据泄露事件。

实施要求：

a) 建立《PHI数据泄露响应与通知程序》。

b) 在发生涉及PHI的数据泄露时，应及时通知相关患者（如适用）和监管机构。

c) 通知应包含泄露的性质、涉及的PHI类型、已采取或拟采取的补救措施等。

d) 信息安全事件应触发以确定是否涉及PHI数据泄露的审查。

8.4.6 健康信息备份与恢复（依据ISO 27799:2016第10章及附录A.11.4）

控制

应建立PHI的备份与恢复机制，以防止数据丢失。

实施要求：

a) 应制定并实施**PHI备份策略**：确定备份范围、备份频率、备份类型、保留周期。

b) 备份数据应**异地存储**，且与生产数据物理或逻辑隔离。

c) 备份数据的加密要求应与生产数据一致。

d) 应定期对备份数据进行**恢复测试**，验证其完整性和可用性（至少每季度一次）。

8.4.7 健康信息保留与销毁（依据ISO 27799:2016第12章）

控制

应根据法律、法规和业务要求管理PHI的保留和销毁。

实施要求：

a) 制定PHI保留策略，明确不同类型PHI的保留期限（应符合医疗法规要求）。

b) 当PHI不再需要时，应根据敏感度进行**安全销毁**：

- **逻辑销毁**：对数据进行多次覆写或加密擦除。
- **物理销毁**：对物理存储介质（如硬盘、磁带）进行消磁、粉碎或焚毁。

c) 所有销毁操作应有**审批记录**和**见证记录**。

8.4.8 健康信息第三方管理（依据ISO 27799:2016第15章）

控制

应确保第三方（如电子病历系统供应商、健康数据分析服务商）具有足够能力保护PHI。

实施要求：

a) **合同约束**：与处理PHI的任何第三方签订的合同，应规定满足本组织健康信息安全义务的最低技术和组织措施。

b) **监控与审计**：对第三方的PHI处理活动进行监控和定期审计，确保其满足合同要求。

8.4.9 健康信息隐私影响评估（PIA）（依据ISO 27799:2016第7.2.5条）

控制

应在引入新的PHI处理活动或对现有处理活动进行重大变更时，进行隐私影响评估。

实施要求：

a) 建立《健康信息隐私影响评估程序》。

b) 在启动新的PHI处理项目或对现有处理进行重大变更时，执行PIA。

c) PIA应识别和评估隐私风险，并提出风险处置措施。

d) 保留PIA报告作为文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：需要被监视和测量的内容（包括健康信息安全过程绩效、PHI安全事件、患者投诉率、培训完成率、合规性偏差等）；适用的方法；何时执行；谁应执行；何时分析和评价结果。组织应评价健康信息安全绩效以及HISMS的有效性。**确保用于监视与测量的资源（如审计工具、日志分析系统）的准确性**。

9.1.2 合规性评价

组织应建立、实施并保持程序，以定期评价其对适用法律法规（特别是健康信息安全相关法律）、标准及自身HISMS要求的遵守情况。**合规性评价应至少每年进行一次**，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关HISMS符合性及有效性的信息。审核员应确保客观性和公正性。审核结果应报告给相关管理层。

9.3 管理评审

最高管理者应按计划的时间间隔评审HISMS，以确保其持续的适宜性、充分性和有效性。管理评审应考虑：

a) 以往管理评审措施的状态；

b) 内外部的变化（如新的健康信息安全法规、PHI处理活动变更）；

c) 绩效信息（包括：PHI泄露事件趋势、患者投诉率、**外部供方（如第三方服务商）的绩效**、合规性偏差、风险评估与处置状态、改进机会等）；

d) 持续改进的机会。

评审输出应包括与持续改进机会及HISMS变更需求相关的决定。

10 改进

10.1 持续改进

组织应持续改进HISMS的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：做出应对、控制并纠正，处置后果；评价是否需要采取措施消除原因；实施所需的措施并评审有效性；必要时对HISMS进行更改。应保留文件化信息作为不符合性质及后续采取措施的证据。**推荐预防措施**以防范潜在不符合的发生（例如，通过定期健康信息安全评估，预防新处理活动带来的隐私风险）。

————————————————