医疗器械企业数据安全技术建议
第一部分：数据安全管理能力
（征求意见稿）

前 言

本文件按照 GB/T 1.1—2020 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由人工智能医疗器械创新合作平台提出并归口。

起草单位：人工智能医疗器械创新合作平台智能化医疗器械核心零部件工作组

1. 范围

本文件从医疗器械企业的基础安全、数据全生命周期安全管理，进一步规范医疗器械企业数据安全管理和技术能力，降低数据安全风险，加强重要数据和个人信息安全。

本文件一方面为医疗器械企业建立规范完备的数据安全保护能力，另一方面为医疗器械企业数据安全能力的测试方法提供参考。

2. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 25069—2010 信息安全技术 术语

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

GB/T 36073—2018 数据管理能力成熟度评估模型

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

《医疗器械网络安全注册技术审查指导原则（2022 年修订版）》

《医疗器械网络安全审查指导原则实施指南》（京药监发[2019]257 号）

卫生健康委 中医药局 国家疾控局 《医疗卫生机构网络安全管理办法》

3. 术语、定义和缩略语

3.1. 术语和定义

GB/T 25069—2010 和 GB/T 35273—2020 中界定的以及下列术语和定义适用于本文件。

3.1.1.

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.1.2.

保密性 confidentiality

指数据不能被未授权的个人、实体利用或知悉的特性，即器械相关数据仅可由授权用户在授权时间以授权方式进行访问。

3.1.3.

完整性 integrity

指保护数据准确和完整的特性，即器械相关数据是准确和完整的，且未被篡改。

3.1.4.

可得性 availability

指根据授权个人、实体的要求可访问和使用的特性，即器械相关数据能以预期方式适时进行访问和使用。

3.1.5.

真实性 authenticity

一个实体正是其所声称实体的特性，即器械相关数据能够体现真实的临床状态，包括生理状态、操作状态、设备状态等。

3.1.6.

可核查性 accountability

实体的一种特性,表征对自己的动作和做出的决定负责，即器械相关数据表征对相关临床动作和决定负责。

3.1.7.

抗抵赖 non-repudiation

证明所声称事态或行为的发生及其发起实体的能力,以解决有关事态或行为发生与否以及事态中实体是否牵涉的争端。即器械相关数据可证明相关临床事态和行为的发生及其发起的能力。

3.1.8.

可靠性 reliability

与预期行为和结果一致的特性，即器械相关数据与临床的预期行为和结果一致。

3.1.9.

数据安全人员 Data security personnel

从事数据安全需求分析挖掘、技术方案设计、项目实施、运营管理等工作的管理技术人员。

4. 基础安全技术能力

4.1. 网络安全管理能力

为提升网络安全管理水平，医疗器械企业可参考以下建议，结合自身情况逐步构建和完善管理能力。

4.1.1. 组织与职责

a. 企业可成立网络安全和信息化领导工作小组，定期召开网络安全办公会，统筹安全管理决策。

b. 可按照“管业务就要管安全”“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，明确各部门（如主管部门、运营部门、信息化部门、使用部门）的安全管理职责。

c. 可建立关键和重要系统清单，并明确其所属负责部门及人员。

d. 对于关键信息基础设施，运营者可对管理机构负责人和关键岗位人员的安全能力与背景进行审查。

4.1.2. 制度与规范

a. 可建立覆盖网络和数据安全的管理制度及操作规程，范围可包括医疗设备、供应链、数据上云、人脸识别等新业务场景。

b. 可根据国家等保定级要求，开展信息系统的定级工作。

c. 当国家及行业新法律法规、标准发布后，可及时跟进并完成内部制度的修订与发布工作。

d. 可加强信息系统自研和外包开发过程中的供应链安全管理。

4.1.3. 运行与保障

a. 新建信息化项目可同步规划并开展网络安全建设。

b. 可明确内部人员入职、培训、在岗、离岗的全流程安全管理要求，并对第三方人员明确网络权限的申请、批准、实名登记、背景审查和保密协议签署等流程。

c. 可确保网络安全管理人员具备相应资质，并执行持续教育制度，定期开展网络安全教育培训。

d. 关键和重要信息系统可定期开展文档核验、漏洞扫描、渗透测试等多种形式的安全

自查；核心系统的检查可由专业第三方安全机构进行。系统可定期进行商用密码应用安全性评估。

4.1.4. 监测与改进

a. 可建立网络安全考核评价机制，并据此开展安全建设整改工作。

b. 可建立应急处置机制，完善应急预案，并定期组织核心和重要信息系统的应急演练。

c. 可建立网络安全态势感知平台，加强威胁情报工作，定期开展网络安全威胁分析和态势研判，并及时向主管部门通报相关情况。

d. 可定期开展核心系统的攻防演练。

e. 企业可积极参与网络和数据安全国家或行业标准的编制工作。

4.2. 数据安全需求分析

为系统化开展数据安全需求分析工作，企业可结合自身情况参考以下建议：

4.2.1. 组织与职责

a. 企业可建立专门的数据安全需求分析组织或虚拟团队，负责统筹相关工作。该团队可由信息系统主管部门、网络安全部门、运营部门、信息化部门、使用部门等共同参与。

b. 核心和重要信息系统的主管部门可定期（如每年）组织开展数据安全需求分析。

4.2.2. 流程与方法

a. 可建立明确的数据安全需求分析管理流程与方法，确保分析工作规范、可持续。

b. 可依据数据资产分类分级结果，明确组织的数据安全需求及相应安全控制措施。

4.2.3. 执行与融入

a. 在新业务或新系统规划阶段，可由主管部门牵头，相关各部门全程参与，开展数据安全需求分析，并编制分析报告，以确保数据安全要求融入建设初期。

b. 数据安全需求分析工作可逐步覆盖企业所有重要业务信息系统及重要医疗设备。

4.2.4. 人员与能力

a. 负责数据安全需求分析的人员可充分理解国家法律法规、标准及行业监管要求，并能够结合业务场景与安全形势，形成有效的数据安全需求分析结果。

4.3. 数据安全策略制定

为系统化建立数据安全策略体系，企业可结合自身情况参考以下建议：

4.3.1. 组织与岗位

a. 企业可设立专职岗位或人员，负责组织制定数据安全制度、流程与策略，确保其覆盖全部业务。

b. 可组织相关人员开展数据安全法律法规的宣贯与学习，增强整体安全意识。

4.3.2. 策略制定与规划

a. 在制定数据安全策略时，可结合组织内外部需求，包括国家法律法规和行业监管要求，形成与实际业务规划相适配的策略内容。

b. 可基于总体数据安全策略，建立以数据安全为核心的管理制度与流程，覆盖核心和重要业务、系统及应用。

c. 可制定组织层面的数据安全策略规划，明确各阶段目标、任务和工作重点，保持策略与业务发展的一致性。

d. 当组织结构、业务方向或内外部环境发生变化时，可及时调整数据安全策略，确保其持续符合组织发展目标。

4.3.3. 宣贯与培训

a. 可建立数据安全相关标准、管理办法和工作流程的评审与发布机制，并组织专题宣贯。

b. 可定期组织数据安全法律法规、策略与标准的培训宣贯，加强人员安全防护意识。

4.4. 数据安全人员管理

为有效管理数据安全相关人员，企业可结合自身情况参考以下建议：

4.4.1. 组织与职责

a. 企业可建立负责数据安全工作的职能部门或岗位，明确各方责任与权利。

b. 可设置专职岗位或人员，统筹数据安全培训管理工作，落实上级相关管理要求。

4.4.2. 内部人员管理

a. 可与数据安全管理人员签署保密协议，明确保密义务。

b. 可在组织层面建立覆盖招聘、录用、上岗、在岗、离岗、考核等环节的人员安全管理制度。

c. 可推动数据安全管理人员持证上岗，鼓励取得 CISP-DSG、CISP-DPO 等相关资质。

d. 人员应了解业务发展目标，将数据安全工作与业务目标有机结合，具备数据保护意

识、风险判断能力，熟悉业务数据场景、调用逻辑及法律合规要求。

4.4.3. 第三方人员管理

a. 可明确第三方合作机构的数据安全管理要求，对接触重要或一般数据（如个人信息、医疗健康数据等）的人员进行审批、登记并签署保密协议，定期开展安全审查。

4.5. 数据分类分级

为系统化开展数据分类分级管理工作，企业可结合自身情况参考以下建议：

4.5.1. 数据资产梳理与清单管理

a. 企业可全面梳理信息系统中的数据资产，建立涵盖一般数据、重要数据与核心数据的数据资产清单。

b. 可明确数据资产管理的相关责任部门与责任人，确保资产信息清晰可查。

c. 可建立数据资产变更管理机制，对数据内容、分类、分级、标识等变更设置审批流程。

d. 可部署数据资产管理平台，支持数据资产的登记、导入、编辑、发布和注销等全生命周期管理。

4.5.2. 分类分级方法建设

a. 可制定符合业务特点的数据分类分级方法、原则和操作指南，为实际工作提供依据。

b. 可定期评审并优化分类分级规范，确保其覆盖现有业务并保持适用性。

c. 可识别同一数据在不同环境或场景下的敏感级别差异，确保安全管控的时效性与准确性。

4.5.3. 制度流程与跟踪机制

a. 可及时跟踪国家及行业主管部门的最新管理要求，适时更新和优化数据资产管理制度与流程。

b. 可建立数据资产的日常管理机制，保障分类分级工作持续有效运行。

4.6. 数据安全监测

为有效识别和应对数据安全风险，企业可结合自身情况参考以下建议，逐步建立和完善数据安全监测体系：

4.6.1. 监测机制与流程

a. 企业可为核心业务系统建立数据安全风险监测机制，定期组织开展风险监测活动。

b. 可建立数据安全预警信息的发布流程，确保在发现隐患时能及时通知相关运营人员，并采取应急响应措施。

c. 可建立数据安全风险信息的上报与共享机制，对监测信息进行统一汇集、分析与研判。

4.6.2. 监测平台与手段

a. 可建立数据安全监测平台，对账号、IP、数据接口等关键要素进行实时监控，识别如账户盗用、数据滥用、外发、篡改、窃取、爬取等安全威胁。

b. 监测平台可支持对安全风险进行可视化展示，提升风险感知与沟通效率。

4.7. 数据安全应急

为有效应对和处置数据安全事件，企业可结合自身情况参考以下建议，逐步建立并完善数据安全应急响应体系：

4.7.1. 制度与流程建设

a. 可建立数据安全事件管理与应急响应的总体流程、工作指南及应急预案，明确数据安全事件的分类、分级标准与处置原则。

b. 可细化不同类别事件的处理流程与规范，涵盖监测、预警、上报、分析、处置、恢复等环节。涉及重要数据与个人信息安全事件的预案可细化至操作指令级。

c. 可建立应急响应复盘机制，对事件处置过程与结果进行总结评估，并向网络与信息安全管理小组汇报。

4.7.2. 培训与意识提升

a. 可定期开展应急响应制度、策略与防范措施的培训宣传，培养相关人员的安全意识与基本响应能力。

b. 可对关键岗位人员进行专项培训与考核，确保其熟悉应急预案与操作流程。

4.7.3. 演练与持续改进

a. 可依据数据安全应急预案，定期组织应急演练活动，以检验预案的有效性与人员的响应能力。

b. 可通过演练与实战复盘，持续优化应急流程、预案细节及技术措施。

4.7.4. 技术平台支持

a. 可部署应急响应管理平台，辅助进行安全事件的监测、预警、协调处置与过程记录。

b. 应急管理系统可逐步集成分析研判功能，探索基于事件分析的预警提示与自动化响应决策能力。

4.8. 数据安全审计

为系统化开展数据安全审计监督，企业可参考以下建议构建持续改进的审计能力：

4.8.1. 审计制度与计划

a. 企业可建立数据安全审计的相关流程、文档模板与操作规范。

b. 可制定数据安全审计计划，明确审计范围、频率与方法，推动审计工作有序开展。

4.8.2. 审计执行与覆盖

a. 可对数据全生命周期各阶段的数据访问与操作行为进行审计，重点关注高风险活动。

b. 可结合自动化和人工审计方法，对数据处理行为进行有效监控。

c. 可定期（如每年）开展审计工作，并形成审计报告，报告中可包含发现的风险点、原因分析及改进建议。

4.8.3. 人员能力与风险识别

a. 负责审计工作的人员可具备数据安全风险识别能力，熟悉组织内部数据访问与操作范围。

b. 相关人员可充分理解审计要求与评估规则，能够准确识别风险并及时采取应对措施。

4.8.4. 审计平台与技术支撑

a. 可建立统一的数据安全审计平台，实现各类数据访问和操作日志的集中处理与分析。

b. 通过平台化支撑，可提升对数据安全风险的感知能力与分析效率。

4.8.5. 闭环管理与持续优化

a. 可依据审计结果，持续调整和优化数据安全管理制度与流程，形成管理闭环。

b. 可结合监管要求及内部策略变化，及时调整审计方向与规则，保持审计工作的适应性与有效性。

5. 数据全生命周期技术能力

5.1. 数据收集

a. 可建立数据收集安全管理制度，明确收集目的、范围、频次及知情同意要求，确保合法合规。

b. 可定义数据收集规则与流程，评估数据源合法性及采集风险，并保障过程完整记录。

c. 可部署具备日志审核功能的数据收集工具，定期评估管理效果，并持续优化规则与手段。

5.2. 数据传输

为保障数据传输过程的安全，企业可参考以下建议建立和完善管理措施：

5.2.1. 制度与规范

a. 可制定数据传输安全管理规范，在数据分类分级基础上，明确各业务场景的安全需求，如传输通道加密、数据内容加密、身份鉴别、签名验签及接口安全等要求。

b. 可建立数据加密与密钥管理流程，明确不同类别数据的加密传输范围、算法选择及密钥管理规则。

c. 可建立数据传输接口安全管理规范，涵盖安全域内、跨安全域等场景的接口安全要求。

d. 可建立传输安全策略变更的审核与监控制度，并定期对传输通道策略、密码算法配置等保护措施进行审核。

5.2.2. 技术措施与能力

a. 可了解常用数据加密策略、安全通道方案、身份认证技术及国家推荐加密算法，结合实际业务选择适当的传输安全管理方式。

b. 可对传输数据实施完整性检测，并具备数据容错或恢复的技术手段。

c. 可根据技术发展评估新型加密保护技术的影响，适时引入以应对新出现的安全风险。

5.3. 数据存储

为加强数据存储介质的安全性，企业可结合自身情况参考以下建议：

5.3.1. 制度体系建设

a. 可建立数据存储安全管理制度体系，涵盖管理政策、实施细则与指导方案，重点完

善个人信息存储的相关规范。

b. 可定义存储介质类型及存储系统架构的设计与安全要求。

5.3.2. 管理规范与配置

a. 可明确数据存储管理的安全规范与配置规则，包括账号权限、访问控制、日志留存时间（如不少于六个月）、数据保存周期（如电子病历数据不少于 30 年）及加密管理等要求。

b. 可建立存储介质管理机制，对物理实体介质、虚拟存储介质等进行分类标识，识别存储内容的敏感度及数据所有者。

5.3.3. 介质保存与环境控制

a. 可建立存储介质的保存环境制度，明确介质引入、出入库、保存环境及可用性保障等要求。

b. 可建立存储介质环境变更与配置变更的管理机制，规范配置规则、操作流程、发布要求与授权管理等标准。

5.4. 数据处理

5.4.1. 数据脱敏

为安全有效地开展数据脱敏工作，企业可结合自身情况参考以下建议：

5.4.1.1. 制度与规范

a. 可建立数据脱敏管理规范与制度，明确脱敏规则定义、策略配置及方法使用限制等基本要求。

b. 可规定数据脱敏的具体处理流程，并对脱敏操作过程进行记录和文档化管理。

5.4.1.2. 流程与分类

a. 可依据数据分类分级清单，针对不同安全级别的数据制定相应的脱敏处理流程。

b. 可在屏蔽敏感信息的同时，保留原始数据的格式与属性，确保脱敏数据在开发、测试等场景中的可用性。

5.4.1.3. 技术工具与手段

a. 可提供脱敏数据识别与验证工具或服务组件，用以验证脱敏结果是否符合法律法规要求。

b. 可提供静态脱敏工具，满足数据共享过程中对重要数据和个人信息的保护需要。

c. 可提供一种或多种风险可控的脱敏措施（如泛化、抑制、干扰等）处理敏感数据。

d. 可针对特定使用场景和策略，部署数据动态脱敏方案。

5.4.2. 数据处理环境安全

为保障数据处理环境的安全可靠，企业可结合自身情况参考以下建议：

5.4.2.1. 环境安全要求

a. 可明确核心系统在数据使用、开发、测试等环境中的安全管理要求。

b. 可在信息系统规划设计、开发建设与运行维护各阶段制定相应的安全控制措施，系统化管理安全风险。

5.4.2.2. 过程控制与日志

a. 可建立数据处理日志管理工具，记录用户在数据处理系统中的操作行为，实现操作可追溯。

b. 使用自动化工具访问或收集数据时，可提前评估其对网络服务性能、功能的影响，避免干扰正常服务或侵犯他人权益，出现问题时及时停止操作并采取补救措施。

5.4.2.3. 技术防护措施

a. 可建立数据处理过程中的数据防泄漏技术工具，防范敏感数据在加工处理环节泄露。

b. 可隔离内部与外部网络环境，重要数据和个人信息的处理操作建议在内网环境中进行。

c. 可针对不同业务场景部署相应的数据防泄露工具，增强重要数据与个人信息的安全防护能力。

5.5. 数据使用

为有效管理数据访问权限，防止未授权访问，企业可参考以下建议构建访问控制体系：

5.5.1. 制度与流程建设

a. 可建立用户身份鉴别和访问控制管理机制，明确数据权限的申请、审批、变更及撤销流程。

b. 可制定数据交易服务安全管理策略，界定安全目标、范围、原则与框架。

c. 可遵循最小必要和职权分离原则，为不同账户分配完成任务所需的最小权限，并形

成权限间的相互制约。

5.5.2. 身份与权限管理

a. 可建立统一的身份鉴别管理系统，实现对数据资源访问的统一身份管理。

b. 可建立人力资源系统与权限管理的联动机制，确保离岗、转岗人员权限及时回收。

c. 可建立并定期更新敏感数据权限清单，明确权限的安全要求、分配策略和授权范围。

d. 可对系统登录用户进行唯一身份标识与鉴别，设置鉴别信息复杂度要求，并启用登录失败处理功能。

5.5.3. 访问控制机制

a. 可明确全部系统（尤其是核心与重要系统）数据库的身份鉴别、访问控制与权限管理要求。

b. 可建立面向数据应用的访问控制机制，管理访问时效并进行安全验证。

c. 可采用技术手段实现身份鉴别与权限管理的联动控制。

5.6. 数据交换

5.6.1. 数据内部共享安全

为规范内部数据共享并控制相关风险，企业可参考以下建议建立管理机制：

5.6.1.1. 制度与流程

a. 可建立核心业务数据的内部共享原则、范围界定、安全制度及审批流程。

b. 可建立数据内部共享安全评估与授权审批机制，对大量或敏感数据的共享进行风险评估与审批控制。

c. 可依据数据分类分级要求，制定符合业务规则的内部共享安全策略，包括授权策略、流程控制及不一致处理机制等。

5.6.1.2. 技术控制与审计

a. 可采取技术措施记录数据内部共享行为，确保操作可追溯。

b. 可采用审计工具定期审计共享行为，防止超出授权使用范围。

c. 可对参与共享的终端设备、用户或服务组件实施有效访问控制，确保身份真实合法。

d. 可制定共享审计策略与日志管理规程，保存共享过程中的出错处理记录。

5.6.1.3. 介质管理与数据清理

a. 在使用存储介质或设备导出数据时，可建立介质标识规范，定期验证导出数据的完整性与可用性。

b. 可在共享完成后及时清理共享通道中的缓存数据，防止数据残留和恢复风险。

5.6.2. 数据接口安全

为保障数据接口调用安全，企业可参考以下建议建立管理机制：

5.6.2.1. 制度建设

a. 可建立数据接口的审批、开通等相关流程制度，规范接口安全管理

b. 可制定数据接口安全控制策略，明确接口使用的安全限制和控制措施，包括身份鉴别、访问控制、安全协议等要求

5.6.2.2. 技术措施

a. 可采用技术工具实现对数据接口调用的身份鉴别和访问控制

b. 可通过时间戳等技术手段增强接口调用的安全性

5.6.2.3. 人员管理

a. 负责数据接口的工作人员可充分了解接口调用的业务场景，具备安全意识、技术能力和风险控制能力

5.6.2.4. 第三方合作

a. 与第三方进行数据接口合作时，可通过签署协议明确数据使用目的、保密要求和安全责任

5.7. 数据销毁

为规范数据及存储介质的销毁处理，保障数据生命周期末端安全，企业可结合自身情况参考以下建议：

5.7.1. 制度与策略建设

a. 可建立数据与存储介质的销毁策略和管理制度，明确销毁原则、场景、对象、方式及效果验证标准。

b. 可依据数据分类分级结果，制定核心业务数据及存储介质的销毁方案，明确操作流程与审批机制。

c. 可定期审核数据存储的合理性，并根据法律法规、合同要求的变化，及时更新销毁方案。

5.7.2. 流程与管控措施

a. 可建立规范的销毁流程和审批机制，对审批及销毁过程进行记录和控制。

b. 可明确已共享数据或已被其他用户使用的数据的销毁管控措施。

c. 可针对不同存储介质建立针对性的销毁流程和检验标准。

d. 可定期对数据销毁效果进行抽样评估，确保销毁有效性。

5.7.3. 人员能力与合规性

a. 负责数据销毁的工作人员可充分了解相关合规要求，并具备制定销毁方案的能力。

b. 销毁工作需符合国家相关法律和标准，特别是对个人信息等敏感数据的处理要求。

5.7.4. 技术手段与资源保障

a. 可配置必要的技术手段，确保敏感数据及其副本以不可恢复的方式销毁。

b. 可提供存储介质销毁工具，如物理销毁设备、消磁设备等。

c. 涉及物理销毁时，可委托经过认证的机构或服务商进行操作。