ICS
CCS

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX—XXXX

数字医疗网络数据安全管理规范

Standard for Data Security Management of Digital Medical Network

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业企业管理协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由××××提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：××××、××××

本文件主要起草人：×××、×××、×××

数字医疗网络数据安全管理规范

1 范围

本文件规定了数字医疗网络数据安全管理规范，涵盖数据分类分级管理、组织架构与责任体系、技术防护要求、应急响应与事件处置、监督与持续改进等。

本文件适用于医疗机构（含公立医院、民营医院、社区卫生服务中心等）、第三方医疗技术服务商、健康管理平台等主体的网络数据安全管理活动，涵盖医疗数据采集、存储、传输、使用、共享及销毁全生命周期，

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37988 数据安全能力成熟度模型

GB/T 39725-2021 健康医疗数据安全指南

DB1310T 338-2024 数字乡村 县域医疗机构网络数据安全管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

重要医疗数据

一旦泄露、篡改或损毁，可能直接危害公共健康、社会稳定或国家安全的数据（如传染病监测数据、基因序列信息）。

3.2

个人健康医疗数据

单独或结合其他信息可识别特定自然人生理/心理健康状态的电子数据（如电子病历、体检报告）。

3.3

数据信托

第三方受托机构在授权范围内对医疗数据进行安全托管与合规流转的模式。

3.4

数据脱敏

通过对数据进行去标识化、匿名化或假名化处理，使其无法直接关联到特定个人，但仍可用于统计分析或研究。

4 数据分类分级管理

4.1 数据分类

医疗数据按业务类型分为：

——临床诊疗数据（如电子病历、医嘱、检查报告）；

——医学研究数据（如临床试验数据、基因测序数据）；

——运营管理数据（如医保结算、医院管理数据）；

——公共卫生数据（如传染病监测、疫苗接种数据）。

4.2 分类维度

4.2.1 主体类别：个人健康数据（C1 级）、重要医疗数据（C2 级）、公共健康数据（C3 级）。
4.2.2 敏感程度：公开级（可共享）、内部级（机构内部使用）、机密级（需国家审批）。

4.3 分级保护措施

4.3.1 C1 级（个人数据）：匿名化处理后方可跨机构共享，存储需符合 AES-256 加密标准。
4.3.2 C2 级（重要数据）：实施“双人双锁”访问控制，跨境传输需通过省级卫生主管部门安全评估。
4.3.3 C3 级（公共数据）：仅限国家疾控中心等授权机构使用，禁止出境。

5 组织架构与责任体系

5.1 机构设置

5.1.1 决策层：医疗机构需设立数据安全管理委员会，由院长或分管副院长担任主任。
5.1.2 执行层：
——设立专职数据安全官（DSO），需具备 CISP-PTE 或同等资质。
——IT 部门负责技术防护，法务部门负责合规审查。
5.1.3 监督层：内审部门每季度核查数据访问日志与权限分配。

5.2 协作机制

5.2.1 跨部门流程：临床科室数据调用需经 DSO 审批，IT 部门实施脱敏处理。
5.2.2 外部合作：与第三方技术服务商签订数据安全协议，明确数据泄露责任归属。

6 技术防护要求

6.1 基础设施安全

6.1.1 硬件防护：医疗数据中心需满足 GB 50174 B 级抗震标准，服务器启用 TPM 2.0 芯片加密。
6.1.2 网络隔离：院内业务系统与互联网服务采用物理隔离，关键系统部署零信任架构（ZTNA）。

6.2 数据全生命周期保护

6.2.1 采集：移动医疗 APP 不得强制索取无关权限（如血糖监测类应用获取通讯录）。
6.2.2 传输：使用国密 SM2/SM4 算法加密，禁止通过公共 Wi-Fi 传输患者数据。
6.2.3 销毁：电子数据采用不可逆擦除算法，物理介质需消磁或粉碎。

6.3 新兴技术应用规范

6.3.1 区块链：节点身份需通过数字证书验证，智能合约代码需经第三方审计。
6.3.2 人工智能：诊断辅助算法需通过可解释性测试，防止种族、性别歧视性偏差。

7 应急响应与事件处置

7.1 预案分级

7.1.1 Ⅰ级(特别重大)：导致核心业务系统瘫痪超过 72 小时或 50 万条以上患者数据泄露；
7.1.2 Ⅱ级(重大)：影响重要信息系统运行 24-72 小时或 10-50 万条敏感数据泄露；
7.1.3 Ⅲ级(较大)：局部系统中断 2-24 小时或 1-10 万条数据泄露；
7.1.4 Ⅳ级(一般)：短暂影响且数据泄露不超过 1 万条。

7.2 应急处置流程

7.2.1 预警与报告

7.2.1.1 监测预警：部署态势感知平台实时监控，建立"三化六防"(实战化、体系化、常态化)机制。

7.2.1.2 初判上报：Ⅰ-Ⅱ级事件须在 30 分钟内报主管部门，Ⅲ-Ⅳ级事件 2 小时内上报。
7.2.1.3 信息通报：按《数据安全法》要求及时向社会发布警示信息。

7.2.2 应急处置

7.2.2.1 隔离遏制：立即断开受影响系统网络连接，防止危害扩大。
7.2.2.2 取证分析：通过日志审计、流量分析等技术手段定位事件源头。
7.2.2.3 数据恢复：启用加密备份数据，确保核心业务系统优先恢复。

7.2.3 事后处置

7.2.3.1 漏洞修复：全面排查系统弱点，更新补丁和防护策略。
7.2.3.2 整改报告：重大事件处置后 15 个工作日内提交整改报告。
7.2.3.3 应急演练：每季度至少开展 1 次模拟演练，检验预案有效性。
7.2.3.4 审计追溯：保留完整访问日志不少于 6 个月，支持行为溯源。

7.2.4 关键技术要求

7.2.4.1 防护体系：部署边界防火墙、WAF、IPS 等设备构建纵深防御体系。
7.2.4.2 数据保护：对敏感数据实施加密存储(AES-256/SM4)和传输(TLS1.2+)。
7.2.4.3 备份机制：核心数据实行异地容灾备份，RPO≤15 分钟。

7.3 攻防演练

每年至少开展1次实战演练（如模拟医院HIS系统遭勒索攻击），演练报告需包含攻击路径复盘与改进计划。

8 监督与持续改进

8.1 合规审计：第三方机构每年评估数据安全成熟度，结果向社会公示。
8.2 违规处罚：严重违规机构纳入“医疗数据安全黑名单”，限制参与政府招标项目。