ICS 11.020
C 07

团 体 标 准

T/CHAS 10-3-7—2023

中国医院质量安全管理

第 3-7 部分：医疗保障 医疗信息

Quality and safety management of Chinese hospital——

Part 3-7: Medical service support —— Medical Information

2023-10-28 发布 2023-12-30 实施

中国医院协会 发布

目　次

前　言

《中国医院质量管理》分为以下部分：

——第 1 部分：总则

——第 2 部分：患者服务

——第 3 部分：医疗保障

——第 4 部分：医疗管理

《中国医院质量管理　第 3 部分：医疗保障》包括以下部分：

——第 3-1 部分：医疗保障　人力资源

——第 3-2 部分：医疗保障　药品保障

——第 3-3 部分：医疗保障　医用材料

——第 3-4 部分：医疗保障　医疗设备

——第 3-5 部分：医疗保障　消毒供应

——第 3-6 部分：医疗保障　多学科联合会诊

——第 3-7 部分：医疗保障　医疗信息

——第 3-8 部分：医疗保障　后勤物资

——第 3-9 部分：医疗保障　环境设施保障

——第 3-10 部分：医疗保障　社工保障

本标准是第 3-7 部分。

本标准按照 GB/T 1.1-2020 给出的规则起草。

本标准由中国医院协会提出并归口。

本标准主要起草单位：江苏省人民医院（南京医科大学第一附属医院），福建省立医院，西安交通大学第一附属医院，中国医学科学院医学信息研究所，华中科技大学同济医学院附属同济医院，浙江大学医学院附属第一医院，浙江医院，云南省肿瘤医院，医院标准化专业委员会。

本标准主要起草人：刘云，王忠民，张琼瑶，卫荣，钱庆，张晓祥，杨荣伟，费科峰，路健，景慎旗，郭建军，戴作雷，朱越石，刘月辉，刘丽华。

中国医院质量安全管理 第3-7部分 医疗保障 医疗信息

1 范围

本标准规范了各级医疗机构医疗信息生成、医疗信息使用和医疗信息管理的关键要素。

本标准适用于各级医疗机构对医疗信息的使用及质量安全管理。

2 规范性引用文件

下列文件对于本标准分册的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准分册。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准分册。

GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

WS/T 788-2021 国家卫生信息资源使用管理规范

全国医院信息化建设标准与规范（试行）（国卫办规划发〔2018〕4号）

国家健康医疗大数据标准、安全和服务管理办法（试行）（国卫规划发〔2018〕23号）

医疗卫生机构网络安全管理办法 （国卫规划发〔2022〕29号）

3 术语与定义

GB/T22081-2016、GB/T 22239-2019、GB/T 37964-2019、GB/T 22240-2020、WS/T 788-2021界定的以及下列术语和定义适用于本文件。

3.1

医疗信息 medical information

医疗机构在开展业务过程中采集、存储、传输、处理和产生的以数字化形式生成、转录的各类信息。医疗信息应具备及时性、准确性、完整性和真实性。

3.2

数据质量 data quality

在指定条件下使用时，数据的特性满足明确和隐含要求的程度。

3.3

数据安全 data security

数据全生存周期的安全管理与控制。

3.4

网络安全 cyber security

通过采取必要措施、防范对网络的攻击,侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。

4 关键要素

医疗信息质量安全管理关键要素见图1。

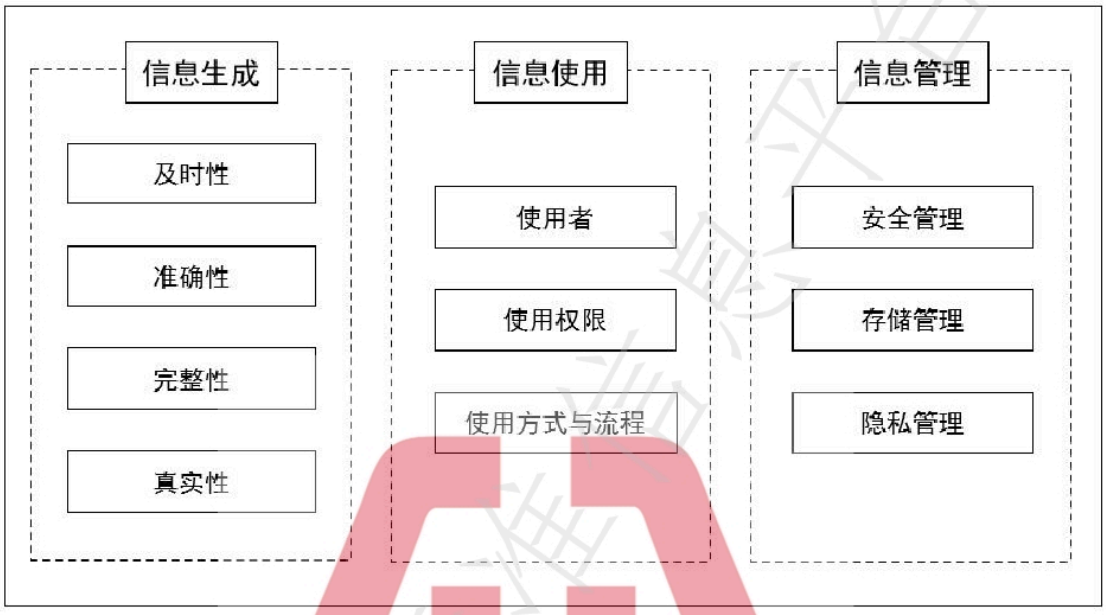

图1 医疗信息质量安全管理关键要素

5 要素规范

5.1 信息生成

医疗机构应制定医疗信息记录的管理要求，医疗机构应全过程、全要素、完整记录医疗业务信息，确保医疗信息的及时性、准确性、完整性、真实性。医务工作人员应客观、真实、准确、及时、完整地记录医疗信息。医疗信息的记录者应对数据的及时性、准确性、完整性、真实性负责，不得随意增加、删除或修改有效数据。

5.1.1 及时性

应确保医疗信息实时、准确地获取和记录。医疗信息传递应及时、准确。尤其是在跨科室协作、会诊和转诊等业务场景下，应杜绝医疗信息更新不及时。具体要求包括但不限于：

5.1.1.1 信息快速共享：医疗机构应将医疗信息电子化存储在存储介质上，实现医疗信息实时共享，提高信息传递速度和效率。

5.1.1.2 自动提醒：医疗信息录入系统应具备自动提醒功能，如检查报告生成时自动通知，以确保及时查看结果并制定治疗方案。

5.1.1.3 实时同步更新：如药品库存、医嘱执行等相关医疗信息应实时同步更新，确保治疗措施及时调整。

5.1.2 准确性

医疗机构应制定严格的信息录入规范，保证医疗信息录入准确。对于医疗信息生成环节的准确性，应包括但不限于以下要求：

5.1.2.1 标准化输入：医疗信息生成系统应有预设的输入模板和数据字典，规范记录人员的信息输入，降低因自由录入、格式或字典不统一等原因导致的信息错误。

5.1.2.2 错误提示和校验：应对输入的信息进行实时校验，如药品剂量超出正常范围时给予提示，帮助医护人员发现并及时纠正错误。

5.1.2.3 数据互联互通：应实现不同部门之间的信息共享，如检查结果、药品库存等，减少因信息传递过程中的失误导致的错误。

5.1.2.4 避免重复信息：应对如患者历史病案记录等医疗信息进行整合和检索，降低因重复输入或遗漏信息导致的准确性问题。应提高信息的多系统复用。

5.1.2.5 自动化数据分析：应通过数据挖掘、统计分析等功能辅助医疗行为，降低个人主观影响，减少人为误差。

5.1.2.6 规范的修正机制：即建立规范的修正机制，在发生信息记录错误后，指导使用者在有痕前提下逐步操作，避免错误信息共享。

5.1.3 完整性

医疗机构应制订包括但不限于以下要求，确保医疗信息记录的完整性：

5.1.3.1 信息一体化存储：应将所有医疗信息集中电子化存储在存储介质中，避免因纸质记录遗失、损坏等原因导致的信息不完整。

5.1.3.2 标准化模板：应提供预设的输入模板，引导记录者按照规定格式填写各项信息，确保记录的完整性。有漏缺项提示与校验。

5.1.3.3 历史记录追溯：应关联和整合患者的历史病例记录，保证医疗信息的完整和连续，为诊断和治疗提供全面的信息支持。

5.1.3.4 数据备份与恢复：医疗机构应制定合理的数据备份策略，定期对医疗信息进行备份，将重要数据存储在安全的云端或本地备份设备中。在面临硬件故障、系统崩溃、网络攻击等意外情况时，可以迅速恢复，确保医疗信息的完整性。降低因数据丢失带来的损失和风险。

5.1.3.5 审计与访问控制：医疗机构应制定合理的数据审计与访问控制机制，限制未授权访问行为，审核并跟踪数据访问、录入、删除的动作，降低数据记录阶段数据被破坏、丢失的可能性。

5.1.4 真实性

医疗机构应制定包括但不限于以下要求，确保医疗信息记录的真实性：

5.1.4.1 信息可追溯：如电子病历等系统，应记录医疗信息的创建、修改等操作过程，应具备追溯信息来源渠道，确保医疗信息的真实性。

5.1.4.2 权限管理：医疗机构应对各医疗系统，设定不同级别的访问权限，防止未经授权的人员篡改或删除患者信息，保障数据的真实性。医疗机构还应建立权限审计和监控机制，定期检查权限使用情况，及时发现并纠正不当行为。在人员离职或岗位调整时，应及时调整其系统权限，防止因权限滥用导致的数据泄露或篡改。

5.1.4.3 数据加密与密码管理：应对医疗信息记录、传输、存储等过程采用国产加密技术管理，确保数据的安全性和真实性。为进一步加强数据安全，医疗机构应制定严格的密码管理制度，要求医护人员使用强度较高的密码，并定期更新。应实施多层次的身份验证机制，如设置不同级别的访问权限，使用双因素身份认证等，以降低医疗信息泄露风险。

5.1.4.4 数字签名：应采用数字签名技术进行身份验证和确认，便于追溯和审计医疗信息的操作记录，便于发现和纠正潜在的错误或不当行为。医疗机构应对医护人员进行相关培训，规范数字签名使用，使其了解数字签名的重要性和使用方法。进一步保障医疗信息的真实性。

5.2 信息使用

医疗机构为信息处理的主体，在对医疗信息进行使用之前，应根据数据资产目录明确标记数据的级别和类别（参考行业标准《WS/T787-2021国家卫生信息资源分类与编码管理规范》），识别核心数据，重要数据及一般数据。针对不同级别和类别的数据制定对应的使用及管理流程。同时，对核心数据及重要数据实施动态管理机制，当数据的业务属性、使用场景、公开范围等发生变化时，医疗机构应重新开展分类和定级。

5.2.1 使用者

5.2.1.1 医疗信息是敏感的个人数据，医疗机构应规范医疗信息的使用者和要求，为保障患者隐私和信息安全，医疗机构应采取严格的管理措施，确保医疗信息只在合法授权的范围内使用。禁止包括但不限于以下对象：

a）未经授权的人员：没有授权的人员，包括但不限于未经许可的工作人员、家属、访客等，不得访问或使用医疗信息。

b）商业机构：商业机构（如医疗企业、广告商、保险公司等）在未经患者明确同意的情况下，不得访问或使用患者的医疗信息。

c）恶意攻击者：黑客、网络犯罪分子等恶意攻击者不得非法获取和使用医疗信息。医疗机构应采取相应的信息安全措施，防止这类行为发生。

d）身份假冒者：医疗机构应严防假冒他人身份访问或使用医疗信息的行为。应实施严格的身份验证机制，确保只有授权人员才能访问相关医疗信息，适用于《电子签名法》。

e）非法信息经营者：擅自出售、传播或泄露他人医疗信息的行为是非法的。违反法律法规的信息经营者不得访问或使用医疗信息。

5.2.1.2 为保障患者隐私和信息安全，医疗机构需采取严格的管理措施，确保医疗信息只在合法授权的范围内使用。同时，所有使用者都应遵循相关法律法规和伦理原则，确保医疗信息的合规、安全和有效利用。

5.2.1.3 医疗信息使用要求因不同的使用者而有所不同，医疗机构应根据临床、科研、教学、管理、个人、医保以及其他机构人员等使用身份划分要求，包括但不限于：

a）临床：临床医生和护士需要具备专业知识和技能，确保能够准确地理解和应用医疗信息，提高诊疗质量。应遵守医疗伦理和法律法规，保护患者隐私。

b）科研：科研人员在使用医疗信息时应遵守科研伦理和法律法规。在获取和使用患者信息时，需要征得患者或其代表的同意，并确保数据的脱敏处理。

c）教学：基于教学目的，在使用医疗信息进行教学活动时，应保证医疗信息来源的真实性和可靠性。同时，遵守教育伦理和法律法规，确保患者信息的数据脱敏处理。

d）管理：在使用医疗信息进行医疗机构管理时，需了解相关法律法规和政策。应确保数据安全、合规，并对数据的使用和存储进行有效权限分级监管。

e）个人：在访问和使用医疗信息时，应确保个体隐私和信息安全。在流程约束和管理监督下，个体可以查询、核对和修改自己的医疗信息（医疗信息修改仅限于修改个人属性数据），但不得泄露他人的隐私。

f）医保：医保人员在使用医疗信息进行审查、结算等工作时，需遵循相关法律法规。应确保数据的真实性、合规性，并保护患者隐私。

g）其他机构人员：公安、监察、法院、审计、保险等机构人员在调用患者诊疗信息时，需严格遵循相关法律法规，依据相关流程，出具正规文件申请调阅。对已调阅的数据，应严格保护患者隐私，严防数据泄露。

5.2.1.4 不同身份的医疗信息使用者都应具备信息安全意识，遵循医疗机构的信息安全规定，分级授权访问数据，以防止信息泄露或被恶意攻击。同时，医疗机构应为不同使用者提供相应的培训和指导，确保医疗信息的合规、安全和有效使用。

5.2.2 使用权限

5.2.2.1 应建立医疗信息创建、修改、归档等操作的授权制度，确保患者诊疗信息可追溯性，严禁随意对后台原始数据进行修改。

5.2.2.2 应建立患者医疗信息使用权限、范围、审批流程和安全保护制度，明确医务人员使用患者医疗信息权限和授权部门。医务人员应当遵循合法、依规、正当、必要的原则，不得擅自出售患者信息，不得未经批准擅自向他人或其他机构提供患者诊疗信息。

a）建立健全对院内医务工作人员因科研、教学、学术交流等对患者诊疗信息复制的审批制度和流程，明确脱敏范围。

b）建立健全公安、监察、法院、审计、保险等机构对患者诊疗信息的调用的审批制度和流程，明确脱敏范围。

c）建立健全患者诊疗信息向社会团体、AI智能诊断代理机构、院外数据平台、卫生行政部门附属机构等以各种形式提供或上传的审批制度和流程，明确脱敏范围。

d）其他非卫生行政部门之外的患者诊疗数据的复制、上报、上传均应纳入数据再利用的制度和流程，明确脱敏范围。

e）建立健全医疗设备工作站、从事医疗业务的计算机、带有存储功能的其他设备报废处置前的患者诊疗数据处理制度和管理流程。

f）建立健全云托管存储服务终止前的患者诊疗数据处理制度和流程。

g）任何人不得未经批准擅自向他人或其他机构提供患者诊疗信息。任何人不得出售患者信息。

5.2.2.3 当医疗机构的核心数据或重要数据在使用过程中涉及跨主体流动或出境的场景，需国家相关部门进行数据安全风险评估，并遵循对应的法律法规。

5.2.3 使用方式与流程

应建立医疗信息使用授权管理制度和流程，医疗信息的使用包括借阅、编辑、修改、访问、查询等接触患者诊疗信息的行为。

5.2.3.1 各职能部门定期对系统操作权限进行查核，发现授权错误或未及时终止的授权问题及时纠正。数据服务人员应注意数据安全保密，不得对无关人员泄露医疗机构和患者个人信息，不在工作终端上长期保存业务数据。在每项服务任务完成后，应将工作终端上该任务所使用的数据删除。

5.2.3.2 医疗信息系统用户权限应采用职能部门统一管理、统一授权的原则，根据业务工作需要设置业务科室权限范围。对新入职、下乡、支援、进修、规培、转岗、退休人员实行权限动态管理。授权操作人员应严格根据授权审批进行授权，禁止私自变更授权范围。

5.2.3.3 医疗机构信息管理部门应建立工作人员和外来人员操作权限授权管理制度和流程，并与接触患者诊疗信息的员工签订患者诊疗信息安全保密责任书。医疗机构与医疗信息的服务公司，如软件公司、系统集成公司、运营商等签订保密协议。医疗机构设置数据服务岗（可兼职）为用户提供数据服务。服务人员需熟悉所分管领域信息系统的数据结构，具备数据查询和统计分析能力。

5.2.3.4 医疗机构使用有效的操作人员身份识别方式，使用用户名、密码登录的，应采用强密码登录规则，或符合法律规范的人工智能登录技术。医务人员应妥善保管自己的用户名、密码或数字身份登录的

Ukey，不得泄露、丢失与外借。各相关职能部门应加强医务人员身份登录管理，严禁使用他人用户名、密码或数字证书等其他非法技术手段登录系统，确保患者诊疗信息的安全。

5.2.3.5 在接受医疗信息使用任务后，要与使用者充分沟通，明确数据源和数据提取条件，严谨细致地进行信息处理。数据服务完成后，要由其他数据服务人员对数据处理结果进行核对检查，确保结果数据准确无误。数据处理过程和主要处理操作，应进行记录，以保证结果数据可再现。

5.2.3.6 各相关职能部门建立患者诊疗信息生成过程各环节的安全保护制度，防止诊疗过程中产生的患者诊疗信息的丢失和泄露。对于非患者医疗直接相关的用户需求，在交付的结果数据中一般不应包含患者个人信息。特殊情况下，需要包含患者个人信息的，在交付结果数据时，由申请者签署数据保密承诺书。

5.3 信息管理

5.3.1 安全管理

5.3.1.1 应建立信息安全管理机制。医疗机构主要负责人是医疗机构患者诊疗信息安全管理第一责任人。建立由医疗机构主要院领导为组长、主管院领导为副组长，医务科、质量管理办公室、门诊办公室、病案管理科、护理部、药剂科、科教科、设备科及信息管理部门等为成员的医疗信息数据安全委员会。

5.3.1.2 实行信息安全等级保护和用户使用权限划分，明确授权部门及具体实施部门权限，并建立权限动态调整机制。定期开展患者诊疗信息安全自查工作，不断提升患者诊疗信息安全防护水平，防止信息遭到篡改、破坏、泄露或者非法获取、非法利用。要建立患者诊疗信息系统安全事故责任追究机制，在发生或者可能发生患者诊疗信息遭到篡改、破坏、泄露或者非法获取、非法利用的情况时，应当立即采取补救措施，按照规定向有关部门报告。

a）建立患者诊疗信息安全定期检查机制，患者信息安全管理小组定期检查各项制度落实情况和信息安全保护情况，记录相应台账。

b）建立患者诊疗信息系统安全事故责任追究机制。

c）在发生或者可能发生患者诊疗信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定向有关部门报告。

5.3.1.3 为保障医疗机构网络系统的安全运行，保护网络系统中的数据安全，防止和减少因各种因素对网络的破坏、干扰和非法入侵等危害应采取各种技术和管理措施包括但不限于：

a）信息管理部门设置网络安全管理员负责医疗机构网络信息安全技术防护和安全管理工作，设置网络安全审计员（可兼职）负责对医疗机构网络安全防护体系运行情况进行监督。网络安全管理员、网络安全审计员与网络管理员、数据库管理员岗位独立，网络管理员、数据库管理员对网络安全管理员和网络安全审计员工作提供协助配合。

b）开展医疗机构网络信息安全风险分析评估，必要时邀请外部技术专家参加。针对安全风险，结合网络安全等级保护相关标准要求，组织制定医疗机构网络信息安全技术防护方案，并按方案实施技术防护，根据情况变化提出安全防护改进措施。

c）网络安全审计员对网络安全运行情况进行日常监测和分析，每周对网络信息安全防护设备设施的工作日志、数据库访问审计日志进行检查分析，对检查结果进行记录，发现异常及时报告和处置。

d）网络安全管理员负责各类系统软件安全补丁的收集、安装和病毒库升级。当补丁安装涉及生产系统运行时，应与相关系统负责人先行测试，稳妥无误后再正式安装。

e）网络交换机、服务器、数据库系统等关键设备设施管理员用户不得使用默认口令和弱口令，管理员用户名和口令不得泄露给他人。

f）信息管理部门应对工作人员、外包服务人员、厂商驻场工程师进行网络安全教育，组织学习网络安全管理相关制度，组织人员签署网络信息安全承诺书。应对于各类系统的API接口进行审核，明确接口调取的数据范围，并签署承诺书。对离职或转岗人员要及时收回其设备、系统、数据操库等作权限。

g）医疗机构应根据《中华人民共和国网络安全法》的要求，针对不同的系统落实不同等级的保护，并每年开展对应的测评工作。

h）医疗机构应根据《中华人民共和国密码法》的要求，针对三级及以上的系统落实同步规划，同步建设，同步运行的原则，每年进行商用密码应用安全性评估工作。

5.3.1.4 信息管理部门负责对医疗信息系统产生的患者诊疗信息的存储、备份、安全防护等，健全技术设施、全流程数据安全管理制度和应急预案，确保信息的可恢复性、患者诊疗信息的完整性、稳定性和可溯源性。建立患者诊疗信息安全风险评估和应急工作机制，制定应急预案。

a）各职能管理部门针对职责范畴，每年进行不少于一次的信息安全风险评估。针对弱口令、漏洞等安全风险进行排查，针对已建设安全设备进行有效性验证，并对体系内资产进行清点梳理。对在医疗流程中可能产生的信息篡改、破坏、泄露的环节的不安全因素采取有效措施，提高信息保护能力。医疗机构信息管理部门应至少每半年组织一次信息系统各类故障应对处置演练，全面检验故障应急准备情况，培训提升故障处置技能。

b）信息管理部门应围绕医疗数据的安全保护，设定专职岗位，培养技术人才，建立健全各项运维制度。至少每年对医疗数据中心的安全措施进行技术评估，采取有效措施，确保患者诊疗数据的安全。信息管理部门负责人直接负责信息系统应急准备和应急处置领导工作。机房管理员、服务器管理员、数据库管理员、网络管理员、网络安全管理员、各应用系统管理员负责各自职责范围内的故障风险评估，分工协同制定应急预案和参与应急处置。

c）医疗机构应有充分的预案，保障数据中心的网络、设备、环境、供电等处于安全有效状态。同时按照各类信息系统故障应对预案，平时应准备故障应急处置所需的备用设备、软件、线路、工具、材料等，并保持处于可用和易获得状态。

d）建立患者诊疗信息安全事故应急预案。在故障应急处置后，应彻底解决故障问题，将信息系统和应急准备恢复至完好状态，对故障原因、处置过程、应急预案的高效性进行总结和评估，采取措施减少故障发生，优化改进处置方案。

5.3.2 存储管理

5.3.2.1 各医疗机构宜按照 GB/T 22081-2016、GB/T 22239-2019和GB/T 22240-2020标准做好医疗信息数据存储管理工作。应对医疗信息系统故障或操作失误可能导致数据的丢失，定期或实时将信息管理部门管理的医疗机构信息系统数据（含数据库、文件数据）复制到生产系统之外的存储介质保存。

5.3.2.2 医疗机构信息管理部门应设置数据库管理员，负责信息系统数据备份方案的设计、数据备份与数据恢复操作的实施工作。应负责对数据备份实施情况进行监督检查。

5.3.2.3 应按照网络安全法和网络安全等级保护2.0的要求，将信息系统划分为核心系统、重要系统和一般系统。核心系统、重要系统的数据备份方案应满足数据可恢复到断点以及断点前任意时间点的要求，核心系统还应提供重要数据处理系统的热冗余，保证系统的高可用性。一般系统的数据备份方案应满足数据可恢复到最近一次备份点的要求。

5.3.2.4 数据备份分为全数据备份和增量数据备份，全数据备份原则上每周一次（医学影像数据除外），增量数据备份除实时方式外每天一次。

5.3.2.5 数据库管理员牵头拟定信息系统数据备份方案，经过方案有效性论证通过后，按备份方案实施。备份方案修改后，需要重新组织技术论证，明确技术实施方案及路径。

5.3.2.6 数据备份操作由数据库管理员按时执行或者由系统自动进行。数据库管理员每天查看备份执行情况，对备份数据及介质做好标识并做好备份记录。

5.3.2.7 为检查数据备份的有效性，数据库管理员每月进行一次数据备份恢复测试，并做好测试记录。
5.3.2.8 数据备份和恢复测试中发现异常情况，应及时向上级报告，并采取补救措施。每周对数据备份记录检查一次。

5.3.3 隐私管理

5.3.3.1 各级医疗机构宜按照 GB/T 37964-2019 开展去标识化工作，去标识化的数据宜应用于受控公开共享或领地公开共享，宜通过数据使用协议约定数据使用目的、方式、期限、安全保障措施等。去标识化策略、流程和结果宜由医疗信息数据安全委员会审批。数据应用于临床研究和医药、医疗研发时，相关要求如下：

a）个人属性数据中可唯一识别到个人的信息或披露后会给个人造成重大影响的信息，宜隐藏。
b）个人属性数据中可间接关联到个人的信息，宜进行泛化、转换等处理。
c）医护人员姓名以及其他身份标识信息，宜删除。
d）对需要追溯到患者的情况，宜由控制者内部建立患者代码索引。
e）去标识化过程中使用的各种参数配置仅限于控制者内部专人管理。
f）在需要进行重标识确定主体时，宜由控制者内部专人处理，处理过程严格保密。
g）宜禁止使用者参与去标识化相关工作。
h）宜签署数据使用协议，约束数据的使用目的、期限以及数据保护措施等。

5.3.3.2 针对外包服务团队应制订外包服务医疗信息隐私相关管理制度与流程，至少应包括：

a）外包服务范围与内容。
b）应明确医疗机构主体与供应商的职责与权力。
c）应明确服务范围、服务期限、服务人员能力要求。
d）外包服务人员的驻场要求。
e）人员更换调整流程。
f）文件化的服务级别管理要求等。

5.3.3.3 同时应制定服务安全管理制度与流程，至少应包括：

a）应与服务供应商签订安全与保密协议，应遵照患者隐私保护条例。
b）外部人员应熟悉医疗就诊服务相关法律，熟悉患者隐私保护要求，签订承诺书。
c）应制定外部服务人员的医疗机构信息系统相关权限分配与回收管理流程。

参 考 文 献

[1]WS/T 788—2021 国家卫生信息资源使用管理规范
[2]GB/T 39725-2020 信息安全技术健康医疗数据安全指南
[3]GB/T 28827.8-2022 信息技术服务 运行维护 第8部分：医院信息系统管理要求
[4]T/GZBC 37-2020 医疗机构数据治理规范
[5]GB/T22081-2016 信息技术安全技术信息安全控制实践指南
[6]GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[7]GB/T 37964-2019 信息安全技术 个人信息去标识化指南
[8]国家健康医疗大数据标准、安全和服务管理办法（试行），国卫规划发23号文，2018
[9]郑万松，黄志中，王占明,等. 持续质量改进在医疗信息系统中的应用[J]. 中国数字医学，2013,000(005):34-35.
[10]李彬.质量管理在医疗信息系统中的应用研究[J].中国数字医学,2015,10(04):116-118.
[11]吕琳. 49例医院信息系统不良事件总结与分析[J]. 中国数字医学，2020，15(11):3.
[12]曾可，王玉，朱卫国. 信息技术相关医疗不良事件[J]. 协和医学杂志，2020，11(2):6.
[13]ECRI Institute's Health Devices Group. Top 10 Health Technology Hazards for 2018[EB/OL].https://www.ecri.org/press/Pages/ECRI-Institute-Release-2018-Top-Hazards-List.aspx
[14]刘文莉，周璟璐，张桂蓉. 基于PDCA理论的医院不良事件管理体系建设探索[J]. 重庆医学，2021,050(024):4297-4300,4306.
[15]孔琳. 智慧医院建设背景下的信息安全问题与对策[J]. 医疗卫生装备，2022，43(9):5.
[16]王雪琴，张静，汪卓赟,等. 医院信息共享的伦理风险及对策研究[J]. 中国医学伦理学，2021,34(5):4.