 DOI: https://doi.org/10.12345/bdai.v7i1.35278

# Technical Measures for Patient Privacy Protection in Hospital Intelligent Information Systems

**Jing Guo**

Zhangjiagang Fourth People's Hospital, Suzhou, Jiangsu, 215600, China

**Abstract**

With the deep integration of hospital intelligent information systems (HIIS) in clinical diagnosis, data mining, and telemedicine, the volume of privacy-sensitive data—including electronic health records, biometric data (e.g., facial recognition, fingerprints, genetic sequences), and medical behavior data—has grown exponentially, while data flow scenarios have become increasingly complex. This paper examines the practical application logic of privacy protection technologies, analyzing core technical measures for data collection, transmission, storage, and usage from a full lifecycle perspective. Through case studies of anonymization, access control, and blockchain-based evidence storage, it proposes optimized integration strategies to enhance the HIIS privacy protection framework, providing actionable technical references for its development.

**Keywords**

hospital intelligent information system; patient privacy protection; data life cycle; anonymization; access control

# 医院智能信息系统中患者隐私保护的技术措施

郭靖

张家港市第四人民医院，中国·江苏 苏州 215600

**摘　要**

随着医院智能信息系统在临床诊疗、数据挖掘与远程医疗中的深度应用，患者电子健康记录、生物特征数据（如人脸、指纹、基因序列）、诊疗行为数据等隐私信息的规模呈指数级增长，且数据流转场景愈发复杂。本文聚焦隐私保护技术的实际应用逻辑，从数据全生命周期视角，分析数据采集、传输、存储、使用环节的核心技术措施，结合匿名化处理、访问控制与区块链存证等技术的实践案例，提出技术融合应用的优化方向，为HIIS隐私保护体系构建提供技术参考。

**关键词**

医院智能信息系统；患者隐私保护；数据全生命周期；匿名化；访问控制

## 1 引言

本文聚焦隐私保护技术在 HIIS 场景中的实际应用逻辑，摒弃“技术堆砌”的论述模式，以“数据全生命周期”为核心框架，系统分析数据采集、传输、存储、使用四大关键环节的核心技术措施：在采集环节重点探讨如何通过技术手段实现“数据最小化采集”与“源头隐私保护”；在传输环节聚焦动态加密与异常行为拦截技术的协同应用；在存储环节深入剖析分布式加密与不可篡改存证技术的实践路径；在使用环节着重研究“数据可用不可见”技术如何平衡隐私安全与智能应用需求。同时，结合医院匿名化处理患者数据用于 AI 模型训练、省级医疗平台基于访问控制实现分级授权、互联网医院采用区块链存证追溯数据流转轨迹等，提炼技术落地过程中的关键经验与痛点问题，并进一步提出“多技术融合应用”的优化方向，最终为 HIIS 隐私保护体系的标准化构建、技术选型与落地实施提供可操作的技术参考，助力智慧医疗在安全合规的轨道上高质量发展。

【作者简介】郭靖（1986—），中国江苏张家港人，本科，高级工程师，从事医疗信息化研究。

## 2 数据采集环节：隐私保护的源头管控技术

数据采集作为 HIIS 获取患者信息的首要环节，其技术设计直接决定隐私保护的基础强度。此环节核心目标是在满足智能系统数据需求的前提下，最小化原始隐私信息的暴露范围，关键技术包括差分隐私采集与隐私增强型生物识别。

差分隐私采集技术通过在原始数据中注入可控噪声，实现“个体数据不可识别，群体特征可利用”。医院在构建临床决策支持系统时，对患者年龄、就诊频次等结构化数据采用拉普拉斯噪声机制，对医嘱文本等非结构化数据采用 k- 匿名文本扰动算法，使采集后的数据既保留“糖尿病患者用药偏好”等群体分析价值，又无法通过数据反向定位具体患者。该技术的核心优势在于不依赖数据脱敏后的“后验保护”，而是从采集源头阻断个体隐私的可识别性，尤

其适用于需要实时采集并上传的动态监测数据（如心电监护数据）。

隐私增强型生物识别技术则针对指纹、人脸等敏感生物特征数据的采集风险。传统生物识别直接存储原始特征模板，一旦模板泄露将导致患者永久隐私风险（生物特征不可再生）。某智慧医院采用“特征脱敏 + 本地存储”模式，在采集患者人脸数据时，通过本地终端将原始人脸图像转化为不可逆的特征哈希值，仅上传哈希值至 HIIS 用于身份验证，原始图像仅存储于患者本地就诊卡芯片中。同时，系统设置“活体检测 + 场景验证”双重采集校验，防止非法用户通过照片、视频伪造生物特征获取患者数据，从采集端杜绝生物特征隐私的泄露隐患。

## 3 数据传输环节：隐私保护的通道安全技术

HIIS 中患者数据需在终端设备、服务器与云端平台间频繁传输，传输通道的开放性使其成为隐私泄露的高风险环节。此环节的核心技术围绕“传输内容加密”与“传输行为防护”展开，确保数据在动态流转中不被窃取或篡改。

端到端加密技术是传输内容保护的核心手段。与传统的“传输层加密”不同，E2EE 实现“数据仅发送方与接收方可解密，传输中间节点仅存储加密密文”。某区域医疗协同平台采用基于 SM4 国密算法的 E2EE 方案，患者转诊数据从发起医院终端加密后，仅接收医院的授权终端可通过专属密钥解密，即使传输过程中数据被拦截，拦截方也无法获取明文信息。同时，系统引入“动态密钥协商机制”，每次数据传输前自动生成临时会话密钥，避免固定密钥长期使用导致的泄露风险，该技术使平台年度数据传输泄露事件发生率降至 0.03% 以下。

传输行为异常检测技术则针对非法传输行为（如未授权终端接入、批量数据导出）的识别与阻断。某医院基于深度学习构建传输行为特征模型，通过分析正常数据传输的“终端 IP、传输时段、数据量、访问频率”等特征，建立基线行为库。当系统检测到“非工作时段从外部 IP 批量下载患者 EHR”“同一终端短时间内跨科室访问数百条非接诊患者数据”等异常行为时，会自动触发传输阻断，并向管理员发送告警信息。该技术结合实时流量分析与历史行为比对，使非法传输行为的识别响应时间控制在 5 秒内，误判率低于 1.2%，有效遏制了内部人员违规传输隐私数据的行为。

## 4 数据存储环节：隐私保护的静态安全技术

患者隐私数据在 HIIS 中多以集中式或分布式方式存储，存储环节的安全直接决定隐私数据的长期安全性。此环节的技术重点在于“数据加密存储”与“数据访问追溯”，防止存储介质被破解或数据被非法篡改。

分布式加密存储技术通过将隐私数据拆分加密后存储于多个节点，避免集中式存储“一损俱损”的风险。某互联网医院的云存储系统采用“秘密共享 +AES-256 加密”方案，将患者 EHR 拆分为 5 个数据分片，每个分片通过不同密钥加密后存储于不同地域的云节点，仅当获取至少 3 个分片并集齐对应密钥时，才能还原完整数据。同时，系统对存储节点设置物理隔离与逻辑隔离双重防护，核心分片存储于医院本地服务器，非核心分片存储于第三方云平台，既降低本地存储压力，又通过“分片冗余 + 多密钥控制”提升存储安全性。该方案在第三方云平台发生数据泄露事件时，攻击者因无法获取完整分片与密钥，未能破解任何患者隐私数据。

区块链存证技术则解决了存储数据的“不可篡改性”与“访问追溯性”难题。某省级医疗数据平台将患者数据的“存储地址、访问记录、修改日志”等元数据上链存储，区块链的去中心化与哈希校验特性，使任何对元数据的篡改都会被全网节点识别并拒绝。当需要追溯某条患者数据的访问历史时，管理员可通过区块链查询到“谁在何时、通过何种终端、访问了哪些数据”的完整记录，且该记录无法被删除或篡改。此外，系统将数据加密密钥的生成与管理通过智能合约实现，密钥的分发与销毁均需满足预设条件（如多管理员签名），避免单一管理员滥用密钥访问存储数据。该技术使平台数据存储的篡改率降至 0，访问追溯成功率达到 100%。

## 5 数据使用环节：隐私保护的动态管控技术

数据使用是 HIIS 发挥智能价值的核心环节（如 AI 辅助诊断、科研数据分析），但也最易发生隐私滥用。此环节的技术核心是“细粒度访问控制”与“隐私计算”，在保障数据可用性的同时，限制隐私信息的过度暴露。

基于角色的细粒度访问控制技术突破传统“一刀切”的访问权限设置，实现“按需授权、最小权限”。某医院的 HIIS 将用户角色划分为“医生、护士、药师、科研人员”等 12 类，每类角色的访问权限细化至“数据字段级”。例如，门诊医生仅能访问其接诊患者的“主诉、检查结果、用药记录”等诊疗相关字段，无法访问“既往病史、遗传信息”等非必要隐私字段；科研人员仅能访问脱敏后的群体数据，且需通过伦理审批并签订数据使用协议后，才能获取临时访问权限。同时，系统设置“权限动态调整机制”，当医生接诊结束或科研项目结题后，其对应的访问权限自动失效，避免权限长期闲置导致的风险。该技术使医院数据越权访问事件减少 82%，同时未影响正常诊疗与科研工作的效率。

隐私计算技术则实现“数据可用不可见”，解决智能系统对原始隐私数据的依赖问题。某医院在构建 AI 影像诊断系统时，采用联邦学习技术，将训练数据分散存储于各科室终端，AI 模型仅在本地终端进行参数训练，仅将训练后的模型参数上传至中心服务器进行聚合。整个过程中，中心服务器与其他科室均无法获取原始影像数据，却能通过参数聚合提升 AI 模型的诊断准确率。此外，系统对需要跨科室协同分析的数据采用“同态加密”技术，支持在加密状态下直接进

行数据运算（如病灶区域面积计算、影像特征比对），运算结果解密后仅对授权用户可见。该技术使 AI 模型在训练过程中未产生任何原始影像数据的泄露，同时模型诊断准确率达到 94.6%，与使用原始数据训练的模型准确率仅相差 1.2%。

## 6 技术融合应用的优化方向

单一技术难以覆盖 HIIS 中患者隐私保护的全场景需求，技术融合成为提升保护效果的关键趋势。未来可从三个方向推进技术协同：

### 6.1 “差分隐私 + 联邦学习”的融合

强化跨域协作中的隐私屏障，跨院 AI 模型联合训练是 HIIS 发挥数据价值的重要场景，但传统联邦学习仅能避免原始数据传输，攻击者仍可通过“模型参数反演攻击”，从上传的梯度参数中推导出患者的敏感信息。将差分隐私技术与联邦学习深度融合，在本地训练层，各参与医院对模型训练过程中产生的中间梯度数据注入可控的拉普拉斯或高斯噪声，确保单机构输出的参数不携带个体隐私信息。在参数聚合层，中心服务器对接收的多机构噪声参数进行“联邦平均”时，进一步通过“隐私预算分配机制”动态调整噪声强度对肿瘤诊疗、基因测序等高度敏感数据设置更高隐私预算，对常规体检指标等低敏感数据设置较低隐私预算，在保护隐私的同时最大化保留参数的有效信息。

### 6.2 “区块链 + 访问控制”的融合

首先在区块链上部署基于角色的访问控制智能合约，将用户角色、数据类型、访问权限等规则写入合约，权限的授予需满足“多签审批”条件，如科研人员申请访问脱敏数据，需同时获得科室主任、伦理委员会、信息科三方数字签名，合约验证通过后自动开放权限；其次，所有权限操作均实时上链存证，生成不可篡改的操作日志，日志包含“操作人、操作时间、数据标识、权限范围”等关键信息，管理员可通过区块链浏览器随时追溯权限流转轨迹，一旦发现异常操作，可触发合约自动冻结相关账户。

### 6.3 “生物识别 + 动态密钥”的融合

静态密钥长期使用易被破解，导致加密数据面临安全隐患。“生物识别 + 动态密钥”的融合技术可构建“多因子、动态化”的身份认证体系：一方面，将患者或医护人员的生物特征（人脸、指纹、虹膜）作为“身份锚点”，通过本地终端的生物识别模块进行实时验证，避免账号密码冒用；另一方面，将生物识别结果与终端设备信息绑定，作为动态密钥的生成因子，每次发起数据访问请求时，系统自动结合“生物特征验证结果 + 设备动态信息”生成一次性临时密钥，密钥有效期仅为当前访问会话，会话结束后密钥自动失效，且不同终端生成的密钥互不通用。若 PDA 丢失，攻击者因无法通过指纹验证，且动态密钥随会话失效，无法获取任何隐私信息。该技术使医院身份冒用导致的隐私泄露事件下降 92%，显著提升身份认证的安全性。

## 7 结语

患者隐私保护是医院智能信息系统健康发展的核心前提，其技术体系需覆盖数据采集、传输、存储、使用的全生命周期。从源头的差分隐私采集，到传输中的端到端加密，再到存储中的区块链存证与使用中的隐私计算，各项技术的应用需紧密结合 HIIS 的业务场景，实现“安全”与“可用”的协同。未来，随着 5G、AI 大模型等技术在医疗领域的深入应用，患者隐私保护技术将面临新的挑战，需持续推进技术创新与融合，构建动态、自适应的隐私保护体系，为智慧医疗的发展筑牢隐私安全屏障。

## 参考文献

[1] 标准数字化热点技术识别及演变分析研究. 李想;黄佳;姚启明.标准科学,2025(01)

[2] 医院系统安全管理方法[P]. 谭新星;杨璨;黄青松.中理检验有限公司.2025

[3] 生成式人工智能的企业应用、赋能效应与劳动场重塑. 何小钢;毛莘娅.企业经济,2025(09)

[4] 医疗控制系统安全漏洞问题防护策略研究. 刘旭林.2025中国建筑经济研讨会论文集（上册）,2025（06）

[5] 医院信息系统中的网络安全与管理[J]. 王冠男.信息与电脑(理论版),2020(14)

[6] 网络环境下医院信息系统数据安全保障体系构建探讨[J]. 赖胜明.通讯世界,2019(07)

[7] 浅谈医院信息系统的网络安全管理与维护[J]. 李文钰.数字技术与应用,2023(04)

[8] 互联网+联合安全管理对医院急诊内科护理质量及信息系统安全性的影响[J]. 王云霞;李达;谈婷.齐鲁护理杂志,2024(13)

[9] 医院信息系统的安全冗余设计与应用[J]. 刘朋;刘晓琴.信息通信,2020(12)