医院信息化数据安全防护实践研究

孙浩琳
中国人民解放军西部战区空军医院　四川 成都　610000

摘　要　随着医院线上服务、医保结算、影像调阅和临床业务协同不断深入，医疗数据在多系统与多终端之间持续流转，数据安全已成为医院信息化建设中的日常管理事项。患者身份信息、诊疗记录、处方数据、医保结算信息和影像资料既涉及隐私保护，也关系诊疗业务连续运行。本文结合医院信息化建设实践，分析多业务系统协同、患者诊疗信息管理和重要业务系统运行中的安全风险，梳理防统方系统访问监管、等级保护测评整改及平台运行保障措施，并从数据分级分类、账号权限审计和运维应急管理方面提出完善路径，使安全要求融入系统建设与日常运维。

关键词　医院信息化；数据安全；等级保护；防统方系统；运维管理

Research on Data Security Protection Practices in Hospital Informatization

Sun Haolin
Western Theater Command Air Force Hospital of the Chinese People's Liberation Army, Chengdu 610000, Sichuan Province, China

Abstract　With the continuous deepening of hospital online services, medical insurance settlement, image retrieval, and clinical business collaboration, medical data continuously flows among multiple systems and terminals, and data security has become a daily management issue in hospital informatization construction. Patient identity information, diagnosis and treatment records, prescription data, medical insurance settlement information, and imaging materials involve both privacy protection and the continuous operation of diagnosis and treatment services. Based on the practice of hospital informatization construction, this paper analyzes security risks in multi-business system collaboration, patient diagnosis and treatment information management, and the operation of important business systems, reviews access supervision of the anti-prescription-statistics system, rectification of classified protection evaluation, and platform operation guarantee measures, and proposes improvement paths from the aspects of data classification and grading, account permission auditing, and operation and maintenance emergency management, so as to integrate security requirements into system construction and daily operation and maintenance.

Key words　Hospital Informatization; Data Security; Classified Protection; Anti-Prescription-Statistics System; Operation and Maintenance Management

医院信息化建设已由单项业务应用逐渐转向多平台协同运行。线上挂号缴费、报告查询、医保移动支付和医学影像存档与通信系统（picture archiving and communication system，PACS）影像调阅改变了部分传统服务流程，也使患者身份信息、诊疗记录、处方数据、费用信息和影像资料进入更多业务节点。全国医院数据安全调查显示，医院数据安全建设已涉及法规认知、制度安排、系统功能和分级评估等多个方面[1]。实际运行中，接口开放范围、账号权限配置、访问日志完整性以及基础平台稳定性相互关联，任一环节处置不当都可能影响患者隐私或诊疗业务连续性[2]。本文从数据流转、隐私管理和业务运行识别风险，进而考察安全要求如何贯穿访问监管、合规整改、平台保障及日常管理。

1　医院信息化数据安全风险识别

1.1　多业务系统协同下的数据流转风险

医院挂号、缴费、检查、报告查询、医保结算和影像调阅已形成跨系统协同流程。医院信息系统（hospital information system，HIS）、PACS、医保接口、线上服务平台和移动支付应用持续交换患者身份、费用、诊疗及影像信息。业务链条延伸后，数据经过的系统与终端随之增加。接口调用范围过宽，账号权限与岗位不匹配，或者终端身份校验不严，都可能使数据超出原定业务边界。信息部门在保障业务可用的同时，还需掌握数据从何处产生、流向何处以及由哪些人员调用，否则系统互联越深入，访问边界越难控制。

这类风险通常隐藏在正常业务流量中，并不一定表现为故

障或攻击。不同系统建设时间和技术架构存在差异，权限模型、日志格式及接口规则难以保持完全一致，后续业务调整还可能扩大原有开放范围。医院信息化系统网络安全防护实践表明，系统漏洞与网络入侵需要同制度管理同步处置[3]。新增接口或调整协同流程时，应同步核验数据项、调用对象、访问频次和日志记录方式，并对长期未使用接口进行清理，保留变更记录。持续维护数据流转边界，可减少因业务便利形成的无序开放。

1.2 患者诊疗信息管理中的隐私风险

患者诊疗信息兼具业务用途与隐私属性。姓名、证件号码、联系方式、就诊记录、检查结果、处方、医保结算和影像资料等，需由相应岗位在诊疗中使用，但访问范围不应超过工作实际需要。处方和用药数据还关系到医疗行为管理，一旦出现脱离诊疗目的的集中查询、违规统计或数据导出，不仅增加隐私泄露风险，也可能干扰医院正常管理[4]。此类行为常借助已有账号和常规功能完成，前台业务仍可正常运行，因而更易长期存在，也不易在常规故障处理中被发现。

内部访问风险与账号管理密切相关。人员转岗后权限未及时收回、临时授权超期或多人共用账号，都会削弱访问行为与具体责任的对应关系。系统若只保留登录信息，缺少查询对象、操作内容和时间记录，异常发生后也难以还原过程。医院应将实名账号、岗位授权和敏感操作留痕纳入诊疗数据管理，防统方系统则针对处方及用药数据持续监测异常访问。管理人员结合日志和业务背景复核，既能避免单靠规则误判，也能提高敏感数据使用的可追溯性。

1.3 核心系统运行中的业务连续风险

医院数据安全还包含数据可用和业务连续。HIS、PACS、医保结算以及报告查询系统与门诊、住院和医技业务紧密相连，一旦系统中断或数据无法正常调用，挂号收费、检查申请、报告查看和医保结算都会受到影响。备份任务长期失败、存储空间不足、服务器资源紧张等问题，早期可能只表现为响应变慢，却会在业务高峰或设备故障时放大影响。信息部门若只在故障发生后处理，缺少容量监测和恢复验证，很难判断业务能够在多长时间内恢复到可用状态，也难以及时评估故障可能波及的业务范围。

PACS集中保存计算机断层扫描（computed tomography，CT）、磁共振、超声和病理等影像资料，数据量大且调用频繁，对存储容量、访问效率和备份可靠性要求较高。虚拟化平台承载多套业务系统后，计算与存储资源能够统一调度，但资源竞争或平台故障也可能同时影响多个应用[5]。医院日常运维因此需要覆盖服务器、存储设备、网络链路、机房环境和备份任务，并对重要系统设置容量与运行状态检查。将基础设施状态与临床业务需求对应起来，可降低平台异常向诊疗流程扩散的概率，并缩短恢复等待时间。

2 医院信息化数据安全防护实践

2.1 基于防统方系统的访问监管实践

防统方系统将处方、用药统计等敏感数据访问纳入持续监管，使管理方式由人工抽查转为按操作记录核查。系统记录处方查询、用药统计、患者信息调取等行为，依据访问频次、查询范围和岗位权限发现异常；对短时间集中查询、跨科室访问或超范围统计，管理人员可依据日志及时核验。其重点不在增加审批环节，而在让敏感数据访问留下完整轨迹，便于事后还原访问主体、时间、对象和操作内容，也为权限调整提供依据。系统监管效果还取决于权限配置与人工复核。不同岗位对处方及用药数据需求不同，权限应随职责变化及时调整，避免长期保留宽泛访问范围；告警规则需结合业务环境判断，部分岗位在特定时期确有集中查询需求，应结合申请记录核实。医院可将防统方日志与权限复核结合，对重复异常访问分析原因，再调整权限或规则并持续复核。技术监测与管理核查配合后，敏感数据访问才能由事后发现转为日常约束。

2.2 基于等级保护测评的合规整改实践

等级保护测评为医院信息系统安全检查提供了较稳定的依据。医院系统数量多，网络区域、服务器、数据库和应用之间关系复杂，仅靠日常故障处理难以发现配置和管理隐患。等级保护覆盖安全目标、建设实施和测评验证，医院可据此检查网络边界、主机配置、账号权限、日志审计和数据备份。测评中发现的问题若仅用于完成材料，整改价值有限；只有对应到具体系统和责任岗位，合规要求才能转化为日常管理动作，后续运行也可持续检查整改是否有效。

整改需围绕实际风险展开。网络访问边界应检查重要业务区与办公区之间的访问关系，减少无业务需求的开放；服务器和数据库需核查账号口令、补丁状态及权限设置；应用系统应保证身份认证和敏感操作记录完整；备份任务不仅要查看执行结果，还要验证恢复过程是否可用。整改结束后，相关要求应进入巡检清单和系统变更流程，避免测评结束后配置逐渐回到原状。通过测评发现问题、完成整改并在运行中复核，可将阶段性检查转化为持续性的日常安全管理。

2.3 基于平台建设的运行保障实践

PACS和虚拟化平台承担着医院重要业务数据的存储与运

行任务，平台建设不仅涉及性能，也关系数据可用性和系统连续运行。影像系统上线后，CT、磁共振、超声和病理等影像资料由分散流转转为集中存储与在线调阅，临床使用更加便捷，同时也带来更高的存储占用和访问压力。医院需要同步关注影像调阅权限、存储空间、备份执行情况以及系统响应状态，防止容量不足或设备异常影响诊疗使用。医院网络安全协同防御实践也将业务可视和威胁监测纳入运行管理。

虚拟化平台扩容后，多套业务系统共享计算和存储资源，资源配置更加集中，故障影响范围也可能随之扩大。信息部门需要持续监测虚拟机负载、存储空间、宿主机状态和备份告警，并结合系统业务量调整资源。日常值班、主备机房巡检、网络故障排查和设备维护，应与平台监测结果相互印证。当运行指标出现持续异常时，应在业务受影响前安排扩容或检修。平台建设与日常运维衔接起来，还应保留资源调整和故障处置记录，使数据安全从系统上线时的配置要求延伸到长期运行过程，并便于后续复核。

3 医院信息化数据安全优化机制

3.1 建立数据分级分类管理机制

医院数据类型多样，统一保护易致管理失衡。患者身份、诊疗、处方、医保结算和影像资料需严格访问控制；系统日志、设备台账和运维记录则重在留存追溯。分级分类旨在明确重点保护对象、可用岗位及流转场景，为权限和审计划定边界。分类结果应进入业务流程。诊疗数据重点控制查询、修改和导出；处方与医保数据侧重统计权限和使用目的；影像资料兼顾调阅、存储与备份恢复；日志和运维记录应完整可检索。医院可在新系统上线、接口调整、权限审批和日常巡检时同步核对类别，及时修订。资源有限时，优先覆盖敏感度高且使用频繁的数据。

3.2 完善账号权限动态审计机制

账号权限连接人员岗位与系统数据，需持续维护。医生、护士、医技、收费、医保和信息运维人员职责不同，访问范围各异。若开通缺审批、转岗未调整，权限会逐渐叠加。医院可按实名账号和最小授权原则配置，由科室与信息部门共同确认需求，使权限有据可查。

权限不能开通后长期不变。新员工入职明确范围，转岗重新核定，离岗及时停用，临时权限设有效期。患者信息查询、处方统计、影像调阅、报告下载和医保审核等敏感操作应保留日志并定期抽查。审计既追查异常，也发现职责变化和权限偏差。长期未用或频繁触发异常的账号应及时核查调整。

3.3 健全运维巡检应急响应机制

数据安全需落实到每日运维。医院运行环境包括服务器、存储、网络、数据库、虚拟化平台和机房设施，任何异常都可能影响数据访问。信息部门可建立固定巡检，检查服务器负载、存储空间、数据库备份、网络状态、机房环境和重要系统日志。巡检记录不能只登记“正常”或“异常”，还应关注容量变化、重复告警和运行趋势，以便在临床业务受影响前安排扩容、检修或调整，并判断同类异常是否反复出现。

应急处置与巡检需形成闭环管理。针对系统故障、网络中断、数据访问异常和备份失败等情况，应明确发现、上报、研判、处置、恢复及复盘责任。故障时优先维持挂号收费、诊疗、检查报告和医保结算等重要业务，再按范围恢复其他系统。恢复后核对数据完整性并分析原因，将问题转入配置调整、制度修订或后续演练，从而积累可复用经验，逐步修正巡检重点和应急预案。

4 结束语

医院信息化建设扩大了医疗数据流转范围，也使安全管理由单个系统防护转向业务流程与运行环境管理。多系统协同需要控制接口和访问边界，患者诊疗信息使用需要保留可追溯记录，HIS、PACS等重要系统兼顾数据可用和业务连续。防统方系统可加强敏感访问监管，等级保护测评有助于发现配置与管理问题，PACS和虚拟化平台运行保障关系数据长期可用。医院应将分级分类、权限审计、备份恢复、巡检和应急处置纳入日常工作，使安全措施随业务变化调整，在保护患者信息的同时维持诊疗业务稳定运行。

参考文献

[1]郑攀,刘华,琚文胜,等.我国医院数据安全现状调查分析[J].医学信息学杂志,2024,45(5):71-75.

[2]解春生.医院信息化系统中的网络安全防护策略分析[J].集成电路应用,2024,41(12):350-351.

[3]伍毅强.医院信息系统信息安全等级保护分析[J].网络安全技术与应用,2023(12):120-122.

[4]曹晓均,翟志斌.医院网络安全协同联动防御体系建设实践[J].中国医疗设备,2024,39(12):64-70.

[5]吴震天,夏逸舜,莫远明,等.医院数据资产安全治理体系的建设研究[J].中国数字医学,2025,20(4):21-28.

（本文编辑 杜宇琪）