基于全域管控的防统方体系建设方案及应用*

郑云肆　吴晓芬

（上海市同济医院信息处　上海 200065）

〔摘要〕　**目的/意义** 通过构建防统方体系，提高防统方能力，更有效地保护患者的数据安全。**方法/过程** 借助网络准入控制、数据库审计、资源监控平台等信息安全设备，优化原有的防统方系统算法，结合移动端综合平台，实现全方位的防统方体系建设，线上审核归档。**结果/结论** 建设更为完善的防统方体系，为数据安全管理部门及纪检部门提供更及时高效、定位清晰的防治手段。

〔关键词〕　纪检监察；防统方系统；安全设备；数据安全；全域管控

〔中图分类号〕R－058　　〔文献标识码〕A　　〔DOI〕10.3969/j.issn.1673－6036.2023.11.016

Construction Scheme and Application of the Pharmaceutical Rebate Prevention System Based on Global Control

ZHENG Yunlu, *WU Xiaofen*

Shanghai Tongji Hospital Information Office, *Shanghai 200065*, *China*

〔**Abstract**〕　**Purpose/Significance** Through the establishment of the pharmaceutical rebate prevention system, the capacity of prevention of pharmaceutical rebate can be improved, and the data security of patients can be protected more effectively. **Method/Process** With the help of information security equipments such as network access control, database audit, and resource monitoring platform, the algorithm of the original pharmaceutical rebate prevention system is optimized, and the comprehensive mobile terminal platform is combined to achieve a full range of pharmaceutical rebate prevention system and online audit and archiving. **Result/Conclusion** A more comprehensive defense system is built, and the system provides a more timely and efficient prevention and control means with clearer positioning for data security management departments and discipline inspection departments.

〔**Keywords**〕　discipline inspection and supervision; the pharmaceutical rebate prevention system; safety equipment; data security; global control

1　引言

为贯彻落实《关于加强医疗卫生机构统方管理的规定》（国卫纠发〔2014〕1号）、《关于印发医疗机构工作人员廉洁从业九项准则的通知》（国卫医发〔2021〕37号）要求，进一步加强行风建设，严禁不正当商业目的统方。医院防治非法统方行为手段不能局限于技术人员职业道德约束和简单的平台监控，数据安全问题迫在眉睫。归纳总结原防统

〔修回日期〕　2023－05－30

〔作者简介〕　郑云肆，工程师，发表论文10篇；通信作者：吴晓芬，高级工程师。

〔基金项目〕　上海市“科技创新行动计划”技术标准项目（项目编号：22DZ2203900）；2022年申康“三年行动”研究型医师创新转化能力培训项目（项目编号：SHDC2022CRT004）。

方系统的问题，优化防统方体系，借助已有防统方系统，结合数据库审计[1]、准入系统、运维监控平台等安全设备，依照事前防范、事中控制、事后追溯的原则，建设全域管控、多层次安全防御体系，增强统方实时告警与事后溯源、分析、审计能力，加大医院对非法统方行为的打击力度，保护患者隐私。

2 原防统方系统方案的问题

2.1 模糊查询难发现

测试过程中发现，系统对全库/表查询、下载等大批量、频繁操作[2]这些常见的疑似统方行为，可以通过发送短信或页面弹窗的形式报告给防统方管理员。但对于故意采用模糊查询条件，查询后再二次筛选或拼装的行为，系统给出的风险判断等级较低，一般会被防统方管理员忽略，存在统方风险。

2.2 追溯难

防统方系统支持及时保留统方操作痕迹，再现统方结果，形成防统方监测报告，留存异常日志。由于多人共用一台电脑，仅靠 IP 无法准确定位，需借助摄像等操作，供事后追溯。

2.3 滞后性

原统方系统采用旁路镜像的模式搭建[3]，其拓扑结构，见图 1。这种事后干预方式不会影响正常业务运行，但是响应相对滞后，需要依靠防统方管理员及时追溯，从大量语句中筛选疑似语句。

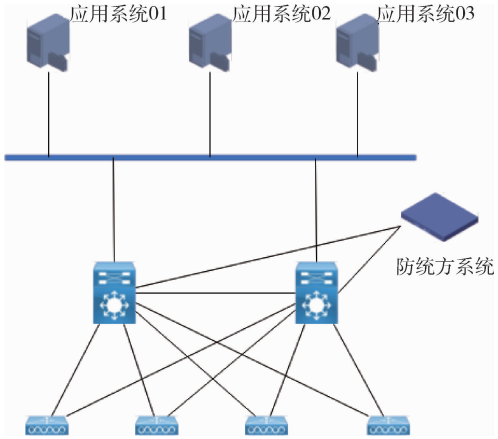

图 1 防统方系统接入拓扑结构

3 全域管控防统方体系设计

目前医院信息化建设发展迅速，各业务系统关联性越来越复杂，核心数据泄密的隐患也越来越突出[4]，数据安全不能单单依靠一套系统，全域管控防统方体系是指防统方系统与数据库审计、准入系统、运维监控平台、网络资源监控平台等安全设备及监控平台交叉合作，提升综合管理效率，达到统方实时预警与事后溯源、及时定位、协助分析、结果验证并举的效果。

3.1 多维度、全方位、全范围监控阻拦

本方案体系主要从 4 大场景展开：数据安全威胁监测场景、数据安全威胁处置场景、保障业务连续性场景、日常运维场景。结合医院安全设备，形成多维度、全方位、全范围的数据安全体系，交错验证终端准入，上网行为管理设备限制可连接设备，结合网络策略阻断访问。

3.1.1 数据安全威胁监测场景 监测维护人员的操作行为，详细记录其操作内容，以保障重要数据安全为出发点，完整记录、分析对关键数据的查询、变更、删除等操作，为统方行为的溯源提供助力[5-6]。

3.1.2 数据安全威胁处置场景 当数据被大量复制，甚至范围扩展到整个数据库时，会被资源监控平台记录，即时触发报警，工程师联动桌面管理软件智能阻断数据访问，通过桌面系统录屏、锁屏、阻断等，极大提高了系统取证及控制能力。防统方系统、数据库审计通过对医院核心数据的实时监控，使管理者能够及时掌握数据的应用情况，及时发现用户的使用问题，纠正存在的安全隐患。

3.1.3 保障业务连续性场景 在医院业务系统全方位打通、高强度融合的背景下，网络安全已经从以系统为中心逐渐转向以数据为中心，传统的基于清晰边界隔离的围栏式静态安全保护方法已经无法满足数据流动下的动态安全防护体系化需求。基于全域管控防统方体系的准入系统、防统方系统等安全设备，结合网管平台、网络资源监控平台，做到

事中记录、实时防护，保障业务连续性。

3.1.4 日常运维场景 日常运维管理中，对于涉及患者敏感信息的需求，由信息安全小组介入，以最小够用原则评估业务的必要性[7]。对于借助数据平台的项目，例如专病库、科研管理平台等，则配合脱敏系统对接数据，层层设置对应的用户权限[8]。当下载数据用于科研项目时，由科研员提交 OA 申请，经科主任、临床研究中心管理员审核，待申请通过后，由管理员下载并保留操作痕迹，以备审查。对于需对接的系统，经信息安全小组评估通过后，定期检查数据平台接入内容，审查所有接口的调用记录，及时清理舍弃的接口，减少数据泄露的可能，见图 2。多安全设备相互协作，辅助保障数据安全。多平台验证分析结果，形成闭环管理。

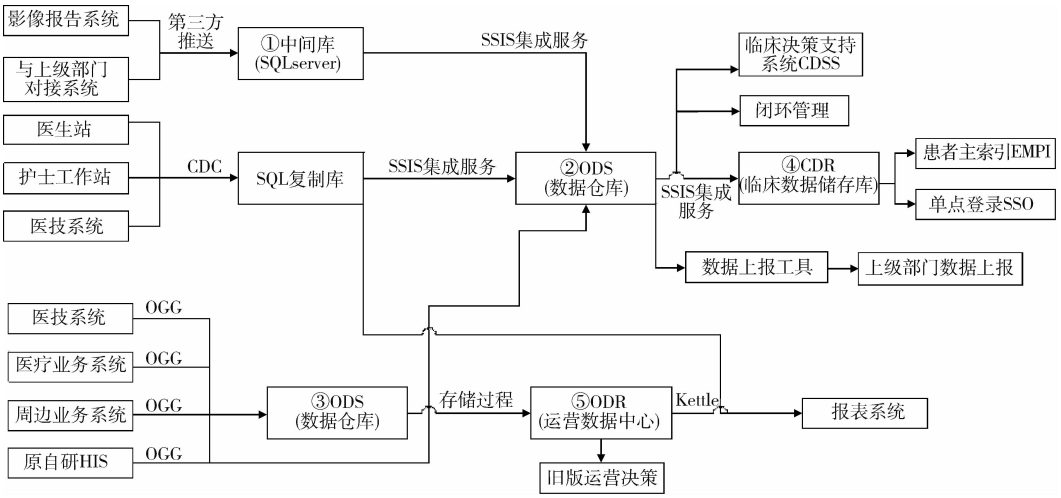

图 2 接口调用记录

3.2 基于自学习的防统方系统算法

整合线性规划、非线性规划等算法，加上传统的经验法，更快定位疑似行为，应用独特的业务活动分析技术，可以区分真正的攻击与无害的用户行为变化，特有的阻断技术为数据提供实时保护，防止利用数据库信息进行“统方”、医患数据外泄、擅自篡改医院和患者信息数据等问题。系统采用加密传输机制，避免可能存在的嗅探行为，保证安全[3,9]。

系统内置防统方知识库，对于可疑筛选操作，定期进行人工辅助识别，并将结果反馈给防统方系统，供其自动学习。经过一段时间的学习，防统方结果会更加准确。同时还设有实时更新的合理用药、供应链管理、耗材等知识库。

3.3 基于移动端联动处理

传统架构下的提醒功能通过平台弹框和短信提示，随着业务拓展，业务与数据量成倍增长，短信成本较高，且无法查看详细可疑语句，倒查追溯困难。结合医院自研的综合平台和钉钉平台，可大幅减少运营成本，防统方管理员也能更精准、便捷定位。借助综合管理平台定期分析敏感数据，防统方管理员可在平台上分配分析任务，分析结果支持多人复核，在平台上选择审核部门进行逐层上报。审核结果生成电子档案，长期保留供下载或者打印存档，也可解决纸质档案不易保存的问题。

4 应用效果及社会效益

4.1 防止管理员权限滥用

管理员根据工作岗位需要，依据“最小化配置”原则配置权限。安全设备（如数据库审计系统）记录所有用户数据库操作，审计员可以审计用户行为，借助设备还原出原操作记录，形成闭环管理。能够提供多角度、可追溯的制度与响应机制，防止管理员权限滥用。

4.2 降低维护人员窃取数据风险

现有医疗业务系统依赖大量运维人员，运维人员可以直接接触核心数据，且配有大部分系统的权限。对于运维人员，除了定期培训、明确网络安全责任和签署保密协议外，还要规范外部准入行为，做好进出身份核实、实名登记与背景审查、在运维专区设置摄像头、配置专属运维电脑等，达到数据“可以使用，无法带走”的运维管理效果。

4.3 保护重要数据安全

保护患者数据安全是智慧医疗的生命线，要像对待医疗安全一样对待网络安全。作为非传统安全的重要组成部分，网络安全是稳步推进数字化转型的前提和基础。以保障患者的诊疗数据安全为目标，事前防范、事中控制、事后追溯，完整记录和分析对关键数据的变更，促进行风建设，提升医院形象。

5 结语

构建基于全域管控的防统方体系，能够有效提升网络管理、网络准入控制、数据库防火墙防范和专用防统方系统等技术措施的效果；优化原防统方系统算法，提高全域防统方能力；借助移动端综合平台、线上审核归档等功能，使行风管理员工作更高效，为数据安全管理部门及纪检部门提供了一种有效的执法与监控手段。

参考文献

1 王俊新，李伟，尚明伟，等．基于医院数据库审计的防统方系统思考与应用［J］．中国数字医学，2019，14（7）：109－111.
2 黄为．防统方管理在医院纪检监察工作中的运用研究［J］．办公室业务，2021（19）：56－57.
3 聂喆，王文文，刘同波．医院防统方解决方案的设计与实现［J］．中国数字医学，2020，15（12）：41－43.
4 葛伟. 面向业务的医疗云流量安全防护系统设计与实现［J］．中国数字医学，2022，17（12）：107－111.
5 朱卫红，吕艳，庞刚，等．防统方管理在医院纪检监察工作中的运用与探讨［J］．大众科技，2017，19（4）：115－116，121.
6 李享，殷海波，薛万刚，等．医院防统方系统建设实践［J］．中国医疗设备，2016，31（3）：96－98，73.
7 侯爽，李寅，许扬．基于等保2.0标准的互联网医疗系统三级等保测评实践探索［J］．中国数字医学，2022，17（3）：101－104.
8 臧璆，汪春亮．基于安全等级保护的医院网络安全优化方案实践［J］．医学信息学杂志，2022，43（3）：79－83.
9 王涛，万笛．医院信息系统防御勒索病毒的策略与实践［J］．中国数字医学，2022，17（8）：106－109.

（上接第62页）

根据具体实践不断完善，以更好地指导及规范中医药科技查新工作。

参考文献

1 李凤玲，杨坤杰．知识管理在中医药科技查新中的应用探索［J］．国际中医中药杂志，2011，33（10）：913－915.
2 杨坤杰，李凤玲．中医药科技查新的“中医特色”［J］．医学信息，2009，22（3）：320－321.
3 杜娟．查新结论的规范化模式探讨［J］．医学信息学杂志，2008，29（2）：59－62.
4 李海燕，孟凡红，杨坤杰，等．中医药科技查新技术规范［J］．中国中医药图书情报杂志，2023，47（3）：1－10.
5 全国信息与文献标准化技术委员会．科技查新技术规范：GB/T32003—2015［S］．北京：国家质量监督检验检疫总局，国家标准化管理委员会，2015.
6 袁学敏．科技查新新标准视角下专利查新与科技查新对比［J］．甘肃科技，2017，33（7）：71－73.
7 闫军堂，刘晓倩，邹慧琴，等．中医药科技查新的实践探讨与展望分析——以北京中医药大学教育部科技查新站为例［J］．中医药管理杂志，2018，26（23）：28－31.
8 李凤玲．如何确立中医药科技查新项目的查新点［J］．中国中医药信息杂志，2008，15（4）：107－108.
9 杜娟．查新报告零相关文献时对网上散在信息利用的探讨［J］．医学情报工作，2006，27（1）：60－62.