我国医院数据安全现状调查分析

郑 攀[1] 刘 华[2] 琚文胜[1] 陈 臣[1] 马 扬[3]

([1] 北京市卫生健康大数据与政策研究中心 北京 100034
[2] 中国医院协会信息管理专业委员会 北京 100027 [3] 北京数字认证股份有限公司 北京 100080)

〔摘要〕 **目的/意义** 通过调研和分析了解全国医疗行业数据安全现状，为监管部门、医院信息化从业人员、医院信息化厂商提供数据安全建设建议。**方法/过程** 面向全国医院信息技术部门负责人及数据安全建设、维护等相关管理人员开展医疗行业数据安全调查研究，内容包括对法律法规的了解程度以及医院数据安全建设现状、存在问题、系统功能、分级评估等方面，进而分析全国医疗行业数据安全现状。**结果/结论** 全国医院数据合规意识明显加强，绝大多数医院已具备一定的数据安全技术保障能力，但在数据安全与个人信息保护方面仍存在诸多不足。

〔关键词〕 医院信息化；数据安全；法律法规
〔中图分类号〕 R-058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2024.05.012

Investigation and Analysis of the Data Security Status of Hospitals in China

ZHENG Pan[1], LIU Hua[2], JU Wensheng[1], CHEN Chen[1], MA Yang[3]

[1] Beijing Municipal Health Big Data and Policy Research Center, Beijing 100034, China; [2] China Hospital Information Management Association, Beijing 100027, China; [3] Beijing Certificate Authority Co., Ltd., Beijing 100080, China

〔**Abstract**〕 **Purpose/Significance** To investigate and analyze the current situation of data security in the national medical industry, and to provide suggestions for data security construction for regulatory authorities, hospital informatization practitioners and hospital informatization manufacturers. **Method/Process** A survey and research on medical industry data security is conducted for the heads of hospital information technology departments and relevant management personnel in data security construction and maintenance nationwide. The content includes understanding of laws and regulations, as well as the current situation, existing problems, system functions, and hierarchical evaluation of hospital data security construction, in order to analyze the current situation of data security in the national medical industry. **Result/Conclusion** The awareness of data compliance in hospitals across the country has significantly strengthened, and the vast majority of hospitals have a certain level of data security technology support capabilities. However, there are still many shortcomings in data security and personal information protection.

〔**Keywords**〕 hospital informatization; data security; laws and regulations

1 引言

医疗行业性质特殊，是攻击者重点关注对象，常见攻击手段有勒索病毒[1]、APT 攻击、漏洞利用

〔修回日期〕 2023-12-18
〔作者简介〕 郑攀，高级工程师，发表论文 10 余篇；通信作者：琚文胜。

等，医院内部人员也是信息泄漏的重要来源[2]。在云计算、物联网、5G、人工智能等新技术的应用浪潮中，全新的数字医疗生态正在构建，单个医院医疗过程产生的数据量正从 TB 级向 PB 级跃进。医院数据通常包括患者的诊疗数据、影像报告数据、机构运营数据等，如果能精确收集并加以分析利用，将有助于医院临床业务、医院管理和患者满意度的提升，促进医院的高质量发展。医疗数据安全研究对于我国医疗行业的健康发展具有重要意义。目前我国医疗数据安全领域的研究热点为涉及电子病历、医学影像等的医疗数据隐私保护、医疗数据安全技术、医疗数据共享[3]等技术层面，缺乏对医院数据安全管理和技术现状的整体研究。因此，面向全国医院开展医疗行业数据安全现状调查研究，为监管部门、医院信息化从业人员、医院信息化厂商提供参考，以便更好地开展数据安全建设。

2 研究方法

2.1 调研方法

向全国二级及以上医院发放调研问卷，共计 769 家，回收 720 份有效问卷，覆盖全国 31 个省、自治区、直辖市，遍及全国 93.6% 的医院，研究结果具有代表性，可全面反映我国医院数据安全现状。

2.2 调研内容

调研全国二级及以上医院核心业务等级保护建设情况、网络安全建设投入与业务关联度、医院数据安全建设现状、存在的问题、系统功能、分级评估等。

2.3 问卷回收统计

经过查重和筛选，共回收 720 份有效问卷，回收有效率为 93.6%。有效问卷中，三级医院 399 家，占 55.42%，三级以下医院 321 家，占 44.58%。

2.4 分类统计

按照级别将医院分为三级医院和三级以下医院。

3 调研结果

3.1 医院情况

核心业务等级保护建设方面，三级医院有 82.46% 通过等保三级测评，三级以下医院通过等保二级测评的比例最高，为 28.04%。网络安全建设投入与业务关联度方面，电子病历应用分级评估等级与网络安全建设投入呈正相关关系。电子病历分级评价 4 级的医院中，安全建设投入 5% ~10%（含）的占比 41.18%；电子病历分级评价 5 级的医院中，安全建设投入 5% ~20%（含）的医院占比 56.09%。

3.2 医院数据安全与个人信息保护现状

3.2.1 数据安全政策整体认知程度 （1）相关法律学习。74.44% 的三级医院和 64.8% 的三级以下医院组织学习《数据安全法》《个人信息保护法》，三级以下医院学习力度不足。（2）内部数据保护制度建立情况。三级医院有近 6 成已建立数据安全制度和流程，三级以下医院超过 5 成建立了相关制度和流程。（3）数据安全建设进展。一半以上医院计划按照《数据安全法》《个人信息保护法》要求加强数据安全建设，三级医院和三级以下医院已经开展的比例分别为 37.09% 和 27.15%。

3.2.2 数据安全保障能力 （1）数据安全保护措施。目前三级医院使用最多的安全保护措施是数据库审计和具备勒索病毒查杀能力的杀毒软件，见表 1。（2）数据收集。“告知 - 同意原则”的落实方面，两类医院比例相当，七成以上医院按照《个人信息保护法》中的“告知 - 同意原则”要求向患者告知处理事项。未成年人个人信息保护方面，三级医院和三级以下医院按照《个人信息保护法》要求制定措施的数量相当，占比分别为 34.59% 和 34.58%。（3）数据传输。数据接口的风险中，两类医院已使用方案排名相同，占比排名前 3 位的是合并数据接口，减少暴露面，增加可管理性；明确管理责任边界；在重要数据共享时避免使用开放数据库视图等不安全的数据共享方式，封装为私有接

口，且具备身份验证等能力。（4）数据存储。三级医院和三级以下医院使用最多的存储方式是将数据存储在各信息系统的数据库（89.72% 和 86.6%）。（5）数据使用。三级医院在互联网医院开展的隐私保护机制集中在入侵防护检测、病毒检测和防护、身份认证方面；三级以下医院则集中在身份认证、病毒检测和防护、入侵防护检测方面。（6）数据提供。三级医院和三级以下医院面临的数据交换风险一致，依次是缺乏对敏感信息和个人隐私的数据保护（84.71% 和 74.45%），缺乏数据脱敏系统（79.95% 和 64.49%）；后两位分别为缺乏对原始数据的保护和缺乏对跨安全域、内外网、系统的数据传输安全。

3.2.3 数据安全与个人信息保护重难点 三级医院最担心的数据安全风险是勒索病毒（80.45%），三级以下医院最担心的是外部攻击导致数据丢失或损毁（66.36%），见图 1。两类医院面临问题基本相同，排前 3 位的分别是缺乏数据安全专业能力、缺乏资金支持、缺乏相关标准与指导。两类医院最希望得到的服务中排前两位的相同，但三级以下医院日常运维管理服务需求更突出。三级医院最紧迫开展的工作是数据分类分级，识别敏感数据需求紧迫；三级以下医院则是购买并实施数据安全产品。

表 1 医院现有数据安全保护措施

数据安全保护措施	三级医院（%）	三级以下医院（%）
数据库审计	84.96	39.25
具备勒索病毒查杀能力的杀毒软件	83.46	63.55
数据备份	81.95	65.73
数据库防火墙/网关	76.94	75.39
防统方	68.67	23.36
数据访问控制	63.91	45.48
数据脱敏	31.33	4.98
数据加密	28.32	22.43
数据防泄漏	23.31	8.41
零信任	6.27	3.43
暂未使用	0.75	2.49

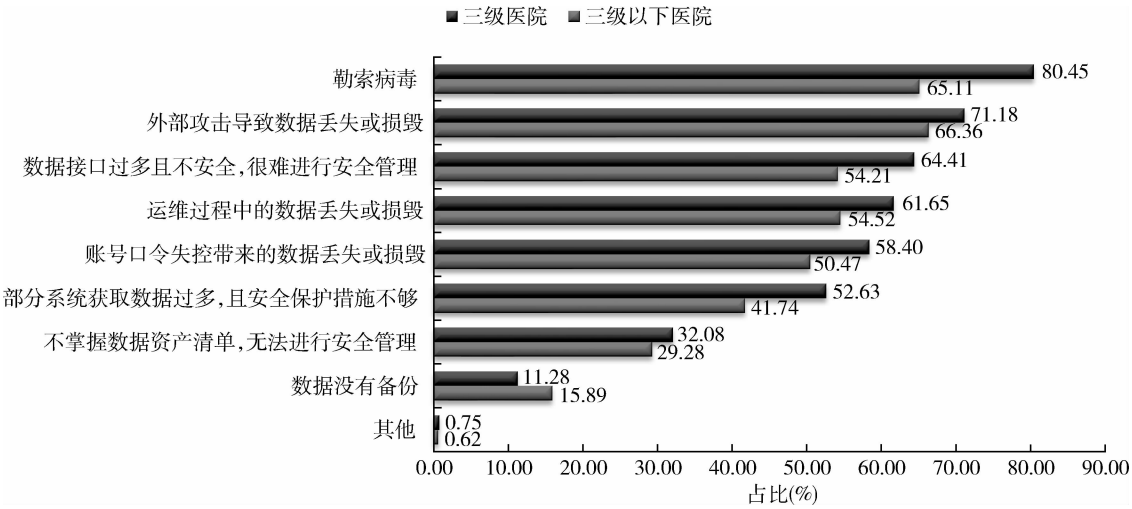

图 1 医院已经存在或最担心的数据安全风险

4 分析结论

4.1 医院数据合规意识明显加强，但有待进一步深入

当前医院对数据安全、隐私保护等相关法律法规的落实已取得一定进展，但仍存在政策宣贯不充分、数据安全意识不足等问题，应更进一步贯彻落实。有 70.14% 的医院已组织开展对《数据安全法》《个人信息保护法》的学习与宣贯，且 57.5% 的医院已对照法律要求调整及完善相应制度。在数据保护实操上，多数医院尚未正式开展院内数据安全保护建设工作，且未建立专门的数据安全与隐私保护管理监督机制。已按《数据安全法》《个人信息保护法》要求加强数据安全建设的医院仅有 32.64%。医院仍需进一步加强对数据安全与隐私保护的重视程度。

4.2 绝大多数医院已具备一定的数据安全技术保障能力

53.16% 的医院核心业务系统已满足网络安全等级保护三级要求，仅 1.53% 的医院未采取任何数据安全保障措施，其中三级医院仅占同级医院的 0.75%，绝大多数医院已采取数据安全保障措施且具备技术能力。《数据安全法》《个人信息保护法》均提出要对个人信息数据的收集、存储、使用、加工、传输、提供、公开等处理活动履行安全保护义务，开展医疗服务涉及的个人基本信息、病情信息等数据的处理。当前医院在数据生命周期各环节已采取部分保护措施。一是数据收集环节，70.56% 的医院按照《个人信息保护法》要求向患者事前告知，34.58% 的医院已建立未满 14 周岁未成年人隐私保护制度。二是数据传输环节，面对接口过多带来的安全风险，50% 以上的医院采用合并接口的方式减少传输过程中的数据泄漏风险。三是数据存储环节，75.25% 的医院通过定期安全检查保障医院数据库安全，55.28% 应用数据库运维的身份识别、运维审批、流程管理等监管措施。当面对外部攻击风险时，医院多采取对院内数据加强纵深防御、建设态势感知平台或安全监测平台等技术手段。四是数据使用环节，主要涉及的应用场景为互联网诊疗及临床科研。互联网诊疗依托开放的网络环境，易遭受外部非法入侵和木马病毒攻击；60% 以上的医院已采取病毒检测和防护、入侵防护检测应对个人隐私泄漏风险。临床科研等院内活动，由内部人员造成的隐私泄漏成为首要风险。60.97% 的医院通过设置访问权限严格把控隐私数据的可访问范围，50.97% 的医院与内部人员签订保密协议。五是数据提供环节，涉及与第三方合作的数据提供活动中，有 84.86% 以上的医院偏向于签订保密协议，其次是进行数据安全意识教育（46.94%）。

4.3 医院数据安全与个人信息保护工作仍存在诸多不足

当前医院安全建设的投入占信息化总投入的比例普遍较低，61.94% 的医院在网络安全与信息化的投入占比为 5%（含）以下，仅 8.06% 的医院投入 20% 以上的信息化费用用于网络安全。医院采取的数据安全保障措施仍停留在“等保 2.0”要求的维度，数据库防火墙/网关、数据备份、具备勒索病毒查杀能力的杀毒软件或终端管理软件、数据库审计、数据访问控制成为半数以上医院采取的数据安全保护措施。医院在数据安全保护工作中存在的 3 大困难依次是缺乏数据安全专业能力、缺乏资金支持、缺乏相关标准与指导。

鉴于医疗健康服务、公共卫生服务的特殊性，医院普遍对《个人信息保护法》提到的“个人敏感信息”的具体划分、“撤回同意”后的实际处理、“最小数据范围”的明确界定、“个人信息去标识化”的技术实施等待落实细节存在较大疑惑。

我国《网络安全法》《数据安全法》《个人信息保护法》为数字时代的网络安全、数据安全、个人信息权益保护提供基础制度保障。对其贯彻落实不应仅停留在等保建设层面，应技术手段与监管手段并重，在数据收集、传输、存储、使用、提供等环节保障其真实性、机密性、完整性和不可否认性。

5 建议

5.1 面向卫生主管部门

建议以《数据安全法》《个人信息保护法》为基础，结合卫生健康行业实际特点，主导制订卫生健康行业指导意见、实施细则等指导性文件，引导各医院建立并不断完善个人信息保护管理机制，明确个人信息行为规范及违规后果，为落实个人信息保护提供有效指引。建议将个人信息保护纳入各级医院绩效考核体系。由行业主管部门定期考核数据安全、个人信息保护落实情况，评估业务开展过程中流程操作的规范性，切实促进《数据安全法》《个人信息保护法》在卫生健康行业的贯彻执行。

5.2 面向各级医院

建议设立个人信息保护组织，制定医院内部个人信息保护合规制度，明确个人信息处理的管理人员及相应监管职责，开展内部合规培训，指导各部

门个人信息保护落实工作。在当前信息系统网络安全等级保护建设基础上，进一步加强自主可控、合法合规的技术手段应用，在收集、传输、存储、使用等环节保障健康医疗数据安全，采用身份认证、访问控制、数据加密、数据脱敏、电子签章[4]、手写签名[5]、个人信息匿名化等技术来防止数据恶意泄漏。

5.3 面向卫生健康信息化产业

建议厂商针对卫生健康行业新业态创新研发数据安全防护和数据安全密码应用产品，探索非对称加密、区块链[6]、全同态加密[7]等前沿技术的落地应用，满足健康医疗大数据时代对数据安全、隐私安全的需求。

6 结语

随着医疗数据日益成为国家重要的基础性战略资源，数据和隐私泄漏[8]风险频发。我国医疗数字化改革发展迅速，海量医疗数据经过不断聚合、流动[9]，价值迅速攀升，医疗数据一直是黑客的重点目标。因此，卫生健康行业须不断强化数据安全意识，结合行业特点，制定相关指导性文件，引导行业落实和完善数据安全管理机制[10]。在医院信息化建设中，利用多种措施和先进技术手段，加强数据安全保护，有效实施数据全生命周期安全管理，夯实信息化发展的安全底线。

利益声明：所有作者均声明不存在利益冲突。

参考文献

1 胡国强．从勒索病毒看网络信息安全的隐患与对策［J］．信息安全与技术，2018，9（1）：5－7，20.
2 何剑虎，周庆利．互联网环境下的医疗数据安全交换技术研究［J］．中国医疗设备，2013，28（4）：4.
3 郭鑫鑫．基于 CiteSpace 的医疗数据安全领域研究热点分析［J］．中国病案，2023，24（7）：42－45.
4 万以娴．电子签章法律问题研究［M］．北京：人民法院出版社，2001.
5 颜琬，郑建彬，周莉，等．基于在线手写签名的身份认证技术研究和展望［J］．电子技术应用，2004，30（9）：3.
6 李麟．基于区块链技术的医疗数据安全防护［J］．电子设计工程，2022，30（10）：62－65，70.
7 刘明洁，王安．全同态加密研究动态及其应用概述［J］．计算机研究与发展，2014，51（12）：2593－2603.
8 魏彩霞，李文娟．健康医疗大数据应用中患者隐私保护及对策研究［J］．网络安全技术与应用，2022（10）：64－67.
9 金山．面向医疗大数据的网络数据安全存储检索系统的设计及实验分析［J］．科学技术创新，2023（8）：96－99.
10 李静，张世红，王岳．区域健康医疗大数据中心数据安全管理机制研究［J］．中国数字医学，2020，15（12）：1－4.