CHIMA

医院数据安全调查报告

中国医院协会信息专业委员会 编

序言

本报告是中国医院协会信息专业委员会（CHIMA）首次针对医院数据安全状况进行调研的工作产出。调研的目的包括：一、为医院对标行业整体发展情况，提供测评标准，以便查缺补漏，完善安全防护工作措施；二、为行业行政部门进行政策设计和规划制订，提供监测和评估依据；三、为技术提供商进行产品开发和服务选择提供参考。

近年来，互联网、大数据、云计算、人工智能等技术加速创新，日益融入医院医疗和管理活动过程，医疗数据量快速增长，数据交换与共享需求快速释放，数据已经成为医院医疗服务提供的重要生产要素和运营保障的基础支撑。数字化、网络化、智能化的发展促进了医院医疗质量的提升和运行效率的改进，但同时带来了数据安全风险问题。

医疗机构中大量的患者个人数据和个人敏感数据，成为黑客关注的目标。国外有关调查表明，在2020年，多达34%的医疗机构遭受到勒索软件的攻击，其中65%的攻击是成功的，三分之一以上的单位为此支付了赎金。

为什么会出现这些不安全的问题？一是医院数据引来越来越多黑客的关注；二是物联网和移动APP的应用，网络安全的漏洞增加，对安全防护提出了新的挑战；三是医院安全防护能力的提升滞后于安全风险防范变化的要求。

尽管大家已经意识到医疗数据安全风险的严重性，但是医院数据安全事件时有发生，而且有越来越严重的趋势。医院数据安全成为典型的“灰犀牛事件”。但如何提升医院数据安全能力的思路和办法尚未健全，最终拖延导致了严重后果。

可以说，数据安全是医院信息化发展遇到的一个新难题。医院是数字密集型也是知识密集型单位，数据不仅是医疗管理与决策的要素资源，也是医疗业务协同的必要支撑，没有数据安全就没有医疗安全，也没有医院运营安全，这个道理已是大家的共识。为了做好医院数据安全工作，CHIMA组织专家对此问题开展深入研究工作，凝聚集体智慧，治愈医院数据安全这个“癌症顽疾”。

本报告中包括两部分调查内容。前期共收集医院数据安全工作相关问卷769份，有效问卷720份。后期，针对医院利用AI工具赋能数据安全的做法，收集了176家医院专项调查数据。

本报告的产出旨在能为医院数据安全建设工作带来收益。但是，本次调查没有采用抽样设计方法，因此结果不具备代表性。此外，本次调查的数据采集工作由调查对象网上自行录入，没有采取复核方式控制数据质量，特请读者注意。同时希望各位同仁对本报告中存在的问题和不足，提出意见和建议。

感谢参与编写本报告的各位专家，感谢杭州安恒信息技术股份有限公司对本次活动的支持，感谢为本次调查工作提供数据资料的各位医院领导和专家。

王才有

中国医院协会信息专业委员会主任委员

课题组织架构

- **课题顾问、主审：**

  王才有、薛万国、琚文胜

- **课题组组长：**

  北京市卫生健康大数据与政策研究中心 郑攀

  首都医科大学宣武医院 梁志刚

- **课题组成员：**

  中国医院协会信息专业委员会 朱丽艳、刘华

  北京市卫生健康大数据与政策研究中心 陈臣

  深圳市卫生健康发展研究和数据管理中心 郑静

  中国医学科学院阜外医院 韩作为

  陆军特色医学中心（重庆大坪医院） 黄昊

  中国人民解放军总医院 刘敏超

  浙江大学医学院附属邵逸夫医院 林辉

  中山大学附属第一医院 刘翰腾

  中山大学附属第五医院 马嘉潜

  中国医学科学院北京协和医院 孟晓阳

  香港中文大学（深圳）医院 庞勤

  珠海市人民医院 沙翔

  首都医科大学附属北京友谊医院 王力华

  首都医科大学附属北京朝阳医院 韦力

  深圳市第三人民医院 杨川川

  中山大学附属第七医院 郑子龙

  杭州安恒信息股份有限公司 刘博、段平霞、刘苏、程文博、杨长江、刘硕

  （以上排名不分先后）

感谢安恒信息对本次调研提供的支持

感谢各地方兄弟协会对本次调研提供的支持

目录
CONTENTS

调查研究背景

数据安全是我国信息化发展遇到的新挑战。当前，信息化已步入数字化、网络化和智能化的新阶段，数据无处不在、无时不有，已成为新的生产要素，在经济生产和社会活动中扮演着越来越重要的角色。与此同时，数据安全已成为事关国家安全与经济社会发展的重大问题，也是医院信息化发展面临的新挑战。

近年来，为了做好数据资源利用与安全防护工作，国家发布了《网络安全法》《数据安全法》和《个人信息保护法》等法规。这些法规分别从网络空间安全治理、数据交换共享防护以及个人信息保护责任等方面做出了规定，旨在统筹做好数据资源开发利用与安全防护这两件大事。

为了适应医院信息化发展对数据安全防护的需求，医疗行业行政部门也结合特定业务领域的发展现状，对数据安全工作提出了具体规范。

当前，医院数据安全建设面临着复杂的形势：法律层面有了高位合规约束，政策层面有了具体保护要求，但医院数据不安全事件仍频发，严重制约了医疗健康数据的有序流动和价值释放。

因此，深入了解当前医院数据安全防护的现状，分析其背后的制约因素与问题成因，对于加强和改进行业数据管理具有现实意义。

数据安全法规的新要求

随着我国数字经济时代的到来，数据作为新型生产要素和社会财富，正被广泛地分享、分析与利用。随之而来的个人隐私安全问题，也成为数字社会关注的焦点。为此，国家加快了数字经济领域的立法进程，先后发布《网络安全法》《数据安全法》《个人信息保护法》。这些法律不仅在制度层面为数据确权、开放、流通及交易提供了保障，也为数据安全及个人隐私保护构筑了坚实的法律屏障。

医疗健康领域是典型的数据密集型行业。医疗数据既包含患者的一般信息，也涉及高度敏感的个人隐私数据。这些数据不仅在不同医疗机构间流动，以支撑居民全生命周期的医疗服务，还在医院医疗、教学、科研、预防及管理等多方面发挥积极作用。医疗数据不仅是提供连续性医疗服务的基础，更是国家重要的基础性战略资源。

为统筹医疗数据的开发利用与安全防护，国家相关部门陆续出台了一系列政策文件与标准规范：

2020年12月14日，国家市场监督管理总局与国家标准化管理委员会发布《信息安全技术—健康医疗数据安全指南》（GB/T 39725-2020），于2021年7月1日实施。该指南明确了健康医疗数据的定义与分类体系，并制定了涵盖使用披露原则、安全管理及技术要点的全方位指南。

2022年8月8日，国家卫生健康委、国家中医药局、国家疾控局三部门联合发布《医疗卫生机构网络安全管理办法》，要求采取加密、备份、脱敏等技术，加强数据全生命周期的安全防护，并基于实际业务场景梳理安全策略，实现针对性防护。

2024年国务院公布《网络数据安全管理条例》，2025年1月1日起施行。该条例细化网络数据处理活动规范，涵盖数据分类分级、个人信息保护、重要数据安全、数据跨境安全管理、平台服务提供者义务、监督管理及法律责任。

上述制度、规范与标准从不同维度厘清监管职责、规范数据处理行为。但医院面对多场景数据应用、分散化数据管理的现实情况，既要严守数据安全与个人信息保护合规底线，又要依法依规挖掘数据要素价值，仍面临诸多全新挑战。

医院数据的多源生产、多场景应用及多目的集成，使得数据处理者、控制者与信息主体之间的关系日趋复杂，医疗机构在数据安全与保护工作上的合规性压力也陡然增加。

行业评价标准的新规定

医疗行业历来高度重视安全工作，各类政策文件、管理制度及业务流程均将安全置于重要位置。医疗数据作为医疗活动的基石，其安全性直接关系到医疗服务稳定。因此，国家在推进医院信息化建设的相关政策中，始终从业务目标出发，对数据安全提出明确要求。

当前，医疗行业各类评审与评级工作均将数据安全作为重要考核指标，主要体现在以下标准/评价体系中：

《三级医院评审标准（2020版）》：针对三级医院评审，该标准设定了严格的“前置要求”，即评审周期内“发生大规模医疗数据泄露或其他重大网络安全事件，造成严重后果”，延期一年评审。延期期间原等次取消，按照“未定等”管理。此外，标准明确要求建立信息安全管理制度，确立主要负责人为第一责任人，并落实网络安全等级保护制度，保障患者隐私与业务连续性。

《电子病历系统应用水平分级评价标准（试行）》：分级评价标准5级及以上规定，要求建立数据使用审查机制，跨境传输需经安全评估；规定数据库操作记录需保存六个月以上，且涉及互联网业务时，数据库服务器不得直接暴露于公网。

《医院信息互联互通标准化成熟度测评方案（2020年版）》：互联互通标准化成熟度测评3级及以上强调，数据的完整性与备份措施，要求数据传输加密、关键数据可追溯，并支持对个人健康档案信息进行字段级、记录级或文件级的加密存储。

《医院智慧服务分级评估标准体系（试行）》：智慧服务分级评估标准2级及以上要求，医院建立全生命周期数据管理体系，特别强调在互联网环境下，患者敏感数据须采用国产算法加密存储，所有数据须加密传输，且跨机构数据使用须审批并可追溯。

《医院智慧管理分级评估标准体系（试行）》：明确要求互联网管理信息系统的重要数据须进行加密传输与存储，且加密算法需符合法律法规要求。

面对上述繁杂且具体的政策要求，医院应如何有效落地执行？行业内有哪些成功经验？在执行过程中又遇到了哪些具体问题及解决方案？这正是本次调查希望重点探究的内容。

医院数据安全防护面临的新风险

当前医院数据安全面临的新挑战，正如“灰犀牛”风险，虽然风险显而易见，但由于危机爆发尚需时间，人们往往心存侥幸，认为总会有解决办法，这种心理上的拖延最终导致了严重后果。这与当前医院数据安全工作面临的困境极为相似。

随着医院数据量快速增长，院内及机构间的数据交换共享需求也迅速提升。这些医疗数据资源在助力医院高质量发展的同时，也面临着日益严峻的安全风险。全球范围内，黑客为谋取非法利益，利用勒索病毒等手段窃取和破坏医院数据的事件时有发生。尽管大家已意识到风险的严重性，但此类事件的发生频率和破坏程度却在不断上升。这背后的原因是什么？应采取何种措施做好数据保护？本次调查计划通过收集医院数据安全保护工作的相关数据，分析问题产生原因，从而为政府部门和医疗机构提供政策建议。

医院AI技术应用出现新趋势

人工智能技术在医疗领域的深度应用，在提升诊疗效率的同时，也衍生出更为隐蔽且严峻的数据安全威胁。

医院使用AI赋能应用越来越广泛，对于AI赋能隐私泄露风险从“存储端”向“模型端”蔓延。医疗大模型的训练依赖于海量高敏感数据，这些数据往往包含患者隐私等核心敏感信息。在模型训练、微调及迭代过程中，若缺乏严格的数据安全保护，极易导致医疗数据大范围泄露。

调查基本情况

调查目的

数据安全建设是医院满足国家安全监管政策要求、保证自身业务稳定运行的重要保障。为了探索医院数据安全治理体系建设的经验与问题，应对合规挑战，防范医院数据安全“灰犀牛事件”的发生，中国医院协会信息专业委员会（CHIMA）组织开展了医院数据安全调查研究工作。本次调查旨在全面了解医院数据安全现状、应用效果及问题，为医院制定数据安全规划提供客观依据，为监管部门、医院信息化从业人员及医疗信息化厂商提供数据安全建设参考。

调查方法

本次调查采用问卷的形式。制定调查问卷时，邀请了专家对问卷内容进行意见征求，基本采纳专家的建议。针对全国部分医院信息技术部门负责人及数据安全建设和维护等相关管理人员开展了医疗行业数据安全调查。

调查对象及范围

调查内容包括：（1）医院基本信息调查；（2）医院对《数据安全法》《个人信息保护法》等法律法规的了解以及是否组织学习宣贯；（3）医院数据安全建设现状、存在的问题、系统功能、分级评估等。

本次调研覆盖全国31个省市自治区，回复在50（含50）家医院以上的省市级行政区域划分有4个，分别是河北省、天津市、山西省、北京市；回复在21—50家医院范围内的省市行政区划分有10个，分别是：甘肃省、广东省、辽宁省、新疆维吾尔自治区、江苏省、浙江省、四川省、重庆市、云南省和山东省。详细数据见图2.3_1。

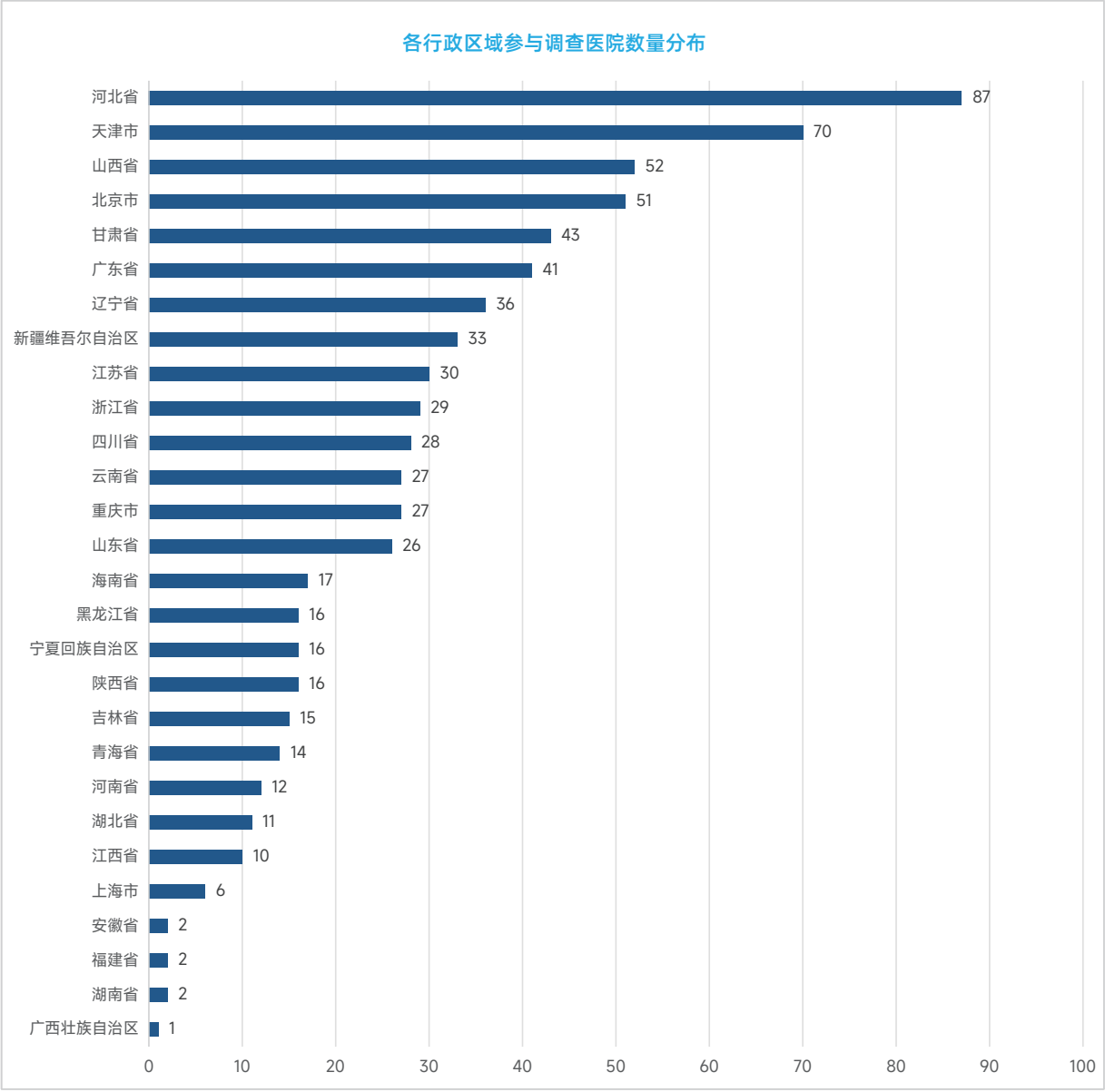

图2.3_1 各行政区域参与调查医院数量分布

本次调查共收回问卷769份，经过初步查重和筛选，共有有效问卷720份数据。其中三级医院399家，占调查样本数的55.42%，三级以下医院321家，占调查样本数的44.58%，详细数据见表2.3_2。

表2.3_2 参与调查的医院级别

参与调研的医院级别	数量	比例[N=720]
三级医院	399	55.42%
三级以下医院	321	44.58%

按照不同医院类别进行统计，综合医院526家，占调查样本数73.06%，专科医院148家，占调查样本数20.56%，详细数据见表2.3_3。

表2.3_3 参与调查的医院类别

参与调研的医院类别	数量	比例[N=720]
综合医院	526	73.06%
专科医院	148	20.56%
其他	46	6.38%

对参与调研的医院性质进行统计，公立医院674家，占调查样本93.61%，非公立医院46家，占调查样本数6.39%，详细数据见表2.3_4。

表2.3_4 参与调查的医院性质

参与调研的医院性质	数量	比例[N=720]
公立医院	674	93.61%
非公立医院	46	6.39%

对参与调研医院按照开放床位数进行统计，26.11%（188家）的医院床位数在501-1000张之间，其次≤250张床位的医院比例为25.83%（186家）。大于5000张开放床位的医院数量最少，为5家，占比0.69%。详细数据见表2.3_5。

表2.3_5 参与调查的医院开放床位数

参与调研医院的开放床位数	数量	比例[N=720]
≤250	186	25.83%
1001-2000	132	18.33%
2001-3000	53	7.36%
251-500	143	19.86%
3001-5000	13	1.81%
501-1000	188	26.11%
大于5000	5	0.69%

对参与调研的医院信息化投入占医疗总收入的占比进行分析，发现信息化投入低于0.1%的医院数量最多，有169家，占比23.47%；其次是占比为1%-2%的区间，有133家医院，比例为18.74%。信息化投入占总收入投入在10%以上的医院数量最少，只有5家，比例为0.69%。详细数据见表2.3_6。

表2.3_6 参与调查的医院信息化投入/医疗总收入占比

参与调研医院信息化投入/医疗总收入占比	数量	比例[N=720]
低于0.1%	169	23.47%
0.1%-0.2%(含)	119	16.53%
0.2%-0.5%(含)	100	13.89%
0.5%-1%(含)	121	16.81%
1%-2%(含)	133	18.47%
2%-5%(含)	47	6.53%
5%-10%(含)	26	3.61%
10%以上	5	0.69%

对参与调查医院的信息安全专管人员数量进行统计发现，接近一半的医院只有1位专管人员（41.11%），其次是专管人员有2人的医院，有139家（19.31%）。没有专管人员的医院数量有83家，占比11.53%。详细数据见表2.3_7。

表2.3_7 医院信息安全专管人员数量

医院信息安全专管人员数量	数量	比例[N=720]
1人	296	41.11%
2人	139	19.31%
3人	67	9.31%
4人	29	4.03%
5人	31	4.31%
5人以上	75	10.42%
无	83	11.53%

调查主要发现

数据安全认知情况

本文中数据安全认知情况的含义是指调查对象对《数据安全法》和《个人信息保护法》两部法律认知情况。下文中《数据安全法》和《个人信息保护法》用“两法”表述。

对“两法”了解情况

对调查医院进行分析发现，非常了解的医院仅占29.17%，68.33%的医院对两者的理解均为了解一点，不了解的占比仅2.50%，合计占比70.83%的医院对两法的了解程度不够深入，医院对《数据安全法》和《个人信息保护法》的解读和宣贯有着迫切需求。详细数据见图3.1.1，表3.1.1。

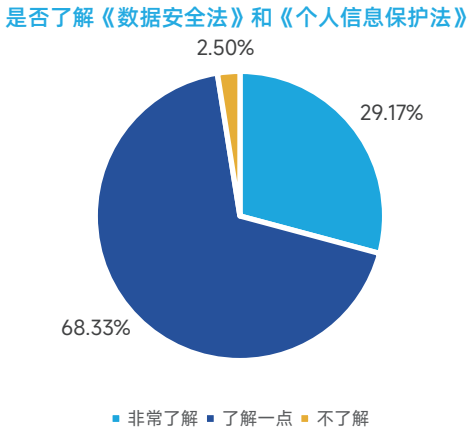

图3.1.1 是否了解《数据安全法》和《个人信息保护法》

表3.1.1 是否了解《数据安全法》和《个人信息保护法》

是否了解《数据安全法》和《个人信息保护法》	数量	比例[N=720]
非常了解	210	29.17%
了解一点	492	68.33%
不了解	18	2.50%

“两法”对医院数据安全管理工作的影响

从调研数据看出，需加强数据安全能力建设（86.53%），需要有专门的数据安全管理人员和相应的制度与流程（76.53%），需加强对数据的安全保护，购买数据安全相关产品（73.61%），分列前三。详细数据见图3.1.2，表3.1.2。

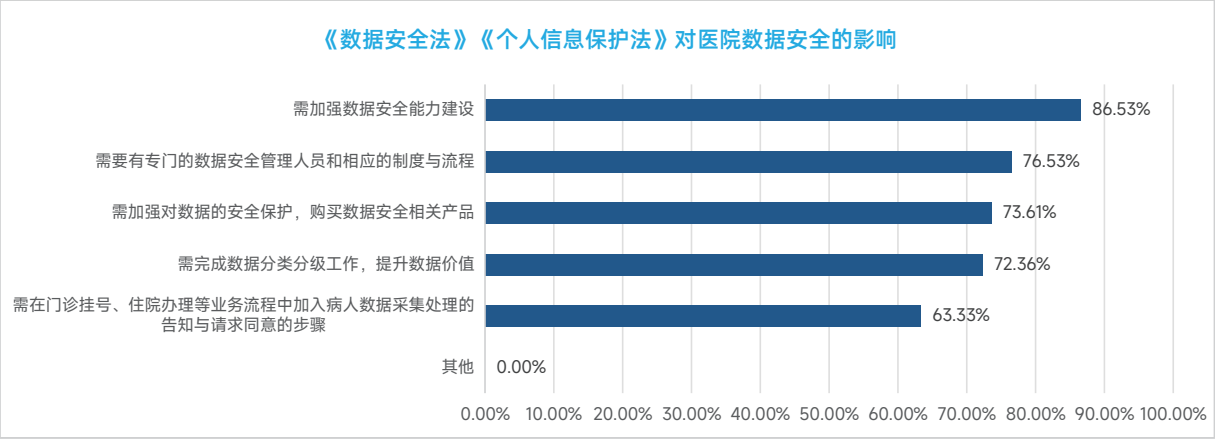

图3.1.2《数据安全法》《个人信息保护法》对医院数据安全的影响

表3.1.2《数据安全法》《个人信息保护法》对医院数据安全的影响

《数据安全法》《个人信息保护法》对医院数据安全的影响	数量	比例[N=720]
需加强数据安全能力建设	623	86.53%
需要有专门的数据安全管理人员和相应的制度与流程	551	76.53%
需加强对数据的安全保护，购买数据安全相关产品	530	73.61%
需完成数据分类分级工作，提升数据价值	521	72.36%
需在门诊挂号、住院办理等业务流程中加入病人数据采集处理的告知与请求同意的步骤	456	63.33%
其他	0	0.00%

对“两法”组织学习情况

调查显示，有70.14%的医院组织学习两部法律，仍有29.86%的医院未开展，说明对《数据安全法》和《个人信息保护法》的培训和宣贯力度仍需加强。详细数据见图3.1.3，表3.1.3。

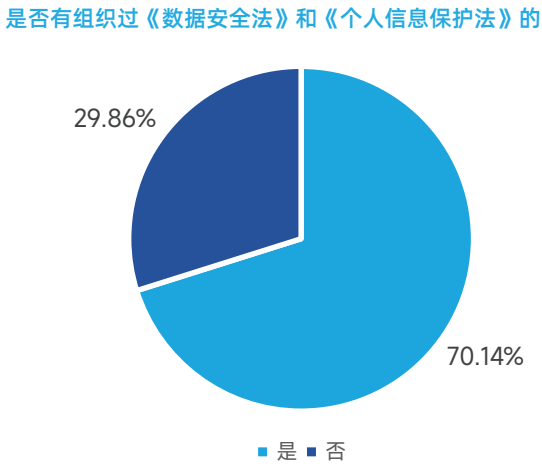

图3.1.3 是否有组织过《数据安全法》和《个人信息保护法》的学习和宣贯

表3.1.3 是否有组织过《数据安全法》和《个人信息保护法》的学习和宣贯

是否有组织过《数据安全法》和《个人信息保护法》的学习和宣贯	数量	比例[N=720]
是	505	70.14%
否	215	29.86%

按“两法”开展制度建设情况

从720家调查医院数据分析可以看出，57.5%的医院均按照相关法律制定了本单位的相关流程和制度。详细数据见图3.1.4，表3.1.4。

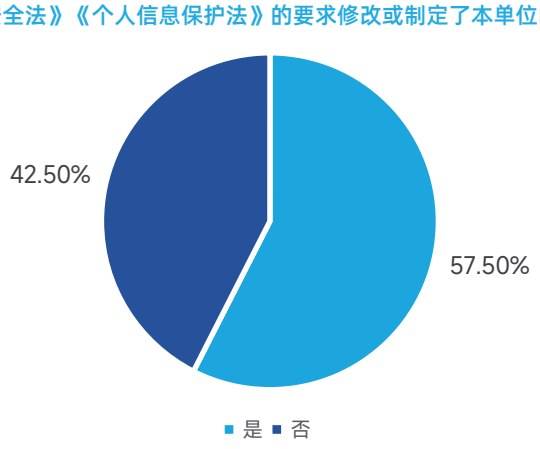

图3.1.4 是否根据《数据安全法》《个人信息保护法》的要求修改或制定了本单位的相关制度和流程

表3.1.4 是否根据《数据安全法》《个人信息保护法》的要求修改或制定了本单位的相关制度和流程

是否根据《数据安全法》《个人信息保护法》的要求修改或制定了本单位的相关制度和流程	数量	比例[N=720]
是	414	57.50%
否	306	42.50%

按“两法”要求建设实施情况

根据调研数据分析显示，超过一半的医院（57.36%）计划按照《数据安全法》和《个人信息保护法》要求加强数据安全建设，已经开展的医院占比32.64%。详细数据见图3.1.5，表3.1.5。

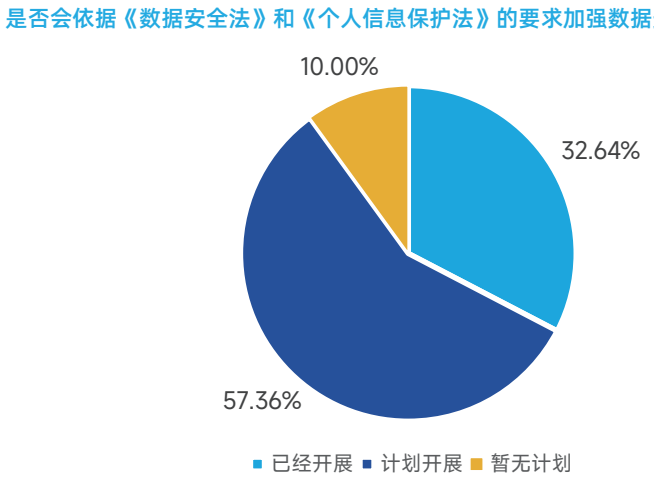

图3.1.5 是否会依据《数据安全法》和《个人信息保护法》的要求加强数据安全方面的建设

表3.1.5 是否会依据《数据安全法》和《个人信息保护法》的要求加强数据安全方面的建设

是否会依据《数据安全法》和《个人信息保护法》的要求加强数据安全方面的建设	数量	比例[N=720]
已经开展	235	32.64%
计划开展	413	57.36%
暂无计划	72	10.00%

数据安全管理情况

开展数据安全能力建设的主要动力

数据分析发现，医院开展数据安全能力建设的主要动力占前两位的是防范风险事件发生（83.75%）和合规需求（77.08%），反映出保障业务运营连续性和确保法律合规是医院开展数据安全能力建设的主要动力。详细数据见图3.2.1，表3.2.1。

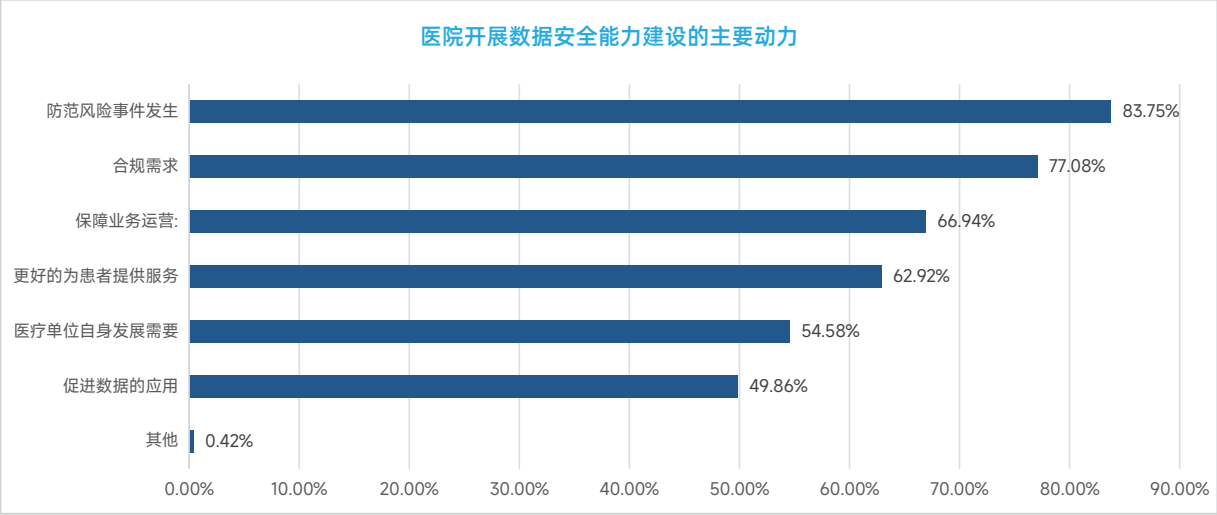

图3.2.1 医院开展数据安全能力建设的主要动力

表3.2.1 医院开展数据安全能力建设的主要动力

医院开展数据安全能力建设的主要动力	数量	比例[N=720]
防范风险事件发生	603	83.75%
合规需求	555	77.08%
保障业务运营	482	66.94%
更好的为患者提供服务	453	62.92%
医疗单位自身发展需要	393	54.58%
促进数据的应用	359	49.86%
其他	3	0.42%

数据安全组织架构情况

调研显示，90.14%的医院认为有必要建立专门负责数据安全的组织机构。详细数据见图3.2.2_1，表3.2.2_1。

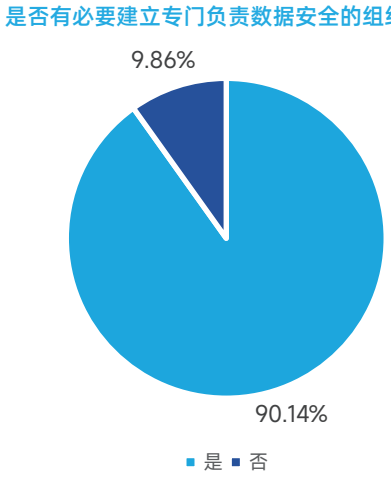

图3.2.2_1 是否有必要建立专门负责数据安全的组织架构

表3.2.2_1是否有必要建立专门负责数据安全的组织架构

是否有必要建立专门负责数据安全的组织架构	数量	比例[N=720]
是	649	90.14%
否	71	9.86%

调研样本中只有17.08%的医院有单独的数据安全团队，45.28%的医院由网络安全团队兼顾负责数据安全，37.6%的医院暂未有团队负责数据安全工作。详细数据见图3.2.2_2，表3.2.2_2。

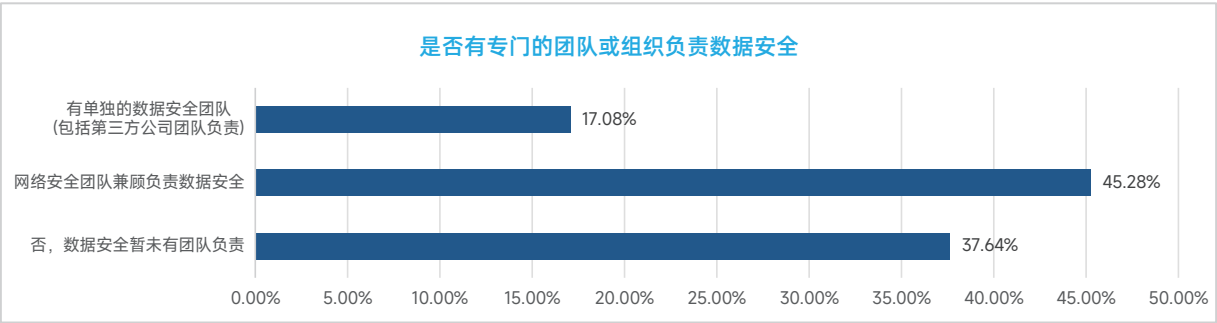

图3.2.2_2 是否有专门的团队或组织负责数据安全

表3.2.2_2 是否有专门的团队或组织负责数据安全

是否有专门的团队或组织负责数据安全	数量	比例[N=720]
有单独的数据安全团队(包括第三方公司团队负责)	123	17.08%
网络安全团队兼顾负责数据安全	326	45.28%
否，数据安全暂未有团队负责	271	37.64%

网络安全建设投入情况

对调查医院上年度网络安全投入/信息化投入占比进行分析，发现投入在0%-5%(含)区间的医院比例最高，占比61.94%；投入在20%以上占比最低，为8.06%。详细数据见图3.2.3，表3.2.3。

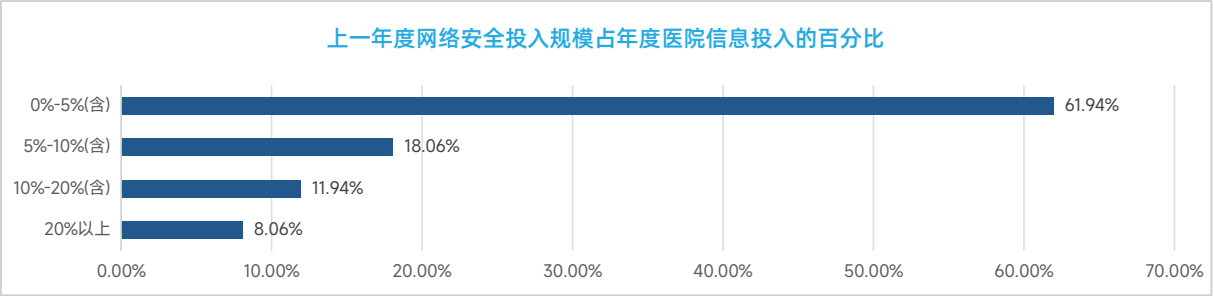

图3.2.3 上一年度网络安全投入规模占年度医院信息投入的百分比

表3.2.3 上一年度网络安全投入规模占年度医院信息投入的百分比

上一年度网络安全投入规模占年度医院信息化投入的百分比	数量	比例[N=720]
0%-5%(含)	446	61.94%
5%-10%(含)	130	18.06%
10%-20%(含)	86	11.94%
20%以上	58	8.06%

与第三方合作时的安全管理情况

数据分析结果显示，与第三方合作时，医院倾向于签订保密协议，占比84.86%；其次是进行数据安全意识教育，占比46.94%；第三是将第三方安全要求纳入数据安全制度的闭环管理，对第三方人员的访问权限进行严格管控，占比43.19%。详细数据见图3.2.4，表3.2.4。

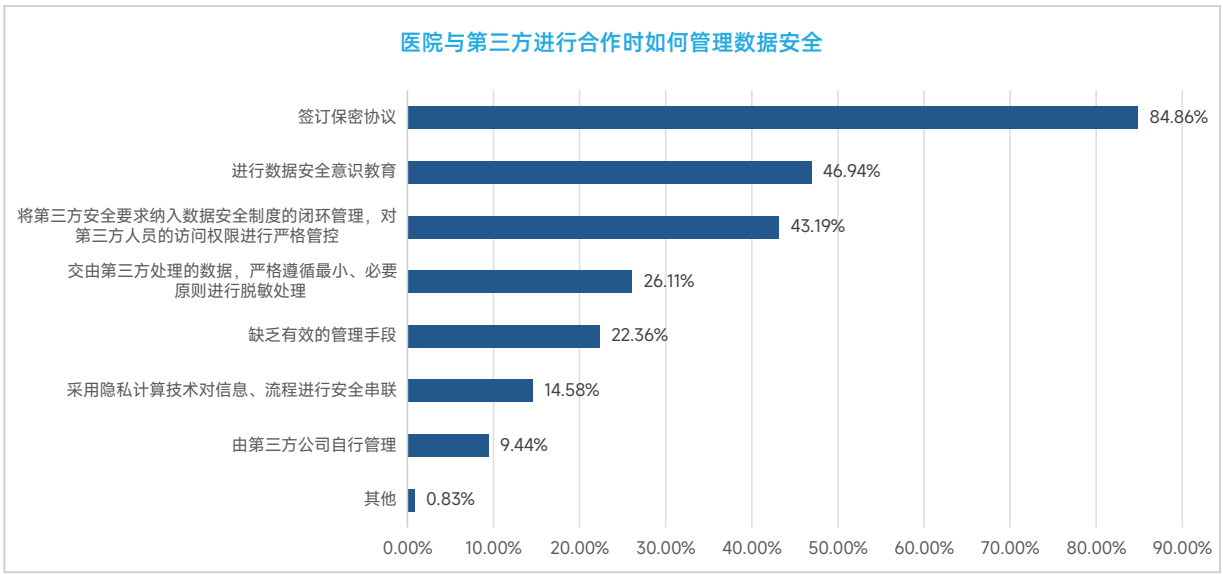

图3.2.4 医院与第三方进行合作时如何管理数据安全

表3.2.4 医院与第三方进行合作时如何管理数据安全

医院与第三方进行合作时如何管理数据安全	数量	比例[N=720]
签订保密协议	611	84.86%
进行数据安全意识教育	338	46.94%
将第三方安全要求纳入数据安全制度的闭环管理，对第三方人员的访问权限进行严格管控	311	43.19%
交由第三方处理的数据，严格遵循最小、必要原则进行脱敏处理	188	26.11%
缺乏有效的管理手段	161	22.36%
采用隐私计算技术对信息、流程进行安全串联	105	14.58%
由第三方公司自行管理	68	9.44%
其他	6	0.83%

计划开展的数据安全工作

从数据分析可以看出，77.64%的医院主要集中在开展数据安全培训。采购数据安全产品（53.75%）和参与数据安全评估测评（51.67%）分列第二、三位。详细数据见图3.2.5，表3.2.5。

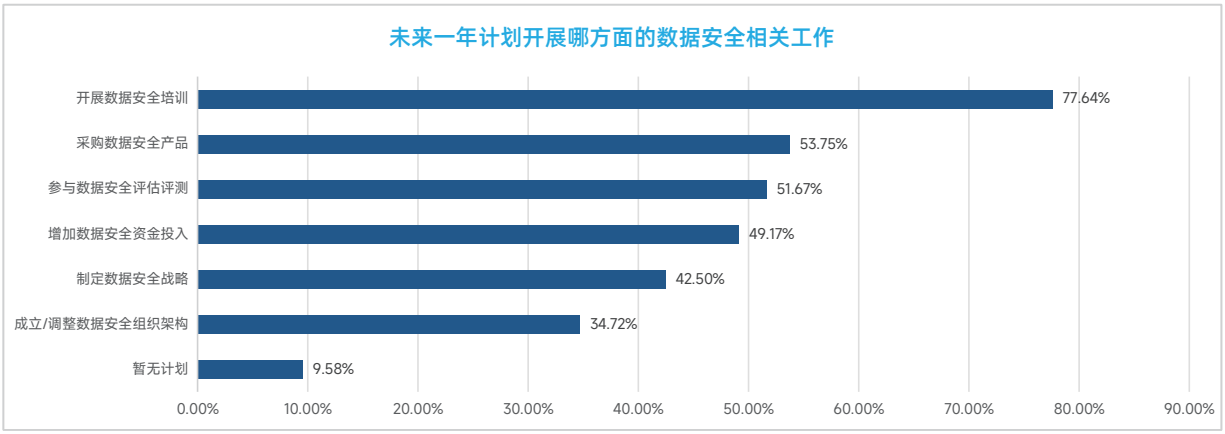

图3.2.5 未来一年计划开展哪方面的数据安全相关工作

表3.2.5 未来一年计划开展哪方面的数据安全相关工作

未来一年计划开展哪方面的数据安全相关工作	数量	比例[N=720]
开展数据安全培训	559	77.64%
采购数据安全产品	387	53.75%
参与数据安全评估评测	372	51.67%
增加数据安全资金投入	354	49.17%
制定数据安全战略	306	42.50%
成立/调整数据安全组织架构	250	34.72%
暂无计划	69	9.58%

数据安全技术应用情况

数据安全保护措施

数据分析显示，数据库防火墙/网关是目前医院使用最多的数据安全保护措施，占比76.25%；其次是数据备份，占比74.72%；第三是具备勒索病毒查杀能力的杀毒软件或终端管理软件，占比74.58%。详细数据见图3.3.1，表3.3.1。

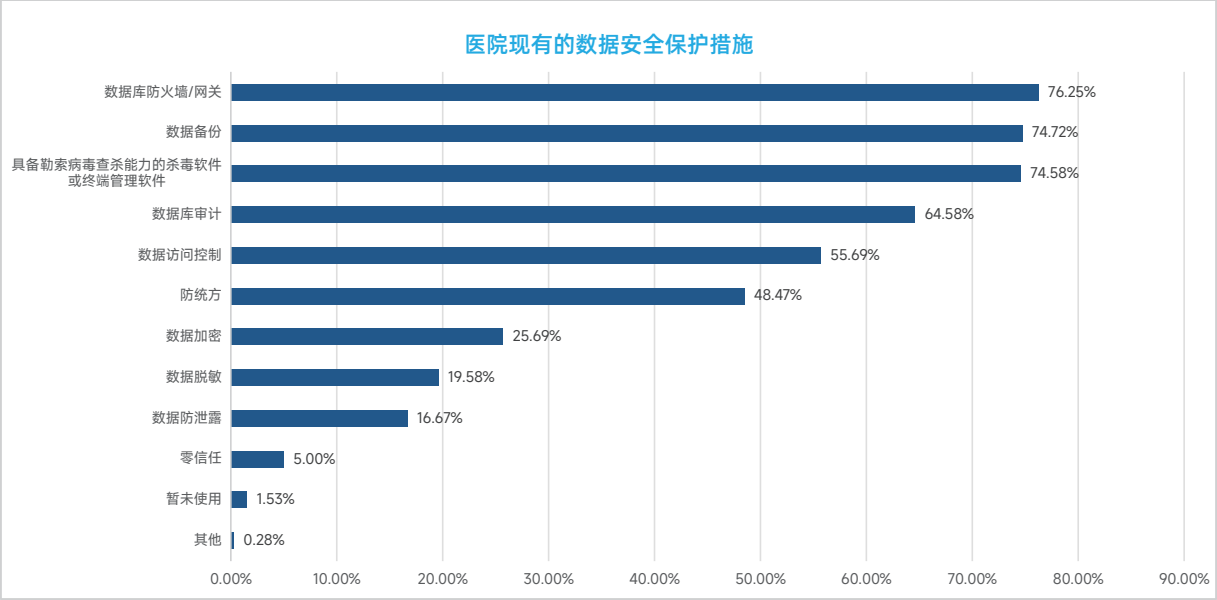

图3.3.1 医院现有的数据安全保护措施

表3.3.1 医院现有的数据安全保护措施

医院现有的数据安全保护措施	数量	比例[N=720]
数据库防火墙/网关	549	76.25%
数据备份	538	74.72%
具备勒索病毒查杀能力的杀毒软件或终端管理软件	537	74.58%
数据库审计	465	64.58%
数据访问控制	401	55.69%
防统方	349	48.47%
数据加密	185	25.69%
数据脱敏	141	19.58%
数据防泄露	120	16.67%
零信任	36	5.00%
暂未使用	11	1.53%
其他	2	0.28%

数据接口防护情况

数据显示，医院数据接口防护多为：合并数据接口，减少暴露面，增加可管理性位列首位，超过50%。详细数据见图3.3.2，表3.3.2。

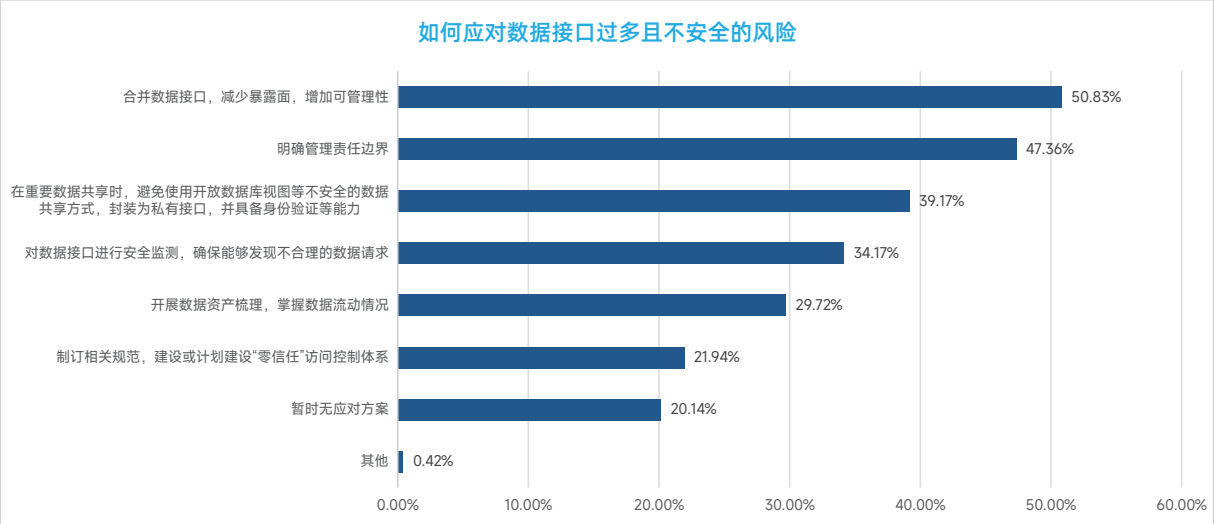

图3.3.2 如何应对数据接口过多且不安全的风险

表3.3.2 如何应对数据接口过多且不安全的风险

如何应对数据接口过多且不安全的风险	数量	比例[N=720]
合并数据接口，减少暴露面，增加可管理性	366	50.83%
明确管理责任边界	341	47.36%
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，并具备身份验证等能力	282	39.17%
对数据接口进行安全监测，确保能够发现不合理的数据请求	246	34.17%
开展数据资产梳理，掌握数据流动情况	214	29.72%
制订相关规范，建设或计划建设“零信任”访问控制体系	158	21.94%
暂时无应对方案	145	20.14%
其他	3	0.42%

数据库安全防御措施

数据分析显示，医院数据库安全建设采取的主动防御措施最多的是定期进行安全检查分析，占比76.25%；第二是数据库运维的身份识别、运维审批、流程管理，占比55.28%；第三是数据库增删改查的权限机制管理，占比47.78%。详细数据见图3.3.3，表3.3.3。

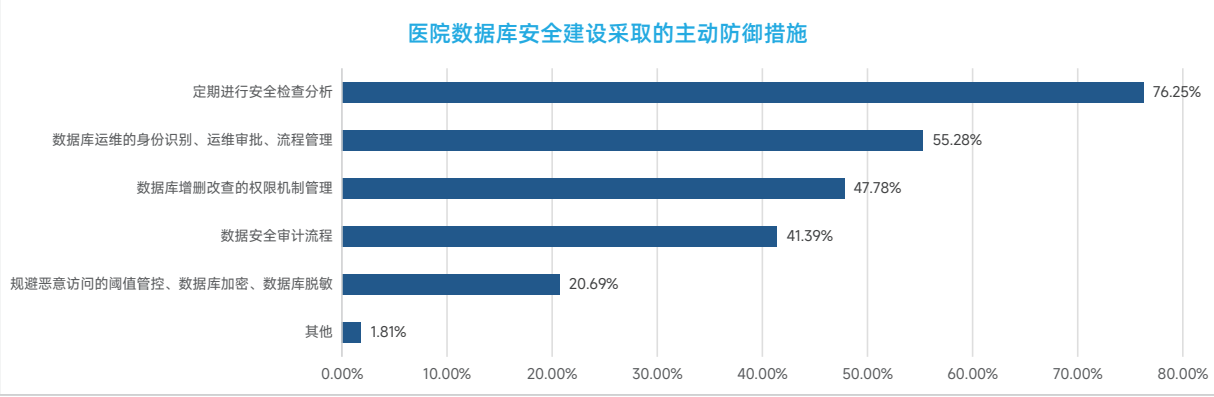

图3.3.3 医院数据库安全建设采取的主动防御措施

表3.3.3 医院数据库安全建设采取的主动防御措施

医院数据库安全建设采取的主动防御措施	数量	比例[N=720]
定期进行安全检查分析	549	76.25%
数据库运维的身份识别、运维审批、流程管理	398	55.28%
数据库增删改查的权限机制管理	344	47.78%
数据安全审计流程	298	41.39%
规避恶意访问的阈值管控、数据库加密、数据库脱敏	149	20.69%
其他	13	1.81%

账户口令安全风险防范情况

分析数据显示，医院主要通过开启强口令策略，要求医护人员定期更换口令，且不可为弱口令，应对风险（67.78%）；其次是实施账号安全责任制，并加强安全意识培训（60%），第三是要求工作账号口令单独设置，不得与个人生活常用账号口令一样（53.19%）。其他选项为堡垒机等技术防护、电子签名/数字签名、CA。详细数据见图3.3.4，表3.3.4。

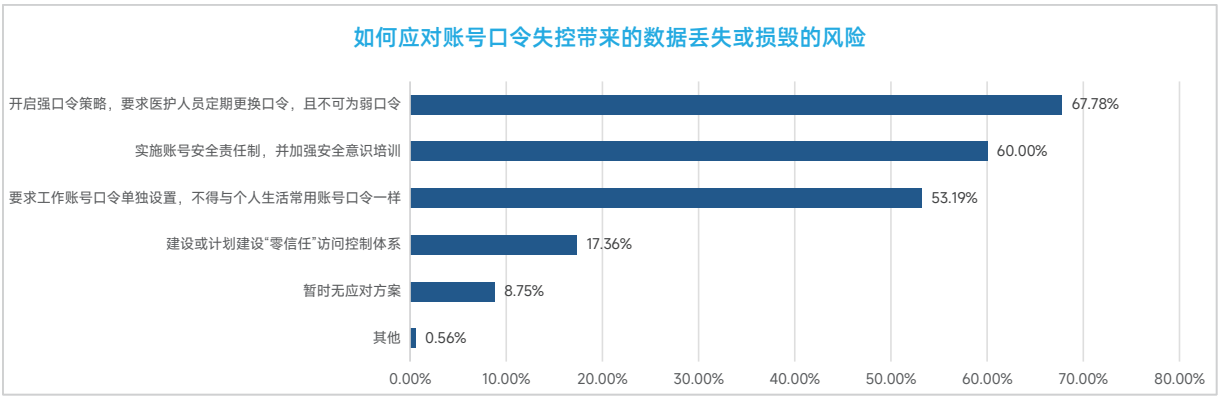

图3.3.4 如何应对弱口令带来的数据安全风险

表3.3.4 如何应对弱口令带来的数据安全风险

如何应对弱口令带来的数据安全风险	数量	比例[N=720]
开启强口令策略，要求医护人员定期更换口令，且不可为弱口令	488	67.78%
实施账号安全责任制，并加强安全意识培训	432	60.00%
要求工作账号口令单独设置，不得与个人生活常用账号口令一样	383	53.19%
建设或计划建设"零信任"访问控制体系	125	17.36%
暂时无应对方案	63	8.75%
其他	4	0.56%

应对外部攻击防护情况

数据显示，医院应对外部攻击主要方式是对院内数据加强纵深防御，占比过半（57.78%），而暂无应对方案占19.72%。详细数据见图3.3.5，表3.3.5。

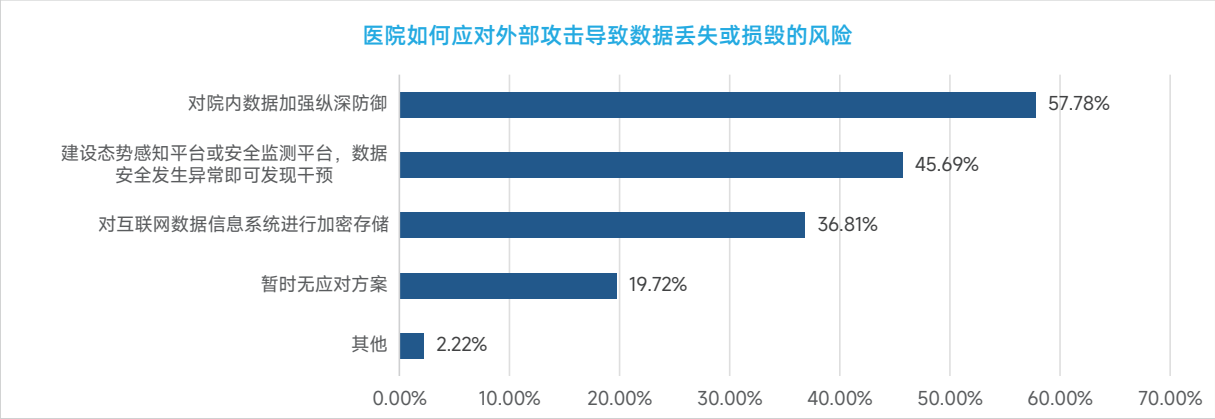

图3.3.5 医院如何应对外部攻击导致数据丢失或损毁的风险

表3.3.5 医院如何应对外部攻击导致数据丢失或损毁的风险

医院如何应对外部攻击导致数据丢失或损毁的风险	数量	比例[N=720]
对院内数据加强纵深防御	416	57.78%
建设态势感知平台或安全监测平台，数据安全发生异常即可发现干预	329	45.69%
对互联网数据信息系统据进行加密存储	265	36.81%
暂时无应对方案	142	19.72%
其他	16	2.22%

系统运维安全防护情况

医院在应对运维过程中的数据丢失或损毁，方式主要为加强运维人员院内活动管理，包括门禁权限、视频监控等，占比70.97%。其次是加强运维方式管理，包括通过必须通过堡垒机运维、默认关闭远程运维通道等，占比69.72%。详细数据见图3.3.6，表3.3.6。

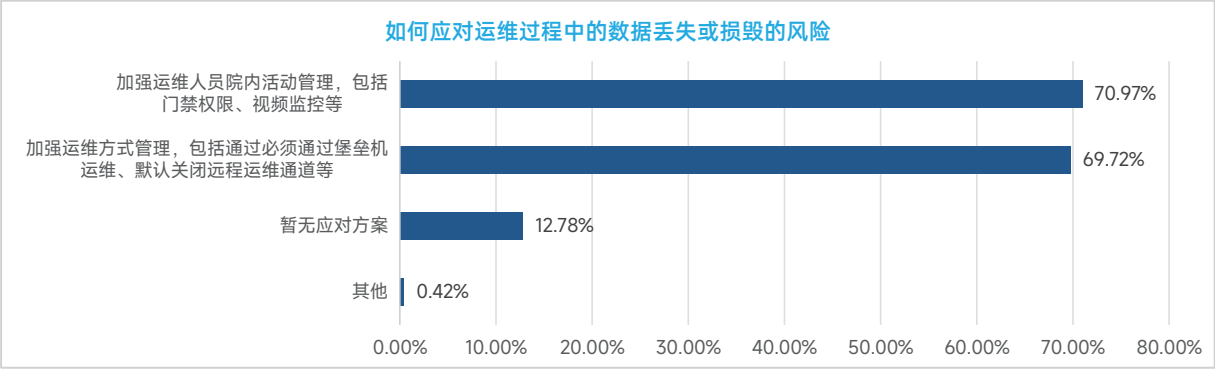

图3.3.6 如何应对运维过程中的数据丢失或损毁的风险

表3.3.6 如何应对运维过程中的数据丢失或损毁的风险

如何应对运维过程中的数据丢失或损毁的风险	数量	比例[N=720]
加强运维人员院内活动管理，包括门禁权限、视频监控等	511	70.97%
加强运维方式管理，包括通过必须通过堡垒机运维、默认关闭远程运维通道等	502	69.72%
暂无应对方案	92	12.78%
其他	3	0.42%

互联网医疗个人信息保护情况

调研数据显示，互联网医院运营中，个人隐私保护设置机制集中在病毒检测和防护（占比67.22%），入侵防护检测（64.86%），身份认证（62.08%）。详细数据见图3.3.7，表3.3.7。

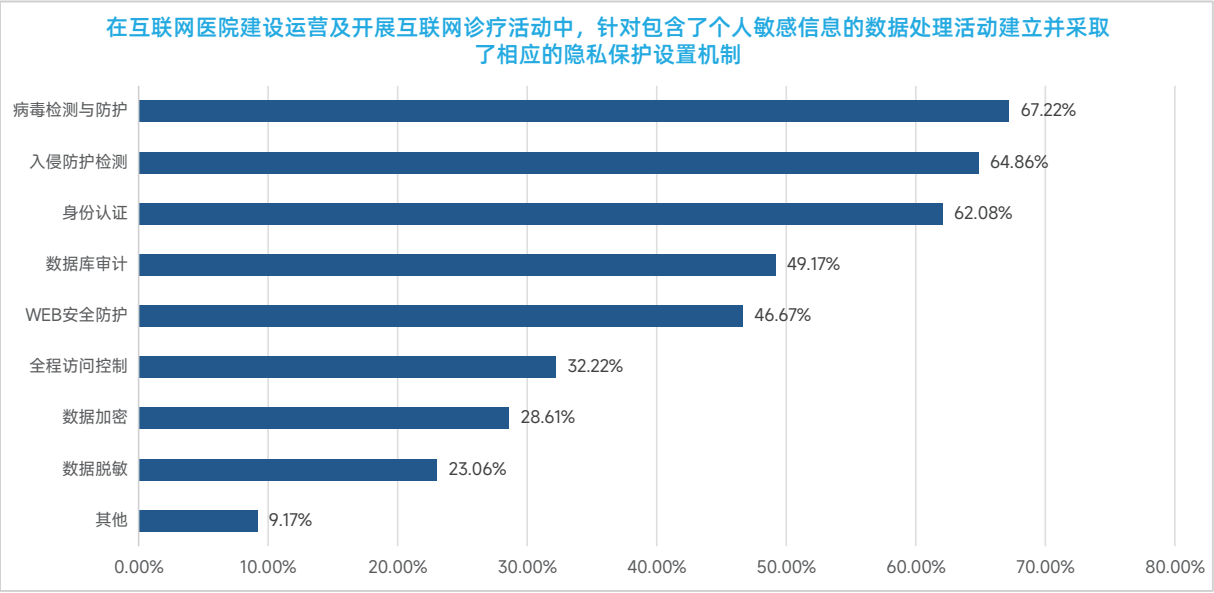

图3.3.7 在互联网医院建设运营及开展互联网诊疗活动中，针对包含了个人敏感信息的数据处理活动建立并采取了相应的隐私保护设置机制

表3.3.7 在互联网医院建设运营及开展互联网诊疗活动中，针对包含了个人敏感信息的数据处理活动建立并采取了相应的隐私保护设置机制

在互联网医院建设运营及开展互联网诊疗活动中，针对包含了个人敏感信息的数据处理活动建立并采取了相应的隐私保护设置机制	数量	比例[N=720]
病毒检测与防护	484	67.22%
入侵防护检测	467	64.86%
身份认证	447	62.08%
数据库审计	354	49.17%
WEB安全防护	336	46.67%
全程访问控制	232	32.22%
数据加密	206	28.61%
数据脱敏	166	23.06%
其他	66	9.17%

医学科研个人敏感信息数据安全保护情况

针对包含个人敏感信息数据处理采取隐私保护设置机制方式，多集中在设置访问权限，占比60.97%；其次为签署保密协议，占比50.97%。详细数据见图3.3.8，表3.3.8。

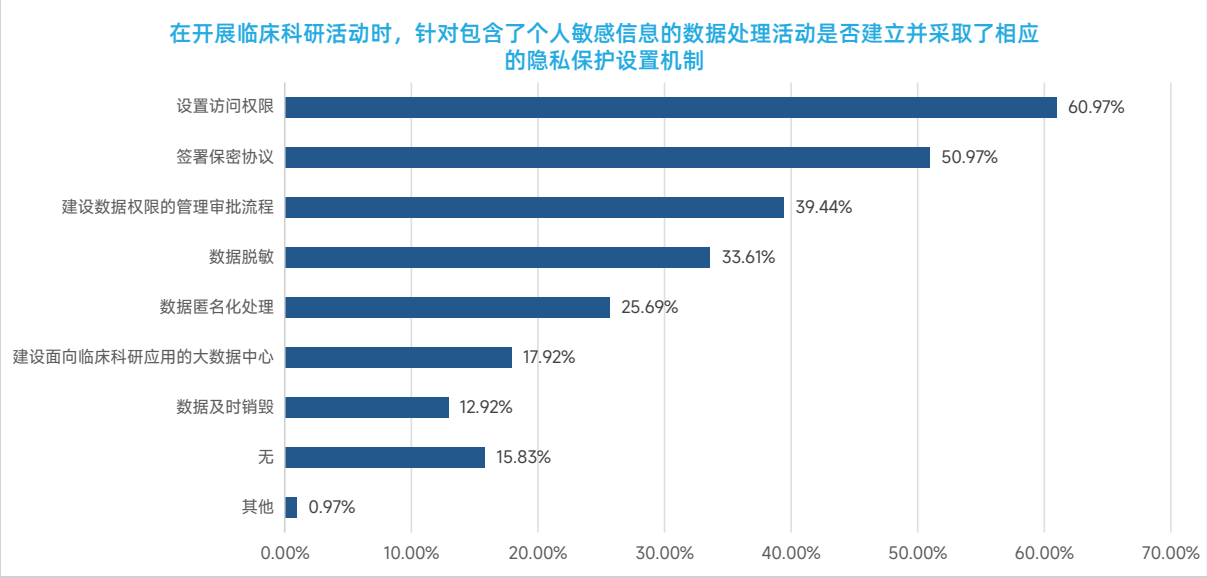

图3.3.8 在开展临床科研活动时，针对包含了个人敏感信息的数据处理活动是否建立并采取了相应的隐私保护设置机制

表3.3.8 在开展临床科研活动时，针对包含了个人敏感信息的数据处理活动是否建立并采取了相应的隐私保护设置机制

在开展临床科研活动时，针对包含了个人敏感信息的数据处理活动是否建立并采取了相应的隐私保护设置机制	数量	比例[N=720]
设置访问权限	439	60.97%
签署保密协议	367	50.97%
建设数据权限的管理审批流程	284	39.44%
数据脱敏	242	33.61%
数据匿名化处理	185	25.69%
建设面向临床科研应用的大数据中心	129	17.92%
数据及时销毁	93	12.92%
无	114	15.83%
其他	7	0.97%

数据安全工作的困难与问题

数据安全保护工作的主要困难

调查显示，医院在数据保护工作中主要存在的困扰主要是缺乏数据安全专业能力（75.14%）、缺乏资金支持（72.22%）、缺乏相关标准与指导（61.25%），均过半。详细数据见图3.4.1，表3.4.1。

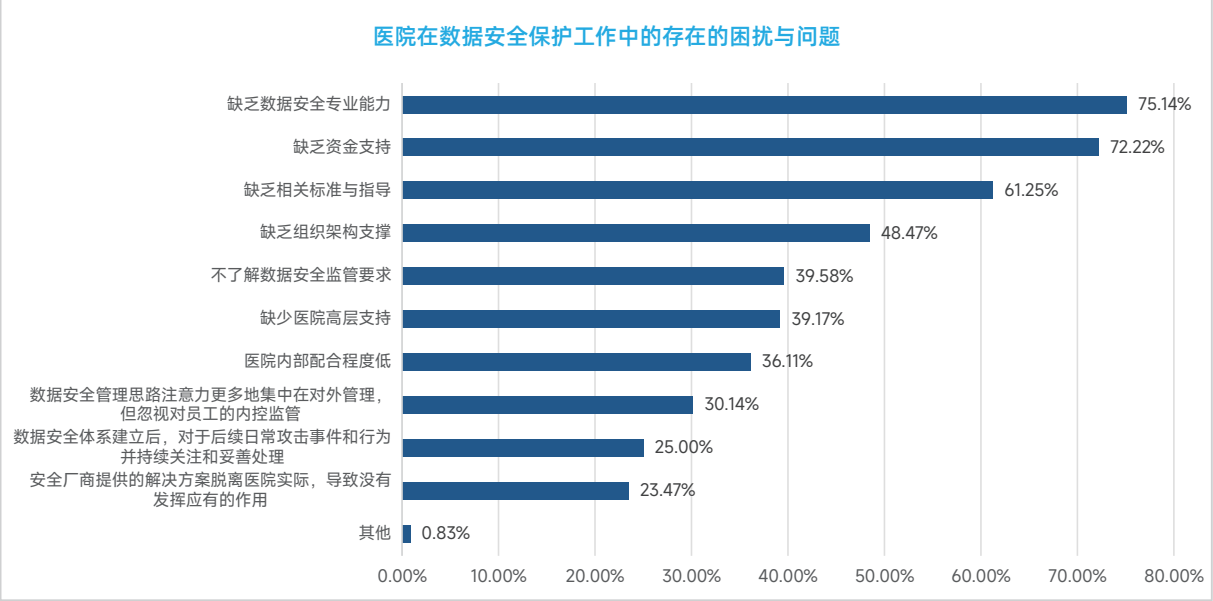

图3.4.1 医院在数据安全保护工作中的存在的困扰与问题

表3.4.1 医院在数据安全保护工作中的存在的困扰与问题

医院在数据安全保护工作中的存在的困扰与问题	数量	比例[N=720]
缺乏数据安全专业能力	541	75.14%
缺乏资金支持	520	72.22%
缺乏相关标准与指导	441	61.25%
缺乏组织架构支撑	349	48.47%
不了解数据安全监管要求	285	39.58%
缺少医院高层支持	282	39.17%
医院内部配合程度低	260	36.11%
数据安全管理思路注意力更多地集中在对外管理，但忽视对员工的内控监管	217	30.14%
数据安全体系建立后，对于后续日常攻击事件和行为并持续关注和妥善处理	180	25.00%
安全厂商提供的解决方案脱离医院实际，导致没有发挥应有的作用	169	23.47%
其他	6	0.83%

数据安全工作的服务内容

调查显示，医院在数据安全领域最希望得到的服务为全面的数据安全咨询服务（73.89%）、数据安全意识培训服务（68.33%）、数据资产盘点与数据分类分级服务（64.03%），排名前三位。详细数据见图3.4.2，表3.4.2。

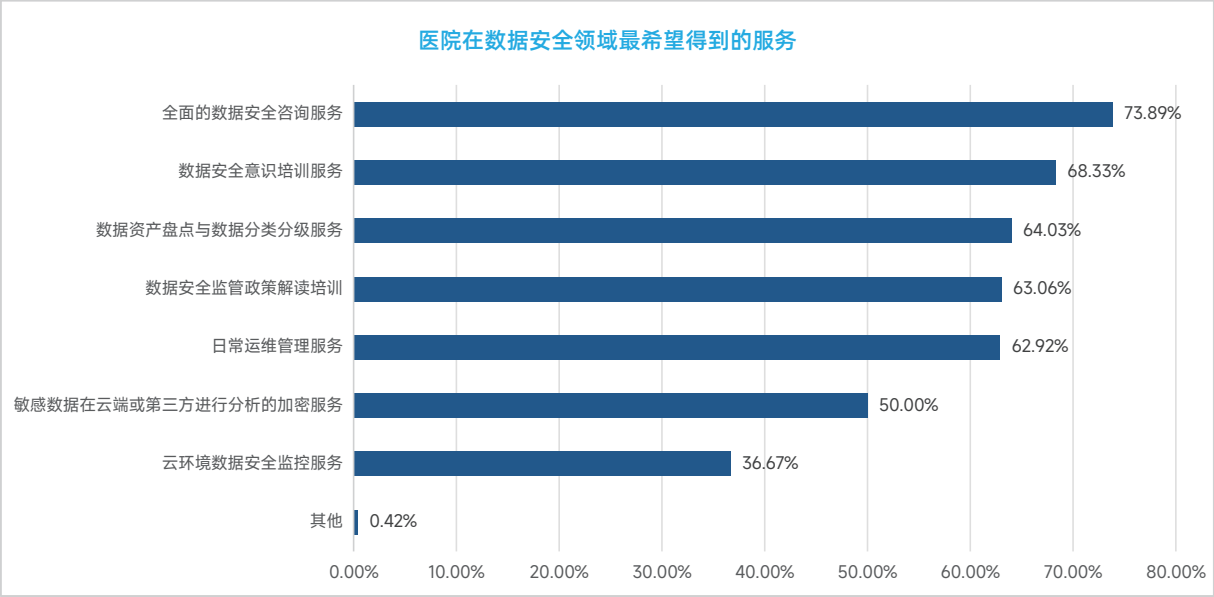

图3.4.2 医院在数据安全领域最希望得到的服务

表3.4.2 医院在数据安全领域最希望得到的服务

医院在数据安全领域最希望得到的服务	数量	比例[N=720]
全面的数据安全咨询服务	532	73.89%
数据安全意识培训服务	492	68.33%
数据资产盘点与数据分类分级服务	461	64.03%
数据安全监管政策解读培训	454	63.06%
日常运维管理服务	453	62.92%
敏感数据在云端或第三方进行分析的加密服务	360	50.00%
云环境数据安全监控服务	264	36.67%
其他	3	0.42%

亟须开展的重点工作

调查显示，医院在数据安全领域最紧迫需要开展的工作分别是：开展数据分类分级工作，识别敏感数据（27.78%）；购买并实施数据安全产品（19.72%）；规划数据安全治理工作，制定安全工作实施路线图（17.08%）。详细数据见图3.4.3，表3.4.3。

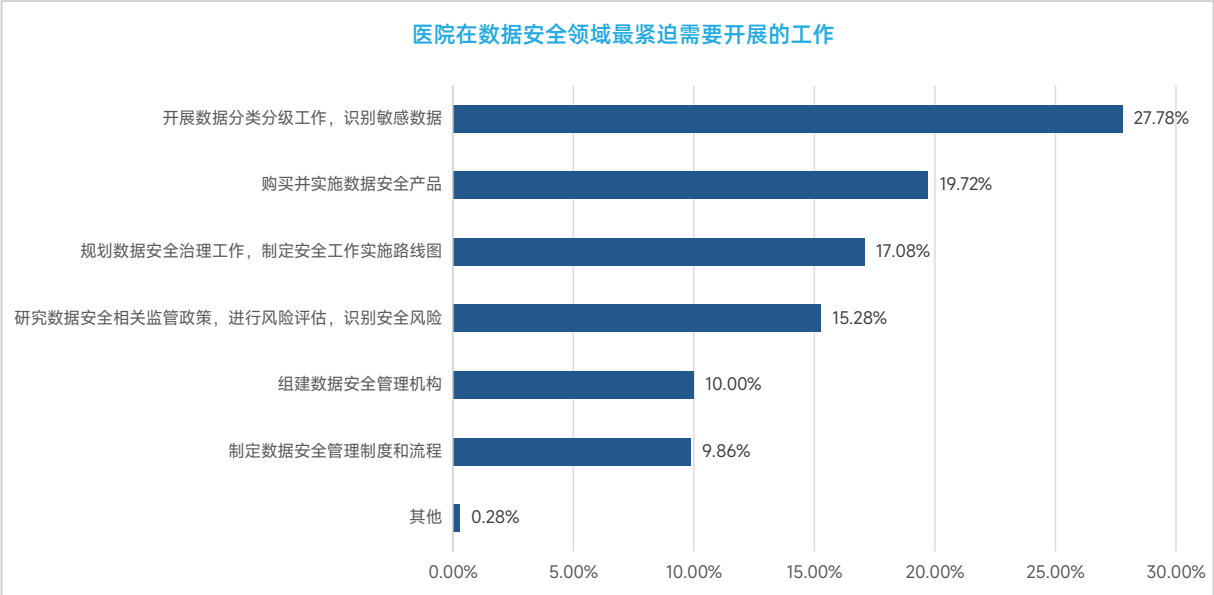

图3.4.3 医院在数据安全领域最紧迫需要开展的工作

表3.4.3 医院在数据安全领域最紧迫需要开展的工作

医院在数据安全领域最紧迫需要开展的工作	数量	比例[N=720]
开展数据分类分级工作，识别敏感数据	200	27.78%
购买并实施数据安全产品	142	19.72%
规划数据安全治理工作，制定安全工作实施路线图	123	17.08%
研究数据安全相关监管政策，进行风险评估，识别安全风险	110	15.28%
组建数据安全管理机构	72	10.00%
制定数据安全管理制度和流程	71	9.86%
其他	2	0.28%

AI赋能医院数据安全调查发现

调查目的及方法

近年来人工智能应用快速发展，AI既可以是“黑客”发现被攻击对象“漏洞”的工具，也可以用于防守武器，守护医院的数据资源。本次调研聚焦人工智能赋能医院数据安全的相关内容。从医院应用AI技术辅助数据安全管理工作的场景，到使用AI+数据安全产品时的关注点和挑战，以期为后续AI技术在数据安全应用等方面提供参考。

本次调研采用调研问卷的形式，针对全国部分医院信息技术部门负责人、数据安全建设维护及人工智能等相关管理人员开展了调查。

调查对象及范围

本次调研覆盖176家医疗机构。其中三级及以上医疗机构112家，占比最高，为63.64%；二级医疗机构22家，占比12.49%。详细数据见表3.5.2_1。

表3.5.2_1 参与调研的医院级别

医院级别	数量	比例[N=176]
三级甲等	87	49.43%
三级乙等	17	9.66%
三级其他	8	4.55%
二级甲等	14	7.95%
二级乙等	3	1.70%
二级其他	5	2.84%
一级或其他	42	23.86%

对参与调研的医院类型进行统计，综合医院129家，占调查样本数73.30%，专科医院34家，占调查样本数19.32%，详细数据见表3.5.2_2。

表3.5.2_2参与调研的医院类别

医院类别	数量	比例[N=176]
综合医院	129	73.30%
专科医院	34	19.32%
其他	13	7.39%

对参与调研的医院性质进行统计，公立医院174家，占调查样本数98.86%，非公立医院2家，占调查样本数1.14%，详细数据见表表3.5.2_3。

表3.5.2_3 参与调研的医院性质

医院性质	数量	比例[N=176]
公立医院	174	98.86%
非公立医院	2	1.14%

考虑应用AI技术辅助数据安全管理工作的场景

调研数据显示，在考虑应用AI技术辅助管理的数据安全场景中，47.16%的医疗机构选择“数据泄露防护”，46.59%选择“数据安全态势感知”，45.45%选择“异常行为监测”，位列前三位。详细数据见图3.5.3，表3.5.3。

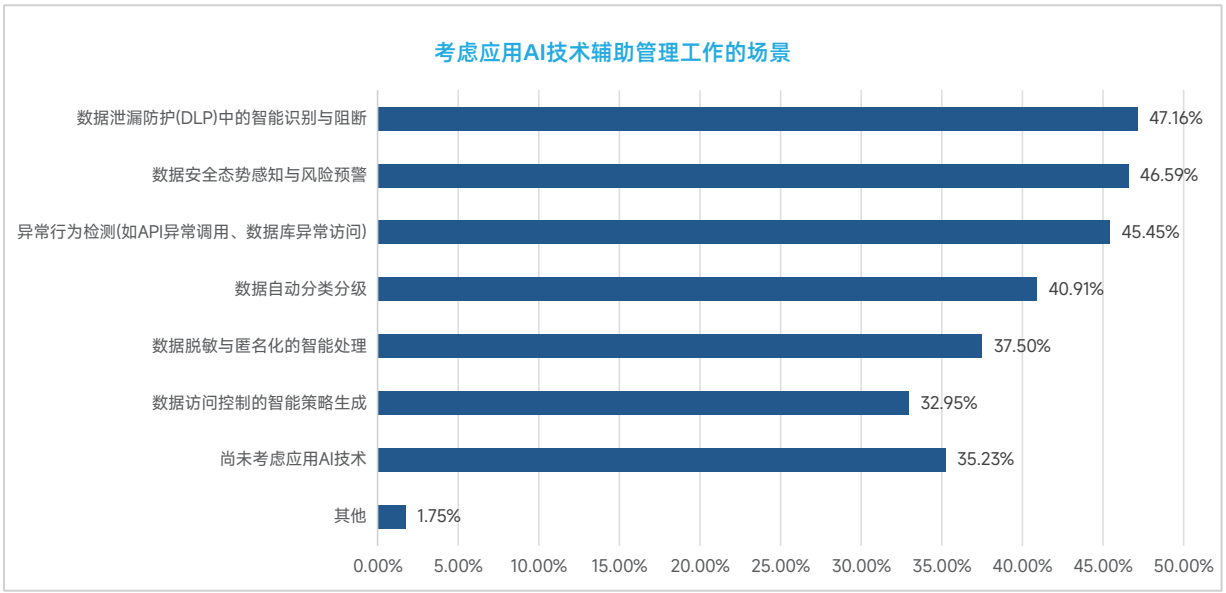

图3.5.3 考虑应用AI技术辅助管理工作的场景

表3.5.3 考虑应用AI技术辅助管理工作的场景

考虑应用AI技术辅助管理工作的场景	数量	比例[N=176]
数据泄漏防护(DLP)中的智能识别与阻断	83	47.16%
数据安全态势感知与风险预警	82	46.59%
异常行为检测(如API异常调用、数据库异常访问)	80	45.45%
数据自动分类分级	72	40.91%
数据脱敏与匿名化的智能处理	66	37.50%
数据访问控制的智能策略生成	58	32.95%
尚未考虑应用AI技术	62	35.23%
其他	3	1.75%

是否认为AI能有效提升主动防御能力

调研数据显示， 64.77%的医疗机构认为AI对提升主动防御能力具有积极作用，其中 26.70% 的机构认为AI能“显著提升”防御能力，38.07% 的机构认为AI“有一定帮助”。详细数据见图3.5.4，表3.5.4。

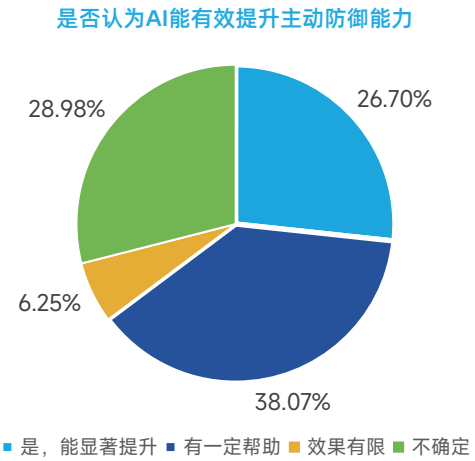

图3.5.4 是否认为AI能有效提升主动防御能力

表3.5.4 是否认为AI能有效提升主动防御能力

是否认为AI能有效提升主动防御能力	数量	比例[N=176]
是，能显著提升	47	26.70%
有一定帮助	67	38.07%
效果有限	11	6.25%
不确定	51	28.98%

是否考虑引入具备AI能力的数据安全功能模块

调研数据显示，医疗机构对引入具备AI能力的数据安全功能模块展现出极高的积极性，36家医疗机构已率先引用，占比20.45%，70家医疗机构正积极规划部署，占比39.77%。详细数据见图3.5.5，表3.5.5。

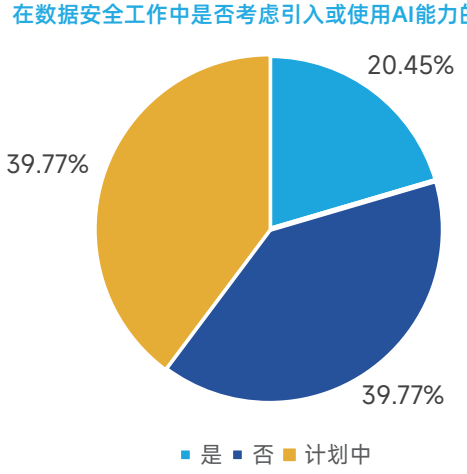

图3.5.5 是否已在考虑数据安全工作中引入或使用具备AI能力的功能模块

表3.5.5 是否已在考虑数据安全工作中引入或使用具备AI能力的功能模块

是否引入或使用具备AI能力的功能模块	数量	比例[N=176]
是	36	20.45%
否	70	39.77%
计划中	70	39.77%

AI具有较高应用价值的数据安全场景

调研数据显示，在AI技术应用价值较高的数据安全场景中，67.61%的医疗机构选择“数据库审计与异常行为监测”场景，65.34%的医疗机构选择“医疗数据资产梳理与识别”场景，64.77%的医疗机构选择“网络安全分析与研判”场景。反映出，医疗机构在推进AI+数据安全建设时，倾向于将AI技术应用于资产盘点、异常监测、泄露防护等主动防御场景，以构建更敏捷、精准的安全防线，应对复杂多变的网络与数据安全威胁。详细数据见图3.5.6，表3.5.6。

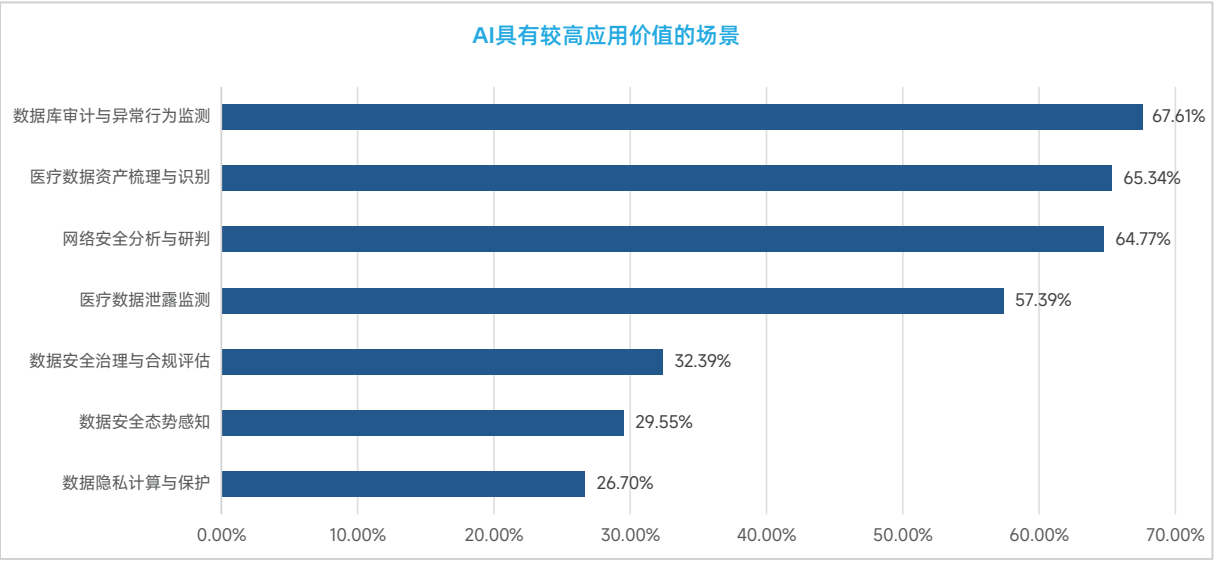

图3.5.6 AI技术在哪些数据安全场景中具有较高应用价值

表3.5.6 AI技术在哪些数据安全场景中具有较高应用价值

AI具有较高应用价值的场景	数量	比例[N=176]
数据库审计与异常行为监测	119	67.61%
医疗数据资产梳理与识别	115	65.34%
网络安全分析与研判	114	64.77%
医疗数据泄露监测	101	57.39%
数据安全治理与合规评估	57	32.39%
数据安全态势感知	52	29.55%
数据隐私计算与保护	47	26.70%

选择AI技术赋能数据安全产品时的关注点

调研数据显示，在选择AI赋能的数据安全产品时，44.89%的医疗机构关注“识别准确率与误报率”，34.09%的医疗机构看重“厂商的技术支持与更新能力”，27.84%的医疗机构关注“成本效益比”。这反映出，医疗机构在引入AI安全产品时，关注产品能否真正解决实际问题，且重视厂商的持续服务能力与投入产出比，力求在保障数据安全的同时实现资源的最优配置。详细数据见表3.5.7，表3.5.7。

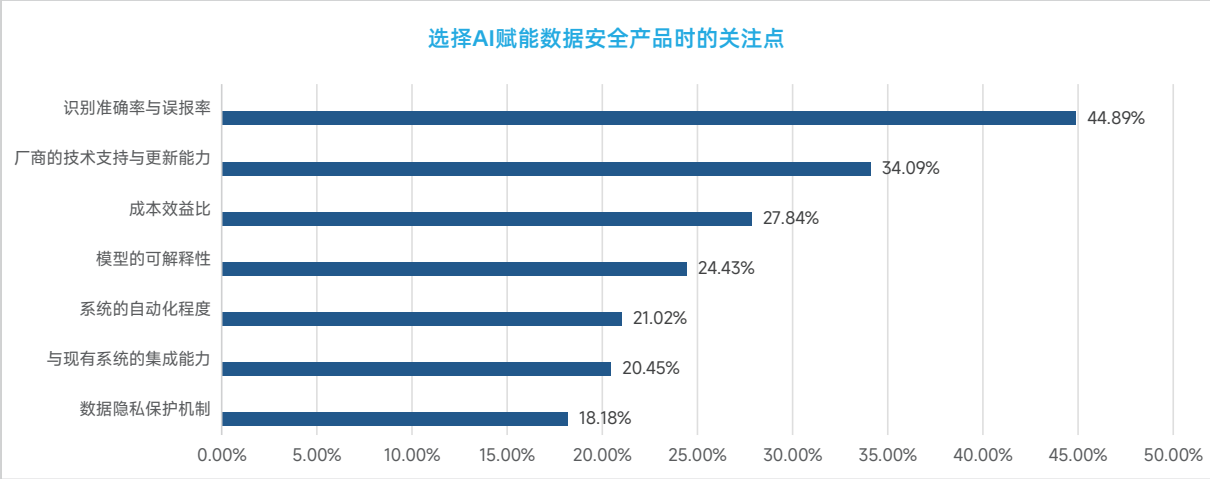

图3.5.7 选择AI赋能数据安全产品时的关注点

表3.5.7 选择AI赋能数据安全产品时的关注点

选择AI赋能数据安全产品时的关注点	数量	比例[N=176]
识别准确率与误报率	79	44.89%
厂商的技术支持与更新能力	59	34.09%
成本效益比	48	27.84%
模型的可解释性	42	24.43%
系统的自动化程度	36	21.02%
与现有系统的集成能力	35	20.45%
数据隐私保护机制	31	18.18%

使用AI+数据安全产品时遇到的主要挑战

调研数据显示，使用AI+数据安全产品遇到的主要挑战的调研中，93家医疗机构选择“缺乏专业人才进行运维与调优”，占比52.84%，73家医疗机构选择“尚未使用，无相关经验”，占比41.48%，71家医疗机构选择“成本过高”，占比40.34%。详细数据见图3.5.8，表3.5.8。

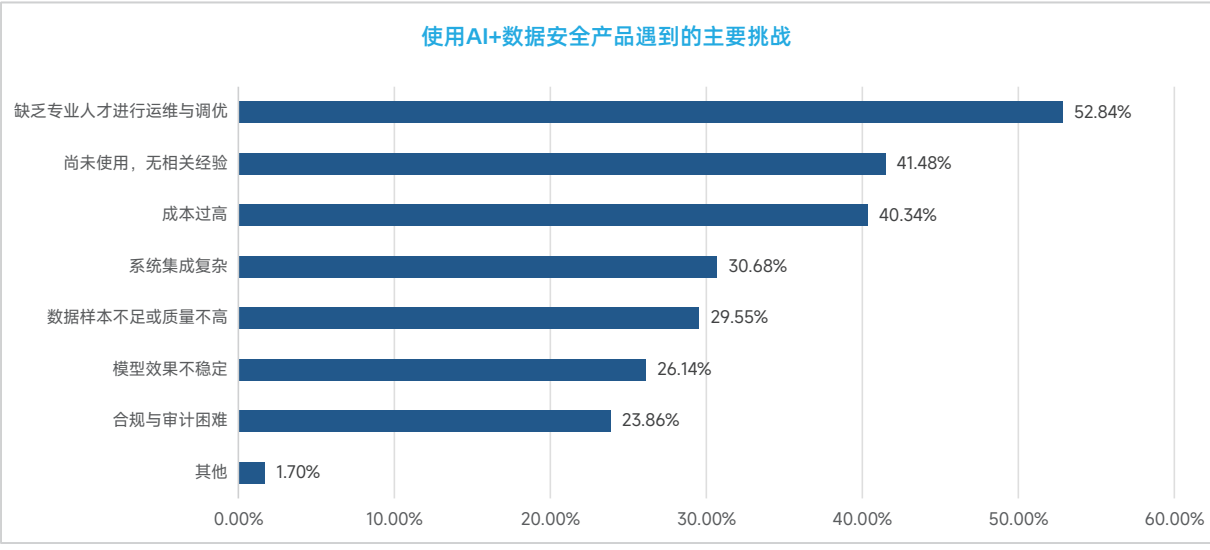

图3.5.8 使用AI+数据安全产品遇到的主要挑战

表3.5.8 使用AI+数据安全产品遇到的主要挑战

使用AI+数据安全产品遇到的主要挑战	数量	比例[N=176]
缺乏专业人才进行运维与调优	93	52.84%
尚未使用，无相关经验	73	41.48%
成本过高	71	40.34%
系统集成复杂	54	30.68%
数据样本不足或质量不高	52	29.55%
模型效果不稳定	46	26.14%
合规与审计困难	42	23.86%
其他	3	1.70%

未来是否会增加AI+数据安全产品的投入

调研数据显示，39.21%的医疗机构已明确或正在规划增加对AI+数据安全产品的投入，30.68%的医疗机构选择视政策与合规要求而定。详细数据见图3.5.9，表3.5.9。

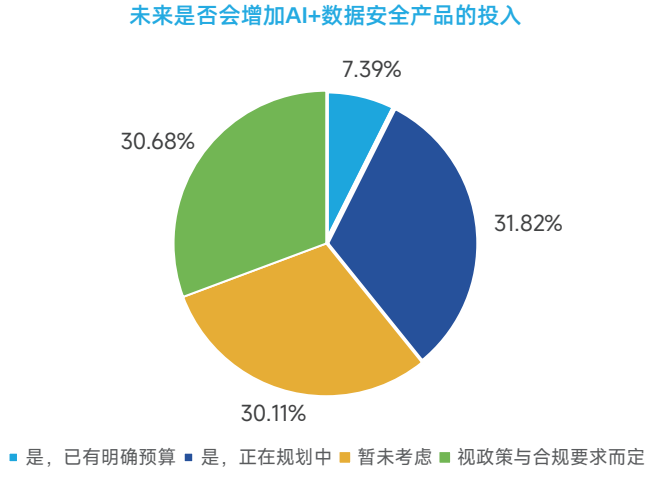

图3.5.9 是否计划在未来1-2年内增加对AI+数据安全产品的投入

表3.5.9 是否计划在未来1-2年内增加对AI+数据安全产品的投入

未来是否会增加AI+数据安全产品的投入	数量	比例[N=176]
是，已有明确预算	13	7.39%
是，正在规划中	56	31.82%
视政策与合规要求而定	54	30.68%
暂未考虑	53	30.11%

调查结果分析

安全管理制度需针对性细化

《网络安全法》《数据安全法》《个人信息保护法》相继发布，为我国数字经济发展建立了基本的法律和制度保障体系。但是，这些法律法规在医疗健康领域实施，还需要建立相应的标准细则和实施指南，以适应医疗健康领域中不同场景情况下，对数据安全和开放使用的许可和制约。例如：《个人信息保护法》提到的“个人敏感信息”内容的范围分类与定义，“最小数据范围”采集的原则与标准，“个人信息去标识化”的规范性要求和技术措施标准值等。此外，在“人工智能+医疗卫生”安全应用调研中，AI应用全流程安全管理制度尚不健全，第三方合作管理规范存在缺位，将进一步加剧医疗机构在AI应用中的合规与安全顾虑。

安全专业人才配置普遍短缺

受访医院认为《数据安全法》《个人信息保护法》对医院数据安全的影响主要集中在需加强数据安全能力建设（86.53%），要有专门的数据安全管理人员和相应的制度与流程（76.53%），要加强对数据的安全保护，购买数据安全相关产品（73.61%）。而在针对“医院在数据安全保护工作中存在的困难”的调研中，占比前三的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。

数据安全得到一定程度重视

2021年《数据安全法》和《个人信息保护法》相继出台，对数据安全和个人信息保护提出了新的要求。本次调查显示，97.5%的调查对象对此有所了解，并且70.14%的医院已经组织了学习了《数据安全法》和《个人信息保护法》。关于开展数据安全能力建设主要动力的前三位是：防范风险事件发生（83.75%），合规需求（77.08%）和保障业务运营（66.94%）。

近年来，CHIMA组织开展卫生健康行业网络安全技能大赛，模拟实战进行攻防演练，提升了行业从业人员专业技能水平。本次调查显示，医疗机构对AI驱动的动态防御（如异常行为监测67.61%、智能DLP 47.16%）展现出强烈需求，标志着安全防护正从“被动响应”向“主动感知”转型。

调查报告显示，近年来，医院对网络安全投入逐年增加。从调查中可以看出医院安全投入分布情况：数据库防火墙/网关是目前使用最多的数据安全保护措施，占比76.25%；其次是数据备份74.72%，第三是具备勒索病毒查杀能力的杀毒软件或终端管理软件，占比74.58%，防统方、数据访问控制、数据审计等数据安全防护手段也日益完备。

数据安全技术防护能力应进一步加强

卫生健康行业是处理数据最密集的行业之一，医疗健康数据的高价值与高风险并存。随着“互联网+医疗”、医学人工智能等新兴业态的快速发展，数据流转场景日益复杂，安全挑战也随之升级。调查显示，当前医疗机构的数据安全保障措施仍以基础合规为主，多数机构的安全防护水平停留在等保2.0的基础要求层面，缺乏针对医疗数据特性的专业化防护手段。数据库防火墙/网关是当前医院使用最广泛的数据安全防护手段，占比高达76.25%；针对医疗数据资产机密性保障的核心安全措施，数据加密技术的采用率为25.69%，数据脱敏技术的应用占比为19.58%。这反映出当前医疗数据安全防护存在结构性矛盾：基础防护措施已较为普及，但针对核心数据的分类分级、分级加密、动态脱敏、全生命周期监测等专业化手段尚未形成体系。

政策与管理建议

调查结果显现出医疗机构在人工智能时代下数据安全方面存在的问题、原因，以及对下一步安全管理工作的期望，随着人工智能技术在医疗领域的深度应用，医疗数据安全关系医疗行业高质量发展。根据本次调查揭示出的问题，以及对调查对象的意愿和诉求的整理，形成以下工作建议，供政府部门、行业组织、医院领导和技术服务企业参考。

加强政府引导，强化制度供给与监管智能

政府部门作为医疗数据安全的顶层设计者和监管主体，应在完善政策体系、强化监管执法、加大资源投入、促进数据流通等方面发挥主导作用，构建政府引导、多方协同的医疗数据安全治理格局。

一是健全标准规范体系。加快制定适应人工智能时代的医疗数据安全法规，明确人工智能在医疗数据采集、存储、传输、使用、销毁等全生命周期的安全要求。细化医疗数据分类分级指标，通过建立数据分类分级管理制度，构建医疗数据分类分级管控机制。

二是建立多部门联合执法机制。医疗数据安全涉及卫生健康、网信、公安等多个部门职责，建议建立跨部门协同执法机制，定期开展医疗数据安全专项检查行动，实现“以检促改、以改促升”，筑牢医疗数据安全防线。

三是加强数据安全风险监测预警。利用大数据分析与人工智能技术，构建医疗数据安全监测与预警机制，实现对医疗数据全生命周期的全天候实时监测与风险精准预警，变“被动防御”为“主动防控”。

细化行业标准，推动标准共建与能力共享

不同医疗机构在技术能力、资源投入、管理成熟度上存在显著差异，单靠各自为政、分散建设的方式，难以形成统一、有效、可持续的安全防护网。因此，行业主管部门亟需发挥顶层设计和统筹协调的作用，在标准落地、经验推广、能力建设等方面发挥积极作用，构建起一个多方参与、成果共享的新生态。

第一，组织医疗机构、技术企业、专家学者等各方力量，共同制定人工智能时代下医疗数据安全相关行业标准、团体标准的研制工作，推动标准更加贴合医疗实际。建立政策解读机制，帮助医疗机构准确理解政策要求，避免执行偏差。

第二，与行业协会合作，推动医疗数据安全行业/团体标准落地试点与推广，组织有条件的医疗机构开展医疗数据分类分级、数据安全评估等标准的试点应用工作，总结试点经验，形成可复制、可推广的实施路径，为其他医疗机构提供工作参考与操作指引。

第三，联合高等院校、行业协会、医疗机构等开发医疗数据安全培训课程体系，覆盖政策法规、技术标准、实操技能等内容。推动将数据安全培训纳入医护人员继续教育学分体系，提高参与积极性。

落实主体责任，提升数据安全治理能力

医疗机构是医疗数据安全的第一责任人，应切实承担主体责任，将人工智能技术深度融入自身的数据安全治理体系，完善管理机制，筑牢数据安全防线。结合调查内容，建议医疗机构从以下四个方面重点加强数据安全建设：

一是加强数据安全组织与管理。及时开展医疗数据资源的统筹管理和安全评估工作，明确管理职责，避免出现安全管理真空。

二是加强内部规划与评估。结合自身安全风险弱点，制定科学的数据安全建设规划，有计划地落实资金投入，稳步提升安全防护能力。

三是完善数据安全技术防护体系，将人工智能技术融入医疗数据全生命周期安全防护，采取加密存储、访问控制、脱敏展示、行为监测等技术措施，形成覆盖数据采集、存储、使用、共享、销毁全生命周期的安全防护体系。

四是构建最小权限访问机制，根据岗位职责精细划分数据访问权限，杜绝"过度授权"和"特权账户"，建立权限审批和定期复核机制，确保数据访问权限始终符合业务需求。

五是强化全员安全意识培训。将数据安全培训纳入医护人员、行政人员、外包人员的入职培训和年度培训必修内容。采用案例分析、场景模拟、考核测试等多种形式，提升培训效果。

推动数据安全技术创新，满足医疗机构多样化需求

医院数据安全技术提供商需以技术创新为核心驱动力，打造贴合医疗场景的解决方案，为医疗机构提供优质高效的技术服务。

一方面积极探索人工智能（AI）技术在数据安全领域的深度应用，重点围绕安全认证与授权、数据脱敏、数据分类分级、链路加密、数据备份及态势感知等关键环节，通过AI技术赋能，研发适配医院业务模式创新的新型安全产品，以技术创新破解安全瓶颈。

另一方面提供端到端的解决方案，技术服务企业深入研究医疗行业业务流程、数据特征和合规要求，准确把握医疗机构在数据安全方面的真实需求和痛点，开发差异化的安全能力，提升解决方案的行业适配性。

CHIMA

CHIMA官方微信公众号