Lenovo NetApp | HC3i.cn 数字医疗网

医院核心信息系统数据安全与数据管理

调研报告

（2021-2022年度）

公开版

Contents

目录

Introduction
前言

为深入了解我国医院核心信息系统安全建设现状及医疗数据应用的进展、真实反映医疗行业在信息系统安全和数据应用与数据管理方面的需求，HC3i数字医疗网联合联想凌拓科技有限公司，围绕“医院信息安全建设的基本情况”、“医院核心信息系统安全建设现状（以HIS、PACS为主）”、“医院数据应用与安全防护状况”等重点方向，特展开为期数月的行业调研工作。

本次调研报告全文共包含四个部分、十四个章节，主要依据调研所涉及的有关医院信息安全建设中的部分核心问题，展开重点说明和讨论。调研数据主要来源于医院信息化主管、医院信息化高级工程师为主的医院信息化建设骨干人群。调查内容涵盖了医院核心信息系统安全建设、医疗数据应用等发展情况的客观数据，并结合专家观点和媒体分析对当前医疗信息化建设所面临的挑战和发展趋势进行研判，以此充分展现我国医疗行业在系统和数据两大方向上的发展现状和前行方向，并为广大医疗信息化建设者提供价值性参考、满足医院和HIT厂商 （HIT全称为：Healthcare Information Technology，具体指代医疗信息化），开展相关信息化项目建设和解决方案的设计研发等工作需求。

· 调研样本描述

本次调研采用HC3i媒体平台公开发布、调研对象自愿填写的方式。截至调研活动结束，共收到问卷反馈351份，其中包含有效答卷314份。(问卷填写完整、同一家医院无重复联系人提交、问卷无明显误答，即判定为有效问卷)。

以上314份(有效)问卷的所属医院均无重复和关联。全部问卷中，没有针对全部调研问题给出完整应答，但所回答部分，超过问卷内容的70%的样本，计入有效数据进行统计。(填写缺失的问卷部分，按照统计学常规的Missing Value进行处理)。

· 版权申明

· 阅读申明

本次调研结果的原始数据均来自于主动给予应答的医院，最终样本未经过严格分层，遵循随机抽样原则，完成样本的抽取工作。因此样本分布存在一定偏态分布，故调查结果仅作为医院信息化发展的参考文献。欢迎广大医疗信息化建设同仁，对于本报告存在的缺陷和不足，给予客观建议，我们将在今后的工作中持续改进，谢谢。

· 撰写说明

本报告数据来源，来自HC3i数字医疗网联合联想凌拓科技有限公司，共同发起的“医院核心信息系统数据安全与数据管理调研活动”。

报告内容，经专家顾问团围绕调研核心内容进行研讨、分析后，由HC3i数字医疗网内容团队，基于专家研讨结果和观点，结合当前政策法规，参考调研基础数据进行撰写，并由专家顾问组进行最终核定。

【专家顾问组名单】

顾问组组长

傅昊阳 | 广东省中医院信息处处长

衡反修 | 北京大学肿瘤医院信息部主任

顾问组组员

包国峰 | 山东第一医科大学附属省立医院信网办副主任

史亚香 | 东南大学附属中大医院信息化建设总工程师

田宗梅 | 首都医科大学附属北京世纪坛医院信息中心主任

王力华 | 首都医科大学附属北京友谊医院信息中心主任

徐红兵 | 安徽医科大学第一附属医院医疗大数据办公室主任

谢颖夫 | 云南省第一人民医院信息中心主任

赵前前 | 首都医科大学附属北京朝阳医院信息中心副主任

左秀然 | 武汉市中心医院信息中心主任

* 按姓名首字母排序

01

调研样本及信息安全建设基本情况

1.1 调研样本描述

为深度了解医疗信息安全建设进程、明晰后续发展要点、为行业提供更多价值借鉴，本次调研将医院信息化建设核心工作者作为调研主体，面向全国不同区域、不同级别、不同类型的医疗机构信息中心管理者及技术骨干，展开全面调研。

1.2 参与调研医院行政区域分布特点描述

当前，由于区域经济发展不均衡等因素，医院信息化建设程度依然呈现参差不齐的现状。为帮助读者更加直观、全面地了解不同经济发展程度下，医院核心系统数据安全与数据管理的建设差异，本报告将各地区经济发达程度进行分层，并对参与调研医院所在地区的经济分布情况进行了统计归纳。

从地区划分来看，本次调研所包含的样本所属区域，覆盖了除香港特别行政区、澳门特别行政区以及台湾省、西藏自治区以外的30个行政区。报告参照《2021中国统计年鉴》中各省市地区的2020年人均GDP，按GDP≥72000，72000＞GDP≥54000，GDP＜54000将各地区经济发展程度分为经济发达地区、经济中等发达地区、经济欠发达地区三层[1]。其中，经济发达地区的样本量占41.35%、经济中等发达地区占49.27%、经济欠发达地区占9.38%。(如图1.2)

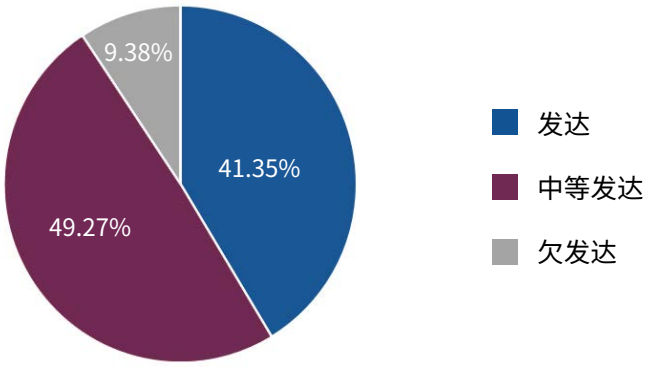


图1.2 参与调研医院所在区域经济发展情况

[1] 分层方法说明

参考《2021中国统计年鉴》中的人均国内生产总值和人均地区生产总值，将人均地区生产总值大于人均国内生产总值的地区划分为发达地区，人均地区生产总值介于人均地区生产总值最低值与人均国内生产总值的平均值之间的地区划分为中等发达地区，剩余地区划分为经济欠发达地区。

1.3 参与调研医院级别情况

根据原卫生部《医院分级管理办法》[2]，医院依其功能、任务、设施条件、技术建设、医疗服务质量和科学管理的综合水平，自高向低分为三级医院、二级医院、一级医院与其他。本报告中将参与调查医院，分为三级医院与三级以下医院两部分。

从参与调研的医院等级来看，本次调研样本中，三级医院数量为199，约占总量的63.40%；三级以下医院数量为115，约占总量的36.60%。（如图1.3）

1.4 医院信息安全建设情况

科技发展驱动互联网医疗、分级诊疗、医联体建设等工作持续推进，医院信息系统逐渐从封闭、隔离的院内网络架构，向开放的互联网体系融合，也成为医院业务和管理工作等诸多方面的核心支撑，保障系统安全，不仅是医院业务高效运行的前提，更是支撑医院高质量发展的关键。

> 所谓核心系统，其实就是影响到医院医疗秩序的最核心的系统，那么核心系统的信息安全也必然是医院非常非常关注的问题。
>
> —— 衡反修
>
> 北京大学肿瘤医院信息部主任

在这样的发展态势下，医院信息系统必然面临更多新挑战：一方面，在互联互通标准化成熟度测评、电子病历应用等级评价管理办法及评价标准、网络安全等级保护建设要求等法规和标准的指引下，原有医院信息系统的功能不断完善，应用水平不断深入，系统复杂度不断提高；另一方面，信息化应用场景不断丰富，使得新系统覆盖的范围进一步扩大，加之物联网应用在医院内部日益普及，各类终端设备种类纷繁复杂，为医院信息安全建设带来新的要求。

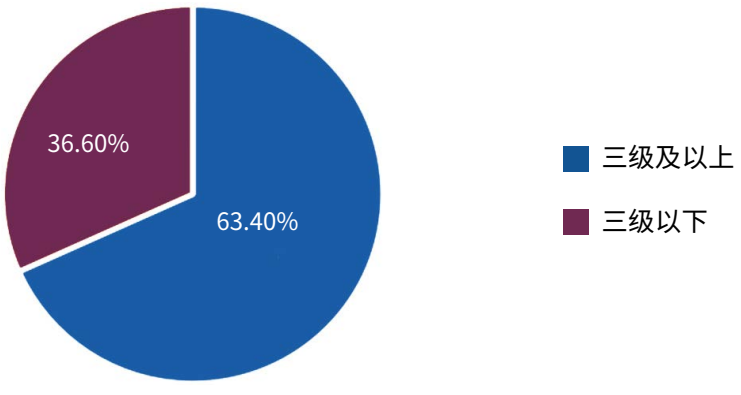


图1.3 参与调研医院级别分布情况

[2]《医院分级管理办法》

《医院分级管理办法》（中华人民共和国卫生部1989年11月29日），对医院分级管理的依据是医院的功能、任务、设施条件、技术建设、医疗服务质量和科学管理的综合水平。医院分级管理的实质是照现代医院管理的原理，遵照医疗卫生服务工作的科学规律与特点所实行的医院标准化管理和目标管理。由卫生行政部门按地方政府的区域卫生规划来统一规划确定。

在医院信息系统安全建设的重要性日益凸显的当前，如何应对不断丰富的应用场景带来的安全建设挑战，已经成为当前医疗信息化建设过程中的重要任务，构建更加完善的信息安全体系，也已经成为医院信息化建设者们所关注的重要话题。

「HC3i新医观点」

科技赋能医疗行业发展，医院信息系统覆盖的范围不断扩张，各类应用程度不断加深，医疗数据价值持续被挖掘，此现状下，保障医院信息安全成为医院高质量发展过程中不容忽视的一项重要任务。

1.4.1 医院信息系统三级等保建设情况

为突破空间局限、缓解疫情特殊时期就医挑战等客观问题，互联网诊疗迎来快速发展新阶段。由于医疗行业数据价值高、医院服务社会影响面广，容易成为不法分子谋取利益的攻击对象，因此医院遭受网络攻击的频次也在快速增长。目前，医院面临的网络安全风险以勒索病毒、恶意攻击等为主，上述安全威胁事件一旦发生，将严重影响医院业务的正常运行，该影响将随着医院信息化建设者知晓网络安全风险时间的时间早晚，有不等层级的业务影响度；同时，医院医疗数据泄露事件频发，也会让医院面临很多法律法规的合规风险。

在信息安全威胁频现的当下，以评促建、以评促改，

「HC3i新医观点」

互联网诊疗在旺盛需求下迎来迅速发展，同时也为信息技术深入行业按下“加速键”，此过程中，医院网络攻击数量快速增长，医院亟待高效的信息安全保障解决方案出现。

通过评级标准指明医院信息系统的底层架构和功能性要求，往往是最直接有效的方式。正因如此，等级保护测评将医疗行业划定为重点对象。

2018年7月，国家卫生健康委员会、国家中医药管理局印发《互联网医院管理办法（试行）》[3]，第三章第十五条提出“互联网医院信息系统按照国家有关法律和规定，实施第三级信息安全等级保护。”该规定将医院信息化建设与安全建设进行了紧密关联，等级保护建设成为互联网医院上线的必要条件；

目前，多数三甲医院的HIS、LIS、PACS、EMR等关键系统的等保定级为三级。根据《信息系统安全等级保护基本要求》[4]，三级等保的测评内容涵盖等级保护安全技术要求的5个层面和安全管理要求的5个层面，包含信息保护、安全审计、通信保密等在内的近300项要求，共涉及测评分类73类。

[3]《互联网医院管理办法（试行）》
《互联网医院管理办法（试行）》由国家卫生健康委员会、国家中医药管理局于2018年7月17日印发的文件，共五章三十六条，自发布之日起施行。

[4]《信息系统安全等级保护基本要求》
《信息安全技术 信息系统安全等级保护基本要求(GB/T 22239-2008)》由公安部和全国信息安全标准化技术委员会提出、由全国信息安全标准化技术委员会归口，起草单位为公安部信息安全等级保护评估中心。该标准已由《信息安全技术 网络安全等级保护基本要求（GBT22239-2019）》替代，《信息安全技术 网络安全等级保护基本要求（GBT22239-2019）》于2019年12月1日起实施。

在参与本次调研的医院中，约有77.7%的医院HIS系统已通过等保三级。PACS和EMR通过等保三级的比例稍有降低，但比例均超过半数。数据显示，除了HIS、PACS、EMR核心信息系统，还有近三成的医院其他系统通过了三级等保。（如图1.4.1）

现状表明，当前医院三级等保建设程度不断加深，以HIS、PACS、EMR为代表的核心信息系统三级等保建设进程正在不断加快，医院的信息安全防护意识不断提升。

「HC3i新医观点」

当前医院三级等保建设程度不断加深，以HIS、PACS、EMR为代表的核心信息系统三级等保建设进程正在不断加快，医院的信息安全防护意识不断提升。

1.4.2 电子病历数据安全要求

病历是医院重要的资产：它不仅能够真实反映患者病情，还可以直接反映医院医疗质量、学术水平及管理水平；是开展医疗、教学、科研等多方工作极其宝贵的基础资料，为医院管理水平提供不可缺少的医疗信息；同时，在医疗保险中，病历是相关医疗付费的凭据。

2018年7月，中华人民共和国国务院发布《医疗纠纷预防和处理条例》[5]，其中明确指出，患者有权查阅、复制其门诊病历、住院日志、体温单、医嘱单、化验单(检验报告)、医学影像检查资料、特殊检查同意书、手术同意书、手术及麻醉记录、病理资料、护理记录、医疗费用以及国务院卫生主管部门规定的其他属于病历的全部资料。因此，在涉

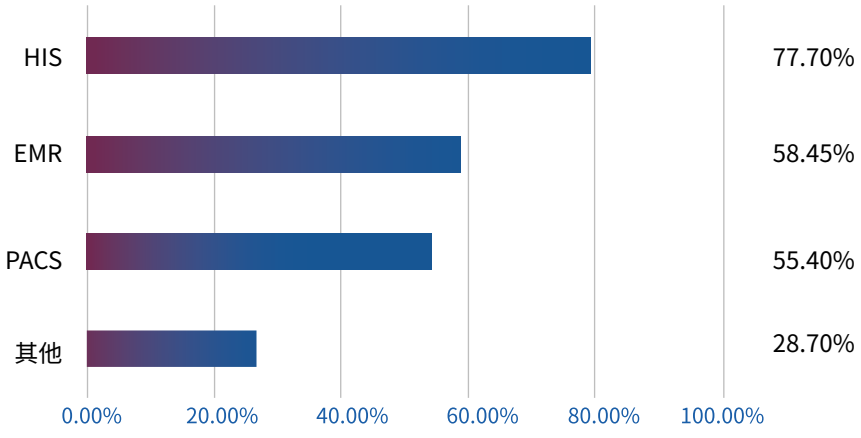


图1.4.1 医院核心系统信息安全等级保护建设情况

[5]《医疗纠纷预防和处理条例》

《医疗纠纷预防和处理条例》是为了将医疗纠纷预防和处理工作全面纳入法治化轨道，保护医患双方合法权益，维护医疗秩序，保障医疗安全而制定的法规。经2018年6月20日国务院第13次常务会议通过，2018年7月31日公布，自2018年10月1日起施行。

及医疗争议时，病历还是判定法律责任的重要依据。

随着信息技术的快速发展，电子病历（EMR）诞生并快速投入应用。它作为医院信息系统的核心部分，对提高医疗质量管理、提高病历的规范性和完整性、病人信息的整理与共享、加强医疗质量的监督、减轻医生的工作量、提高医务人员工作效率等方面具有十分重要的价值。

在2017年发布的《电子病历应用管理规范（试行）》[6]第19条中明确规定，门（急）诊电子病历由医疗机构保管的，保存时间自患者最后一次就诊之日起不少于15年；住院电子病历保存时间自患者最后一次出院之日起不少于30年。在政策法规的要求下，医院需要通过高质高效的方式对电子病历进行保存。

经了解，当前医院最为常见的电子病历保存方式有电子病历和纸质病历同步归档、离线存储介质长期保存、在线存储介质长期保存等。调研显示，目前采用电子病历和纸质病历同步归档方式进行长期保存的医院占比最多，还有不少医院则选择通过在线存储介质长期保存的方式。（如图1.4.2）

离线存储介质以磁带为主，在线存储介质以本地存储系统为主。电子病历长期保存，对于存储介质的可靠性，提出了很高的要求。

1.4.3 防范勒索攻击等安全防护解决方案的部署情况

随着科技与医疗行业的加速融合，医疗数据量快速攀升。而医疗数据价值高、医疗行业信息化起步时间晚、医院安全防护能力不足、医院各系统相对独立等客观情况广泛存在，同时由于医疗服务面对公

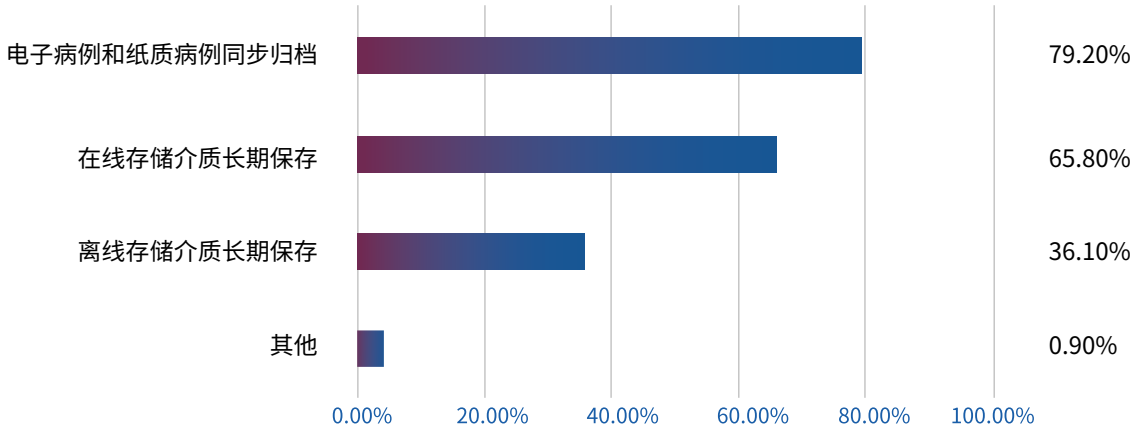


图1.4.2　医院电子病历数据长期保存

[6]《电子病历应用管理规范（试行）》
电子病历基本规范（试行）是二〇一〇年二月二十二日卫生部发布的文件。2017年4月1日，《电子病历应用管理规范（试行）》施行，《电子病历基本规范（试行）》同时废止。

众，暴露面风险也比较大，导致以医院为代表的医疗机构成为不法分子入侵的重灾区，针对医院的网络安全风险和网络攻击也呈现出持续上升的态势。

在勒索病毒攻击频发的现状下，医疗行业开始重视医疗信息安全建设，并开始摸索和推进各种安全防护措施，以确保医疗系统的信息安全。在参与调研的医院中，约七成医院均已进行防勒索病毒攻击等系统安全防护解决方案的部署工作。(如图1.4.3)

目前，勒索病毒的防范主要包含以下两方面内容：
第一，是通过增强网络安全防护能力，来提升抵御黑客攻击的能力；
第二，是通过提高医院数据保护能力，有效将医院网络安全防护屏障因黑客攻击所造成的损失，降低至可接受的程度。

但随着勒索事件的频发和勒索病毒的“进化”，医院在面对勒索病毒攻击时，应该具备更全面的防御措施。

首先，由于医院所遭受的勒索病毒攻击背后，往往是黑客的人为操作，因此，面对有固定目标的黑客攻击，基础的防御措施很难起到决定性效果；第二，当黑客实现对医院 IT 系统的侵入后，会继续进行潜伏和渗透，该阶段中，黑客往往会利用“零日漏洞(0 Day)”从操作系统和应用程序底层发起定时攻击，而“零日漏洞(0 Day)”通常是操作系统和应用程序厂商尚未发现的系统漏洞，因而无法进行严密、有效的防范；第三，黑客在进行攻击时，会特意选定医院数据保护系统，因为该保护系统涉及了数据备份系统、应用容灾系统、持续数据保护系统，能够达到攻击效果的最大化。

综上所述，在网络安全威胁频现、攻击手段快速变换的当下，备份数据安全保障的重要性远超以往。这就要求保存备份数据的存储系统本身，具有难以被黑客攻击的封闭性，能够从硬件级别，为备份数据提供足够的数据安全性保障。

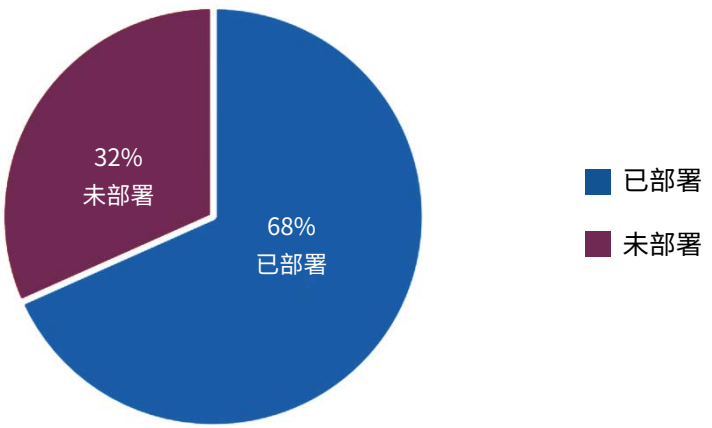


图1.4.3 防勒索攻击等系统安全防护解决方案的部署统计图

「HC3i新医观点」

在勒索病毒攻击频发的现状下，医疗行业开始重视医疗信息安全建设，并开始摸索和推进各种安全防护措施，以确保医疗系统的信息安全。

1.4.4《关键信息基础设施安全保护条例》要求落实情况

2021年8月《关键信息基础设施安全保护条例》[7]（以下简称《关基保条例》）正式发布，于2021年9月1日起开始实行。《关基保条例》从我国国情出发，明确了关键信息基础设施的定义和认定程序：一是明确关键信息基础设施的定义；二是明确关键信息基础设施所在行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门；三是明确由保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并组织认定本行业、本领域的关键信息基础设施；四是规定关键信息基础设施发生较大变化，可能影响其认定结果时，运营者应当及时报告保护工作部门，由保护工作部门重新认定。

《关基保条例》的另一项重大意义，在于强调“运营者的主体责任”（即“责任到人”），通过“同步规划、同步建设、同步使用”的条例内容，要求“运营者主体”在完善关键信息基础设施建设的同时，同步完成网络安全措施的部署和实施。在《关基保条例》第 39 条中明确规定，对于违反《关基保条例》指定情形之一的运营者，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。目前，医疗行业总体处于“较大风险”级别，存在多种网络安全风险及大量可被利用的安全隐患，安全防护能力较弱。报告显示，医疗行业网络安全面临四大风险：资产脆弱性风险、僵木蠕等病毒风险、漏洞风险、网站篡改风险。因此，通过开展多项有效措施，加速落实《关基保条例》至关重要。

调研数据显示，为进一步满足《关基保条例》要求，医院正在不断健全安全保护机制、完善管理部门设置，并通过优先采购安全可信的网络产品和服务、对关键岗位人员进行审查等方式，来提升关键信息基础设施安全防护能力。（如图1.4.4）

从调研结果来看，医院对于信息安全建设的重视程度在不断增加，与此同时，相关政策和法律法规的不断完善，对医疗行业信息安全建设起到也起到积极推动作用。

[7]《关键信息基础设施安全保护条例》
2021年4月27日，经国务院第133次常务会议通过，2021年7月30日，国务院总理李克强签署中华人民共和国国务院令第745号，公布《关键信息基础设施安全保护条例》，自2021年9月1日起施行。

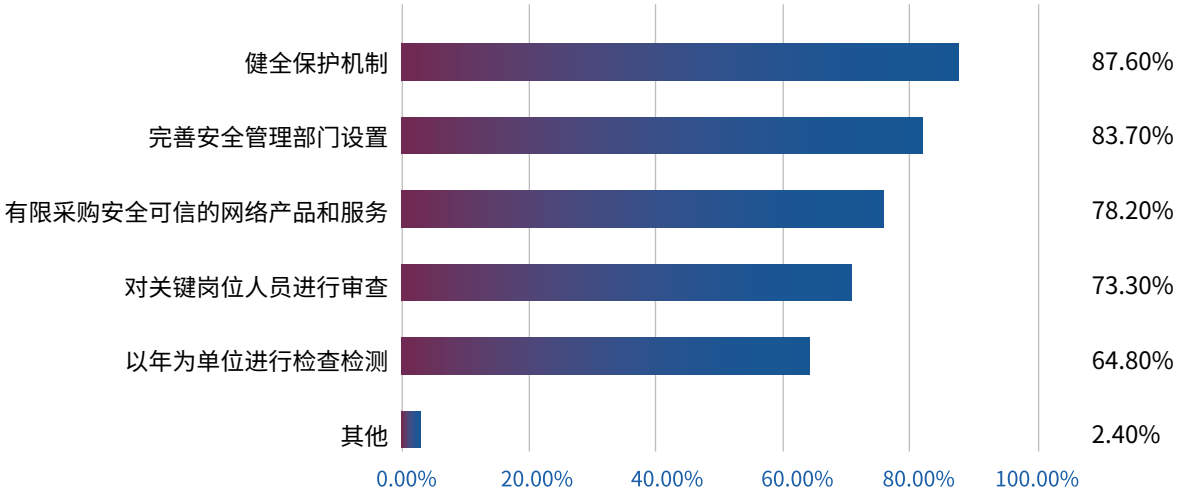


图1.4.4 医院关于落实《关基保条例》的实施措施

02

医院核心信息系统安全建设状况

2.1 医院核心信息系统容灾建设标准与常规技术方案

医院核心业务系统容灾架构的传统建设体系，通常存在容灾子系统彼此割裂的现状。一方面，这会使得医院容灾系统建设资金投入高、容灾系统架构复杂、运维难度大；另一方面，由于医院业务系统多且复杂、数据量大，传统数据备份体系很难满足医院海量数据高效备份业务需求，因而在面对需要数据回滚的容灾业务场景时，医院核心系统的数据恢复时间、业务恢复时间、容灾系统性能供给，难以得到有效保障。

为满足不断攀升的人民健康需求，互联网医院、多院区医院、医联体等医疗新模式在新兴信息技术的推动下，迎来快速发展时期。当信息化建设逐渐走向医院发展的中心位，稳定高效的信息系统已经成为医院走上高质量发展道路的必要条件，如何避免业务中断、数据丢失，也早已成为医院发展进程中的重要保障。

国家卫生健康委员会于2018年4月颁布的《全国医院信息化建设标准与规范（试行）》[8]（以下简称《建设规范》）中第73条“数据备份与恢复”中，强调了医院的数据备份系统需要“具有存储磁盘阵列和存储备份软件等2个组件，支持使用数据快照、同异步数据复制等2种相关技术”；《建设规范》中第74条“应用容灾”，提到了“具有应用服务器、数据库服务器、存储磁盘阵列、集群软件和应用容灾软件等5个组件”、“支持使用集群、负载均衡等2种相关技术”。这些组件和技术的融合部署，为医院核心业务系统的备份、容灾一体化建设，从技术架构方面，提供了良好的参考依据。

事实证明，将备份系统、容灾系统有机融合，能够在容灾系统遭受勒索病毒攻击的时候，利用存储备份软件无需数据还原过程的技术特性，将备份数据直接提供给容灾系统，实现医院核心业务应用的快速容灾恢复。

在容灾系统的规划设计中，医院应该根据不同业务系统的重要程度、依照《建设规范》的要求，确定各个业务系统数据备份与恢复所需要的RTO（恢复时间目标）和RPO（复原点目标），并充分

[8]《全国医院信息化建设标准与规范（试行）》
2018年，4月13日，国家卫生健康委员会发布《全国医院信息化建设标准与规范（试行）》。这是继2016年《医院信息平台应用功能指引》和2017年《医院信息建设应用技术指引》之后，出台的又一个医院信息化建设国家级标准。

考虑诸如勒索病毒攻击等数据逻辑性错误场景下，不同容灾技术实现方式、所提供的医院核心数据和核心系统恢复时间，能否满足医院业务连续性保障要求、数据安全性保障要求以及法律合规的要求。

核心业务系统备份、容灾一体化架构，能够帮助医院在核心系统发生灾难性故障（特别是需要将数据回滚到较早的数据备份时间点的时候），借助硬件技术的帮助，利用存储备份软件快速还原备份数据，从而恢复医院核心业务系统，并通过存储磁盘阵列为容灾业务系统的顺畅运行提供足够的性能支撑。

目前，医院的容灾建设的实现方式主要包括硬件双活、应用双活、数据容灾、应用容灾、持续数据保护（CDP）、数据备份等技术。

1、双活技术（包括硬件双活、应用双活）：

通过数据的实时复制和自动切换，能够有效防范硬件灾难性故障，但是无法有效应对误操作、勒索病毒攻击等数据逻辑性故障。

2、数据容灾和应用容灾：

以实时或异步方式提供数据复制服务，并在灾难发生时通过手动切换来提供业务连续性保障。与双活技术类似，依然无法有效应对数据逻辑性故障，因为数据采用实时复制或尽可能短时间间隔的异步复制方式，很难及时发现和阻止错误数据从生产系统蔓延到容灾系统。

3、持续数据保护（CDP）：

SNIA（全球网络存储工业协会）定义了三种级别的持续数据保护实现方式：应用程序级、文件级、数据块级。CDP提供了更细粒度的持续数据保护能力，在某种意义上是数据备份的一种良好补充。然而，CDP并不能够取代数据备份，主要原因在于CDP很难以可以接受的成本提供更大时间尺度范围的数据保护，同时，文件级CDP和数据块级CDP无法提供应用一致性保障——即无法保护应用服务器内存中的数据，因而有可能导致恢复的数据无法使用。

4、数据备份：

数据备份是确保数据安全的最后一道防线。数据备份软件在执行数据备份操作的时候，必须提供应用一致性保障，以确保备份数据的完整性。此外，灾备演练是确保备份数据安全的最后一道防线。定期的灾备演练，既能验证备份数据的可用性，也能够提高运维人员的操作熟练度，在灾难性故障发生的时候，提高数据恢复的操作效率。

2.1.1 HIS系统容灾部署情况

随着医院信息化程度的不断深化，HIS作为医院的核心业务系统，涵盖了包含挂号、收费、门诊管理、住院管理、医生站、护士站、EMR、LIS、RIS、PACS、耗材管理等方方面面。

当前阶段，HIS系统仍在随着医院业务的不断丰富、信息技术的不断改进而持续完善。医院谋求

未来发展的过程中，正在不断探索更多行之有效的措施，实现建立牢固信息化保障体系的目标。

在参与本次调研的医院中，绝大多数的医院已经进行了院内容灾系统的部署工作，部署同城容灾和异地容灾系统的医院也有一定比例；在参与调研的医院中，仅有少数医院目前尚未部署容灾系统。（如图2.1.1）

2.1.2 PACS系统容灾部署情况

当前，医学影像作为医院开展临床、科研等多方工作的重要工具，不仅在构建全生命周期的健康服务中发挥着巨大作用，更为全面提升医疗健康水平提供了有力支撑。而通过PACS系统，能够在有效节省胶片费用和存储空间的同时，帮助医生更加便捷高效的获取到患者的影像病历资料，大幅缩短患者就诊时间，让患者影像资料能够以数据形式进行传输，从而达到降本增效的目标。

正由于PACS系统所承载的海量数据和所承担的重要责任，为PACS系统部署容灾系统的重要性不言而喻。本次调研显示，绝大多数的医院已针对PACS系统部署了院内容灾系统；一定比例的医院针对PACS系统进行了异地容灾和同城容灾部署；仍有部分医院尚未针对PACS进行容灾部署。（如图2.1.2）

2.2 医院核心系统主要安全威胁与挑战

当前，医院核心系统的安全问题可以主要概括为三个方向，其一是业务连续性保障、其二是数据安全性保障，其三是法律合规要求。系统的中断会给医院造成严重影响。

目前，医院的信息系统普遍存在的问题尚有很多。有关安全制度覆盖场景不全、执行不到位；缺少专职专业安全管理人员、人员误操作和第三方人员流动性带来的系统和数据风险；安全防护测试执行问题、弱口令问题；安全监管落实不到位；数据安全管控不足，相关的数据库审计和监管等管理工作有缺失、系统运行环境因素（如机房温

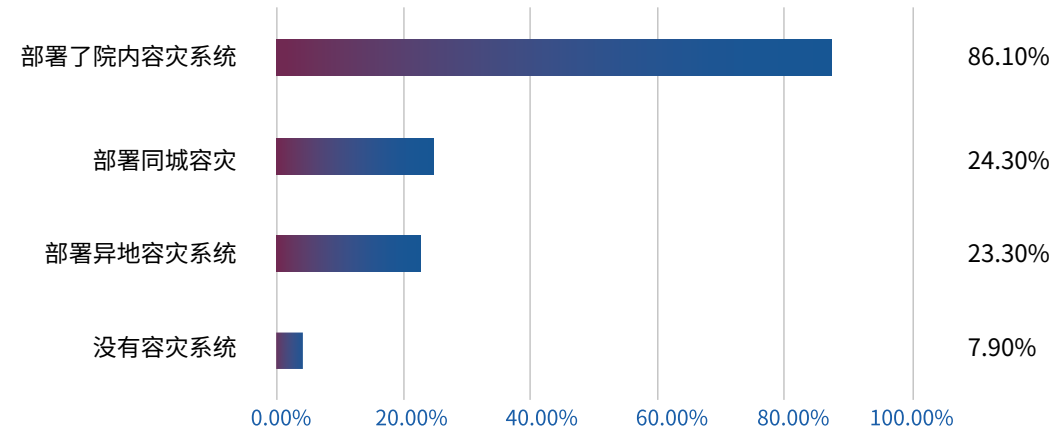


图2.1.1 医院 HIS 系统容灾部署情况

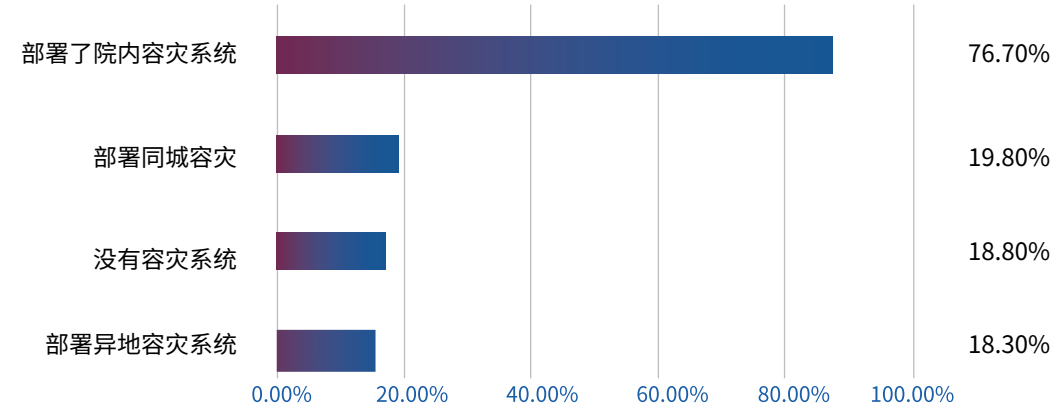


图2.1.2　医院 PACS 系统容灾部署情况

度、系统空间等）、系统升级或变更发布未经全面测试、无法全面满足国家有关法律法规要求等，均为目前医院核心系统中较为常见的安全问题。

> 很多时候，安全是两面的，防护固然重要，但与效率如何平衡，也同样重要，这需要我们进一步关注和完善安全的相关策略。
>
> —— 衡反修
>
> 北京大学肿瘤医院信息部主任

2.2.1 现阶段HIS系统主要威胁

经调研发现，现阶段医院HIS系统常见的核心挑战包括数据库故障，服务器、存储等硬件故障，计算机病毒或黑客攻击，人为误操作、网络安全漏洞等。在参与调研的医院中，各项因素占比较为均衡，其中服务器、存储等硬件故障和计算机病毒或黑客攻击以及网络安全漏洞三个方面占比更为显著。（如图2.2.1）

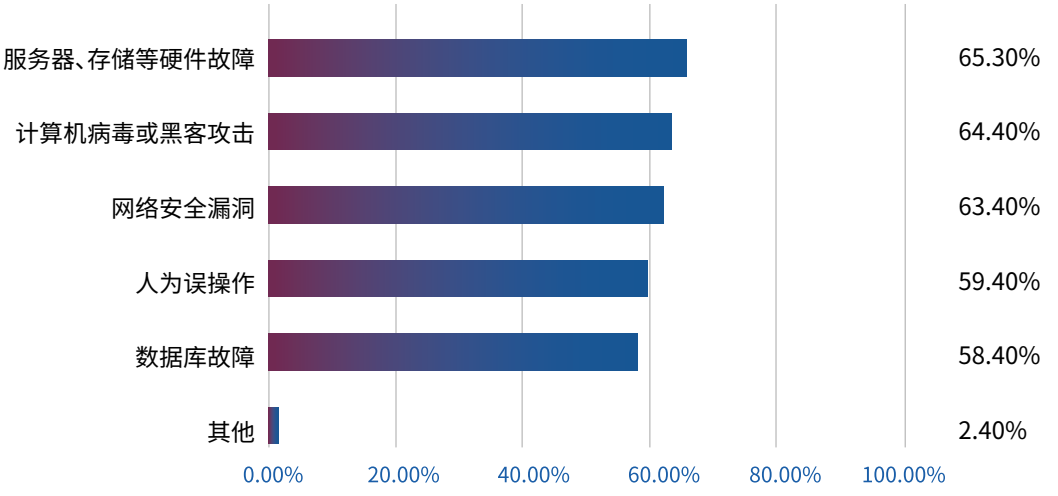


图2.2.1　现阶段医院 HIS 系统主要威胁

虽然参与本次调研的绝大多数医院能够在15分钟-1小时内完成HIS系统的容灾切换，但通过专家调研及研讨等方式进一步了解到，面对勒索病毒攻击、容灾系统和备份数据被恶意加密等广泛性数据逻辑错误的灾难场景，当前医院HIS系统的灾备结构，依然面临多重挑战，难以轻松应对。

《建设规范》建议的基于存储磁盘阵列、存储备份软件、数据快照技术、同异步数据复制技术的HIS系统备份、容灾一体化架构，是医院应对HIS系统核心威胁、降低因HIS系统灾难性故障带来的经济损失和社会影响的有效解决方案。

2.2.2 现阶段PACS存储架构核心挑战

依据《电子病历应用管理规范（试行）》和《医疗纠纷预防和处理条例》的要求，很多医院着手实施数据永久保存策略，其中也包括PACS影像数据的永久保存。随着先进的医学检测设备的引入和增加，和近乎永久数据保存的策略，导致医院PACS系统数据量越来越大。

调研显示，对于PACS存储架构而言，当前最显著的挑战聚焦在运维不够便捷、存储成本较高、数据可靠性保障低、患者数据长期保存对存储需求量大这4大方面。在参与调研的医院中，存储成本高带来的挑战最为凸显，患者数据的长期保存需求也为PACS存储架构带来不容忽视的现实挑战（如图2.2.2）

PACS影像存储系统，首先需要解决的问题，是海量PACS影像数据并发写入和读取的性能问题，这直接影响着医院影像科室的诊断效率。

第二，海量数据的高可靠性存储，也是PACS系统数据安全性保障的核心问题。

PACS影像存储系统需要提供足够高的可靠性保障和可用性保障，并能够应对一定程度上的硬件故障和不丢失数据。PACS影像存储系统还需要提供严格的系统级安全性保护功能，尽可能阻止黑客利用系统底层“零日漏洞（0 Day）”破坏数据。

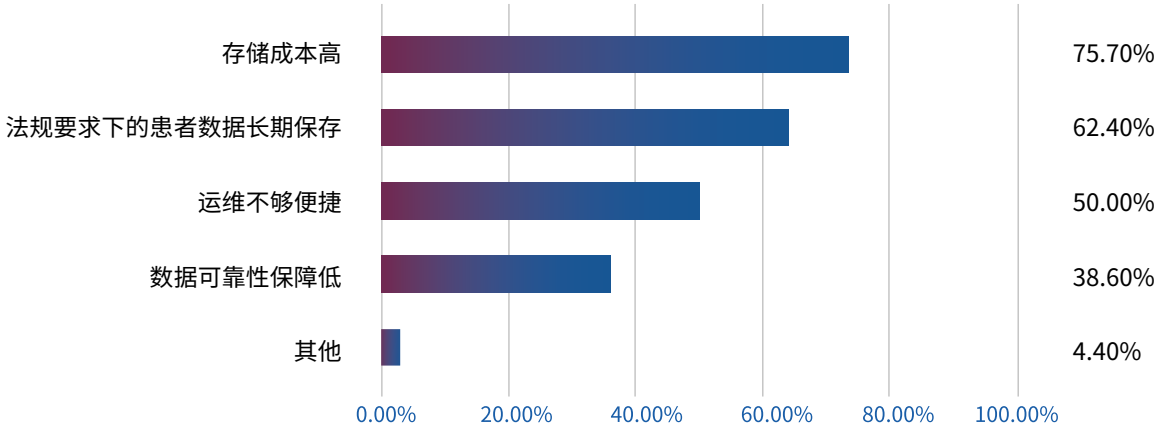


图2.2.2 现阶段医院 PACS 存储架构主要挑战

PACS系统数据安全保障的第三个核心问题，则是数据备份。在医院影像数据管理中，数据备份是一项非常重要的工作。由于PACS影像数据包括海量的小文件，因此必须采用新一代的数据备份技术，以确保在有限的窗口内，完成数据备份和数据恢复。PACS 系统备份数据应具备不依赖于特定应用软件的长期可解读性，以避免由于备份软件供应商变化而可能出现的问题。《建设规范》中提出的存储备份软件，能够以数据原始格式备份数据，比较好地解决了上述问题。

第四，是数据迁移问题。在漫长的PACS数据生命周期范围内，必然要面临 PACS存储系统和备份系统硬件更新换代所引发的数据迁移问题。当医院PACS系统数据达到数百TB乃至数PB或更多时，单纯针对应用层面的数据迁移，已经很难满足医院对于数据迁移可靠性和迁移窗口时间的要求。此外，依靠存储系统硬件底层技术的数据迁移，也必须要解决医院医学影像中心系统对迁移数据的可访问性问题。这就要求 PACS影像存储系统和备份系统具备数据透明迁移技术，即在数据迁移完成后，能够在医学影像中心系统不做任何变更的前提下为PACS系统提供数据访问能力的保障。

2.3 医院核心系统灾备建设

2021年6月，国务院办公厅发布《国务院办公厅关于推动公立医院高质量发展的意见》[9]，在引领公立医院高质量发展新趋势中，指出要强化信息化支撑作用。推动云计算、大数据、物联网、区块链、第五代移动通信（5G）等新一代信息技术与医疗服务深度融合。推进电子病历、智慧服务、智慧管理“三位一体”的智慧医院建设和医院信息标准化建设。

随着信息化建设价值的不断凸显，医疗行业在加速与科技融合的同时，也将信息安全体系建设提上日程：2015年《公共安全业务连续性管理体系指南》[10]出台、2016年国务院办公厅发布《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》[11]、2019年《信息安全技术网络安全等级保护基本要求》2.0版本发布、2021年9月1日起实施的《中华人民共和国数据安全法》[12]、2022年9月国家卫生健康委、国家中医药局、国家疾控局印发的《医疗卫生机构网络安全管理办法》[13].....多个信息安全相关法律法规的出台，让信息安全体系建设成为医院开展信息化建设、实现高质量发展的必要前提。

[9]《国务院办公厅关于推动公立医院高质量发展的意见》

《国务院办公厅关于推动公立医院高质量发展的意见》旨在推动公立医院高质量发展及更好满足人民日益增长的医疗卫生服务需求；国务院办公厅于2021年6月4日发布。

[10]《公共安全业务连续性管理体系指南》

此处指《GB/T 31595-2015公共安全业务连续性管理体系指南》。《GB/T 31595-2015公共安全业务连续性管理体系指南》由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会于2015年6月2日发布，并于2016年1月1日实施。

[11]《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》

《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》是为了而制定的法规，2016年6月21日，《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》由国务院办公厅发布，自2016年06月21日起实施。

[12]《中华人民共和国数据安全法》

《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于2021年6月10日通过，现予公布，自2021年9月1日起施行。

[13]《医疗卫生机构网络安全管理办法》

2022年8月29日，国家卫生健康委、国家中医药局、国家疾控局印发《医疗卫生机构网络安全管理办法》。

目前，不断扩增的医院信息系统复杂性日益提高，应用系统规模也在持续扩大，医疗数据量激增等现状带来的安全问题逐渐凸显，为医院信息系统的“数据安全”及“业务连续性”带来极大挑战：庞大核心系统和多元应用带来大容量、高吞吐等要求；医院数据作为重要资产，容易受到人为失误、勒索病毒或恶意攻击的影响；医院数据备份与异地容灾的部署相对复杂、支出成本高昂；面向灾备系统的专业运维人员匮乏；医院缺乏数据备份及应急接管的演练工作，导致业务系统日常加固和升级不足……

医院高质量发展之路上，围绕医院核心信息系统建设高效稳定的灾备体系，已经成为医疗行业信息化建设中的首要任务。

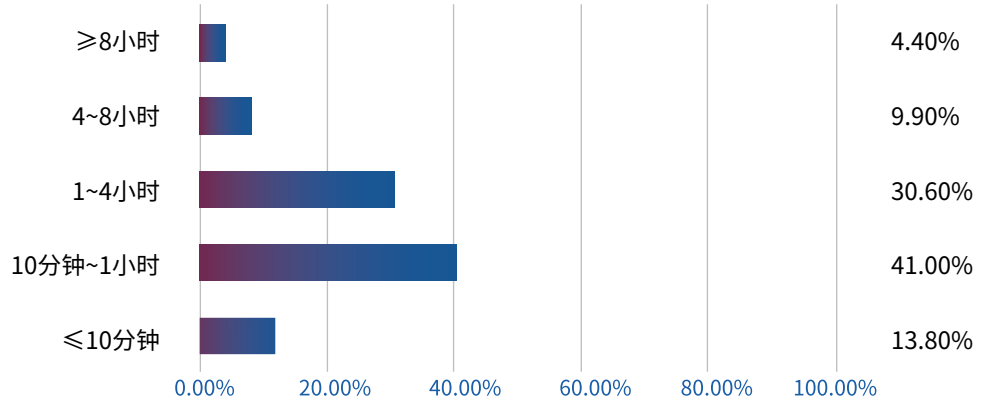
2.3.1 HIS系统数据备份

HIS作为医院的核心信息系统，包含了医院各业务流程中的所有关键信息、与医院运营管理息息相关。因此，保障医院HIS备份的可用性和高效性，对于医院信息安全和业务稳定运行具有不容忽视的重要意义。

本次调研结果显示，在参与调研的医疗机构中，约41%的医院HIS系统完成全备份时间在10分钟到1小时内；30.6%的医院HIS系统完成一次全备份的时间在1~4小时内；约13.8%的医院可以在10分钟内完成HIS系统全备份操作；HIS系统全备份时间在4~8小时和8小时以上的医院占比较少。（如图2.3.1）

2.3.2 HIS系统业务容灾切换

医院数字化建设程度不断深入，日渐庞大的系统和不断丰富的应用，让医疗数据量呈现快速上升态势。HIS作为医院核心信息系统之一，贯穿着医院业务流程的各个环节，在医疗服务和医院管理等方面均发挥着核心支撑作用，因此，实现7*24小时不间断运行的需求，对系统的安全性、可靠性、稳定性都有很高要求，HIS系统需要高可用高可靠的灾备系统来为业务数据保驾护航。



（图2.3.1 医院 HIS 系统完成全备份所需时长统计

在参与本次调研的医院中，约49.5%的医院能够在15分钟内完成HIS容灾切换；34.6%的医院完成HIS容灾切换需要15分钟至1小时的时间；约13.8%的医院完成HIS容灾切换需要1至4小时；仅有少数医院需要4至8小时甚至更长时间完成HIS容灾切换。（如图2.3.2）

2.3.3 PACS系统数据备份

随着医疗水平的不断提升，覆盖多学科、多模态的影像数据快速涌现，医院开展临床诊疗、医疗科研工作时，对数据管理和应用的要求愈发迫切。

调研结果显示，在参与调研的样本中，约53.4%的医院完成PACS数据备份的时间需要4至8小时；约23.7%的医院能在10至15分钟内完成PACS数据备份；约14.3%的医院完成PACS数据备份时间在8小时以上；还有少数医院尚未部署数据备份系统。（如图2.3.3）

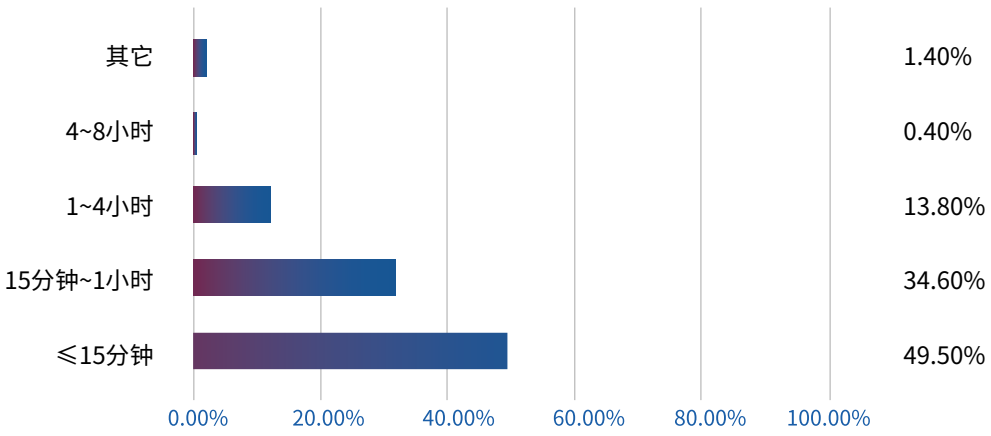


图2.3.2 HIS 系统业务容灾切换所需时长统计

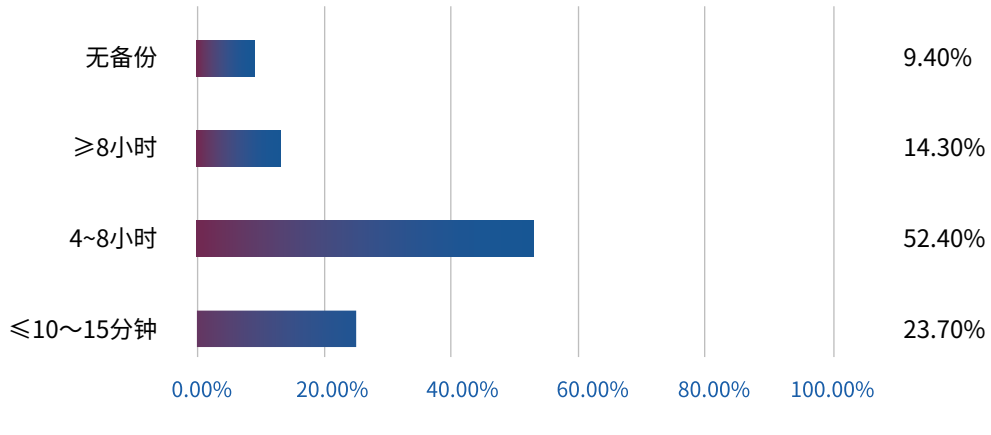


图2.3.3 PACS 系统数据备份所需时长统计

2.3.4 PACS系统业务容灾切换

PACS中所存储的数据是医院开展临床诊疗、医疗科研、医疗培训等多方工作的重要保障，如果PACS数据库出现故障，会严重影响到医疗业务的开展，甚至会造成重要医疗数据的永久丢失。因此，PACS数据库的稳定运行对医院正常业务的开展至关重要。

参与本次调研的样本中，约有39.1%的医院进行PACS容灾切换的时间在15分钟至1小时内；约36.6%的医院PACS容灾切换时间小于15分钟；约15.3%的医院PACS容灾切换时间在1至4小时之间；少部分医院的PACS容灾切换时长需要4至8小时甚至更久。(如图2.3.4)

2018年4月，国家卫生健康委员会发布《关于印发全国医院信息化建设标准与规范（试行）的通知》[14]。该《通知》针对医院信息化建设的各个方面，给出了可执行的量化指标，特别是规范了医院数据保护和应用容灾的 RPO、RTO 指标。

总体来说，医院灾备建设需要考虑到多个方面：从使用角度来说，要以RTO和RPO 两项指标作为具体灾备解决方案部署的出发点；从实际项目上来说，则还要考虑投资成本（TCO）和项目回报率（ROI）两项指标。最终的容灾部署和实施，需要根据具体情况展开分析。

> 核心信息系统的安全仍有不少难点有待突破，其一是在互联网化的当前，面对线上支付、核酸检测申请及报告下载、云胶片等应用需求，如何应对用户量激增带来的系统压力；其二是医疗数据如何进行分类分级管理、数据资产如何进行梳理、梳理后如何落实责任；其三是安全和效率的平衡如何把握。
>
> —— 包国峰
>
> 山东第一医科大学附属省立医院信网办副主任

「HC3i新医观点」

医院谋求未来发展的过程中，正在不断探索更多行之有效的措施，实现建立牢固信息化保障体系的目标。

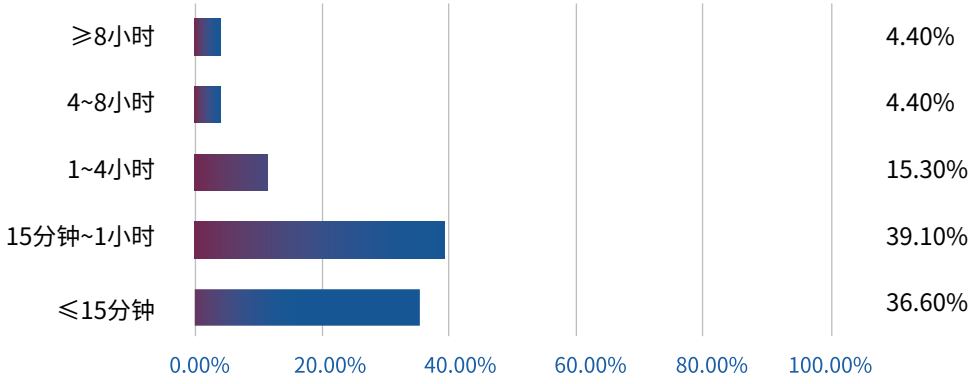


图2.3.4 PACS 系统业务容灾切换所需时长统计

[14]《关于印发全国医院信息化建设标准与规范（试行）的通知》
为促进和规范医院信息化建设，在《医院信息平台应用功能指引》和《医院信息化建设应用技术指引》基础上，国家卫生健康委员会制定了《全国医院信息化建设标准与规范（试行）》明确医院信息化建设的建设内容和建设要求，并于2018年4月13日发布。

03

医院数据应用与安全防护发展状况

3.1 医院数据量呈指数增长

在政策引导和技术发展的双重驱动下，医疗系统和应用不断丰富，存储和分析能力持续进阶，医疗行业数据呈现爆发式增长，医疗大数据产业步入快速发展阶段。面对快速涌现的多源异构数据，如何通过信息化手段助力医院充分挖掘数据价值，成为医疗机构在发展过程中不断探索和实践的重要内容。

因为目前医院的数据涉及方方面面，因此有专门的管理人员很重要，应该把多专业的数据治理团队纳入到到数据治理架构中，实现跨专业的通力合作才能将数据治理做得更好；其次，可以先从应用入手，从当前医院在数据应用过程中比较突出的矛盾入手进行整改。

—— 史亚香

东南大学附属中大医院信息化建设总工

「HC3i新医观点」

随着医疗水平的不断提升，覆盖多学科、多模态的影像数据快速涌现，医院开展临床诊疗、医疗科研工作时，对数据管理和应用的要求愈发迫切。面对快速涌现的多源异构数据，如何通过信息化手段助力医院充分挖掘数据价值，成为医疗机构在发展过程中不断探索和实践的重要内容。

3.1.1 近一年内HIS系统数据增量情况

智慧医院发展大潮下，人工智能、互联网、大数据等新兴技术正在不断落地医疗，并推动着医院信息系统向着更多元化、复杂化的趋势发展。

经调研发现，当前医疗机构数据量均处于增长状态。在参与调研的样本中，HIS数据增量为1TB以内的医院占比最高，约为54.9%；HIS数据增量在1TB-3TB的医院也占有一定比例，约为41.7%；增量在3TB-5TB的医院占比较少，约为3.4%。（如图3.1.1）

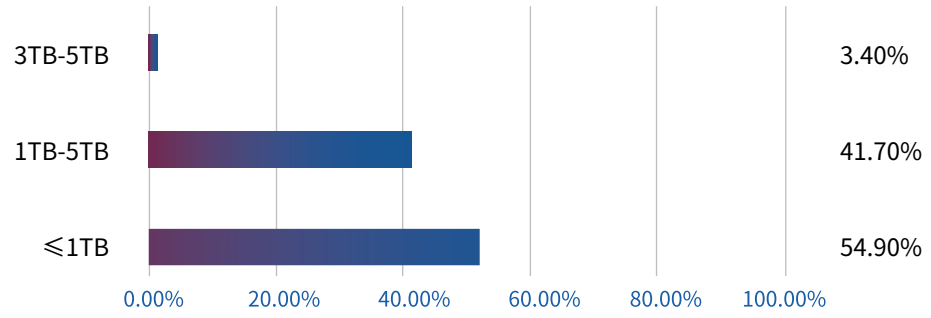


图3.1.1 近一年内 HIS 系统数据增量情况统计

3.1.2 近一年内PACS系统数据增量情况

医疗影像技术的快速发展，让影像精度不断提高、覆盖的学科范围也更加广泛，医院PACS影像数据激增。此外，按照医疗行业法规要求，患者影像数据需至少保存15年以上。因此，医院信息中心在保证PACS影像数据的高性能、高可用体验访问的同时，还要满足数据安全、持久保存要求，实现在线、近线和离线的全生命周期存储和管理。

目前，医院PACS数据均处于快速增长阶段。在参与调研的样本中，PACS数据增量在1TB-50TB区间内的医院占比最高，约65.8%；PACS数据增量在1TB以内的医院，占比约16.8%；而增量在50TB-200TB左右的医院，占比达13.3%；少数医院PACS数据增量可达200TB以上。（如图3.1.2）

3.2 医疗数据核心应用场景

迈入信息时代，数据成为当前各行各业宝贵的无形资产。在卫生健康领域，新兴技术的加速落地为行业发展带来更多可能性，通过数据挖掘和分析，能够助力行业实现降低医疗成本、提升诊疗效能、提高医疗服务水平等目标。

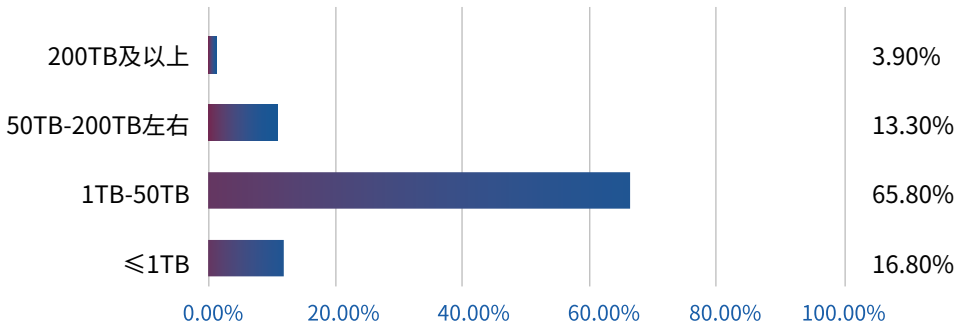


图3.1.2 近一年内 PACS 系统数据增量情况统计

如果仅从信息角度推动数据治理发展难度很大。但在医院高质量发展背景下，医疗数据治理迎来了好机遇，从各级领导部门到医院管理者再到医疗从业者，越来越多的人开始逐渐有了数据应用的概念或思维。

—— 王力华

北京友谊医院信息中心主任

医疗数据涉及的应用场景越来越广，随着医疗应用系统的不断扩增和数据量的不断增大，医院内部和医院间数据整合的力度正在不断加大。

—— 傅昊阳

广东省中医院信息处处长

调研显示，目前医院的数据应用场景主要包括医疗质量监控、面向医院管理的数据分析、文本数据结构化处理、面向科研的数据检索和分析、专病库建设等方面。其中医疗质量监控和面向医院管理的数据分析两大场景的数据应用最为广泛，在文本数据结构化处理和面向科研的数据检索与分析方面也具有相当比例，部分医院已将数据应用场景扩展至专病库建设。(如图3.2)

3.3 医疗数据存储与安全管理

在新兴技术不断落地行业的当前，医疗数据的规模和复杂性为医疗机构挖掘数据价值带来诸多新的挑战。因此，能否提升数据“存管用”能力，决定着医院发展的水平与效率；与此同时，智慧医院建设背景下，数据治理能力与赋能医院构建医疗、服务、管理“三位一体”的效能全面提升紧密相关 —— 医疗数据安全存储、高效利用的重要性不言而喻。

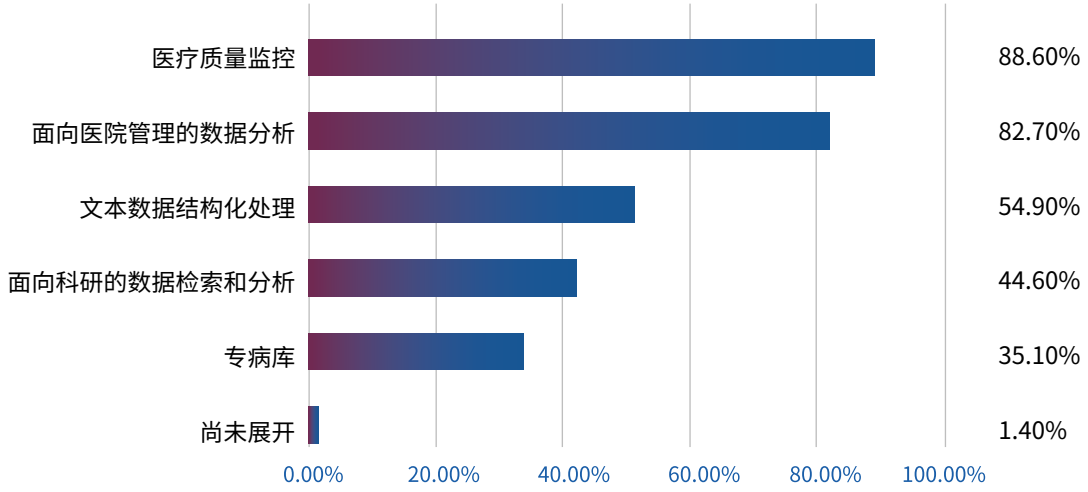


图3.2 医院数据核心应用场景类别分布

对于数据安全而言，怎么从内部把这个数据安全做好?应该先建立好这个处理机制，应该建立完善的监管机制、监控机制，最后还要有监督机制。

——徐红兵

安徽医科大学第一附属医院医疗大数据办公室主任

3.3.1 医院当前需要备份的数据类型

大型规模医院对业务连续性要求更加苛刻，在要求本地数据有完善业务连续性保障和数据安全的同时，需要在远程建立灾备中心，通过灾备中心防止一些自然、人为等灾难因素。

目前，医院信息体系庞大，需要备份的数据类型也越来越丰富。经调研，当前医院需备份的数据主要来自数据库、虚拟机、容器、操作系统和业务应用环境、PACS影像数据。在参与调研的医院中，数据库数据备份的需求最大，其次来自虚拟机、操作系统和业务应用环境，PACS影像的数据备份需求也占有较大比例。(如图3.3.1)

虽然医院各系统中的数据重要性等级存在一定差异(非常重要和相对没有那么重要)，但对于医院来说其实都可以算是核心数据，因为它们都受到法律保护，都要接受医院的管理。

——赵前前

北京朝阳医院信息中心副主任

3.3.2 医院数据保护措施

医疗信息化建设持续推进、互联互通建设不断深入、临床科研需求持续增加……诸多因素让医疗数据应用与共享的范围持续扩大，也为医疗数据安全带来更多隐患。如何进一步夯实医院信息安全体系、提升医院的数据安全保护能力、加强医

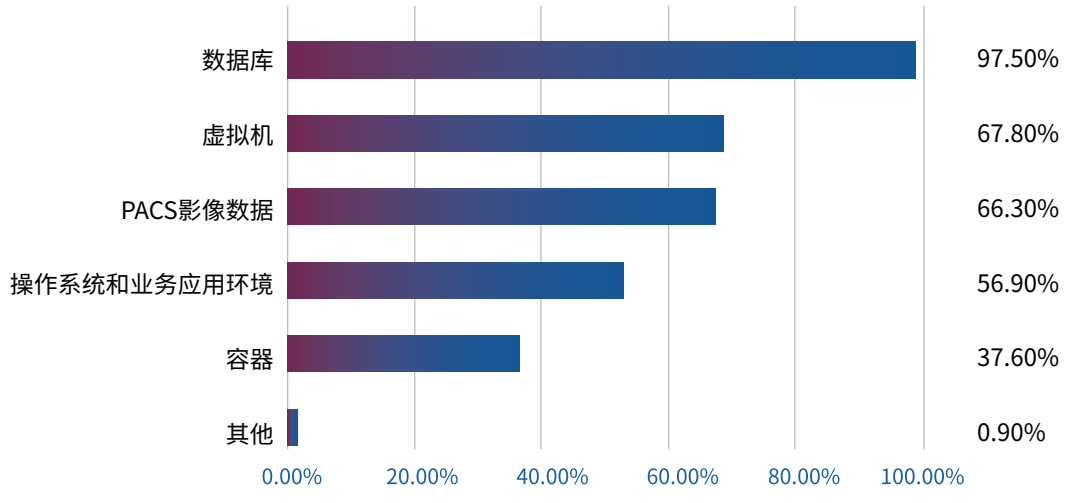


图3.3.1 医院核心数据来源分布情况

院数据数据管理能力，已经成为医院管理者和医疗信息化建设者们需要关注的重要议题。

目前，医院进行数据保护采用的措施主要有数据容灾、数据离线归档、数据备份、CDP（数据保护）等。在参与本次调研活动的医院中，多数采用数据备份和数据容灾手段进行数据保护；通过数据离线归档和CDP方式进行数据保护的医院也占有一定比例。（如图3.3.2）

> 信息部门则需要有一些简明扼要的方法来增强数据保存和安全性防护能力，例如做一些第三中心或者增加一些技术手段来保障数据的安全。
>
> 医院进行数据治理时，通过积累和清洗让数据达到可用状态非常不容易，因此更要做好数据的安全，杜绝被非授权人员盗取盗用数据。
>
> —— 谢颖夫
>
> 云南省第一人民医院信息中心主任

3.3.3 核心数据备份所选存储介质

调研显示，当前医院在进行核心数据备份时，存储介质主要包含服务器本地存储、生产存储磁盘阵列、备份一体机、独立存储磁盘阵列、磁带库、离线移动硬盘等。参与调研的医院在进行核心数据备份时，将独立存储磁盘阵列和备份一体机作为存储介质的占比最高；介质为服务器本地存储的占比也较为突出；以生产存储磁盘阵列为介质占有一定比例；仅有少数医院采用离线移动硬盘和磁带库作为数据存储介质。（如图3.3.3）

3.4 数据管理主要挑战

虽然医疗行业信息化建设已经走向中心位，但医院在进行数据管理的过程中，依然面临很多挑战。经调研，医院数据管理所面对的关键性问题包括：服务器本地存储难以支撑当下对医疗数据应用及管理的需求、数据可靠性保障不足、数据

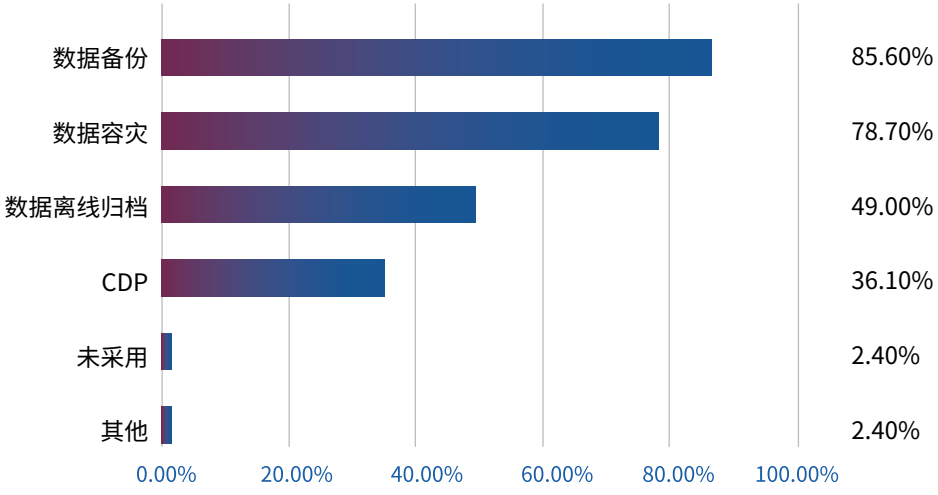


图3.3.2 医院数据保护主要采取的方式

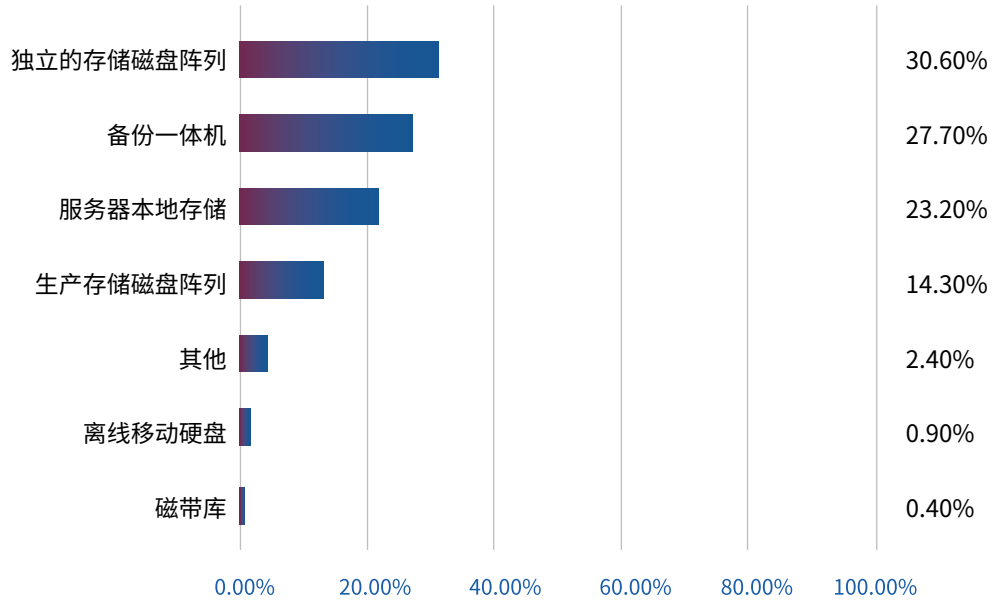


图3.3.3 核心数据备份所选存储介质的类型

跨系统流动的效率和成本较高、专业人才匮乏等；其次，法律合规实施程度不足、数据管理权限不足、部分临床数据不受管理等问题也较为突出。（如图3.4）

> 医院的数据治理，难度比较大的地方在于，这些数据涉及到多个异构系统，且如何确保业务系统的准确性、连续性、一致性等问题，提升数据质量，目前依然是技术层面难以解决的挑战。
>
> —— 王力华
>
> 北京友谊医院信息中心主任

当前医院数据管理及应用所面临的挑战，愈发凸显了医院信息化建设必须与医院业务紧密结合的新时代特征。

备份、容灾一体化架构，能够为医院提供更为高效的业务连续性保障、数据安全性保障和法律合规保障；而数据跨系统流动的效率和成本问题，则可以通过信息化建设全局规划来解决。在医院进行医疗数据价值挖掘的过程中，数据管理要具有在合适的时间内、以可接受的成本、交付给不同业务系统使用的能力。同一份数据，在数据流动过程中，也往往需要转换不同的存储协议、产生多个数据副本，这必然会带来容量、性能、效率之间的取舍问题。因此，如何减少数据流动的次数、减少数据副本的数量，就成为提高数据跨系统流动效率、降低数据跨系统流动成本的重要考量因素。

要减少数据的流动次数，则应尽量将同一份数据

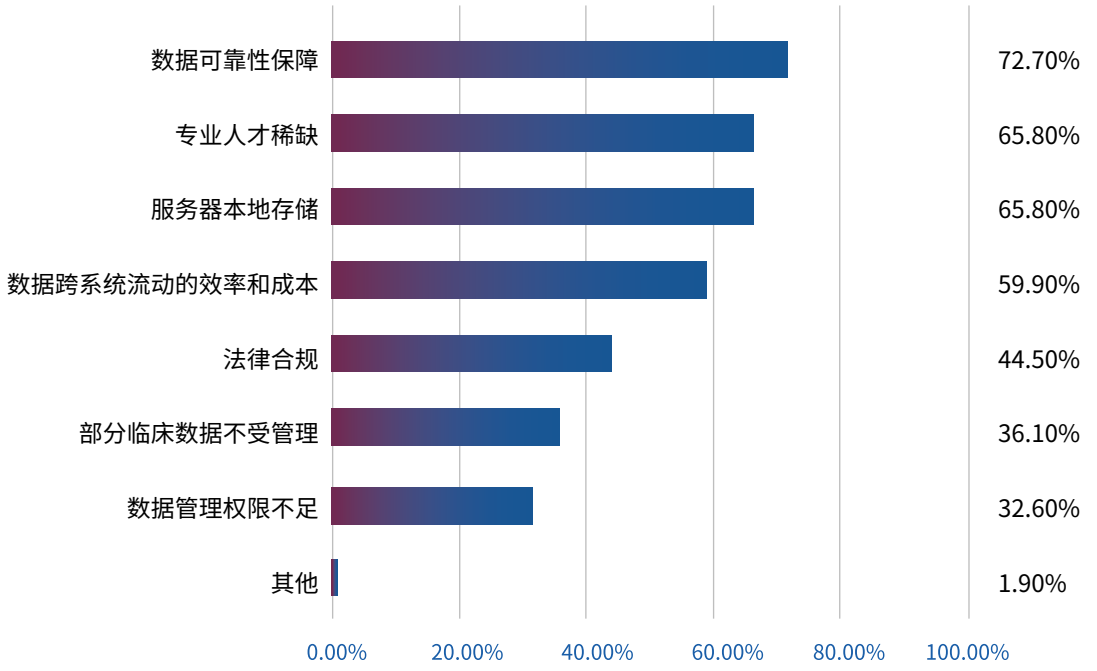


图3.4 现阶段医院数据管理的主要挑战

交付给不同的业务系统使用。考虑到生产系统的重要性，医院一般避免直接将生产数据用于数据价值挖掘。此状况下，医院生产数据备份系统所具备的多个时间点、全量数据副本的特性，就变得尤为重要。备份系统只有具备将任意时间点的备份数据，以虚拟副本的方式快速恢复、快速交付的能力，才能变数据备份为数据管理，进而从数据管理挖掘数据价值。

> 对于医院数据治理来说，数据的分级分类管理尤为重要，即便是核心数据也需要分出级别和类型来，而不能所有数据一刀切。
>
> —— 王力华
>
> 北京友谊医院信息中心主任

医院业务系统	结构化数据（数据库）	非结构化数据		虚拟机	容器	AI		大数据	
		高性能	归档			实时性业务	非实时性业务	实时性业务	非实时性业务
存储协议	FC iSCSI	NAS	NAS 对象	FC iSCSI NAS	NAS iSCSI	NAS	NAS 对象	HDFS NAS	HDFS NAS 对象

而根据上表中的分析结果，减少数据协议转换时，NAS存储协议可同时满足医院绝大多数业务系统高性能、兼容性和易运维的需求，因此采用NAS存储协议能有效降低因存储协议转换而带来的数据流动效率下降和副本数量增加等问题。

建立完善的数据管理监测体系很重要，也很不易，需要进行许多实际的应用工作。数据的安全体系是很复杂的，不仅涉及到整个管理体系，也涉及到了技术体系以及整体的运维体系。

——傅昊阳

广东省中医院信息处处长

04

医院信息安全体系建设痛点概述及发展趋势预测

为更加深入、准确地认清行业现状，本篇报告综合顾问组专家相关行业认知和经验分享，针对医院信息安全建设痛点和未来发展趋势展开如下分析与解读。

4.1 信息安全建设过程中所关注的核心问题与挑战

当前，医院信息化建设已经走入快速发展的新阶段，覆盖面更广、渗透程度更深的信息化应用在发挥重要价值的同时，也带来诸多新的挑战。对于医院而言，信息安全建设过程中，仍有很多突出问题有待解决：

在人员方面，随着医院信息系统的复杂化和应用的多元化，信息安全建设的难度持续增加，缺少有效的信息安全专业人员是当前医院普遍存在的现象；此外，信息化已经渗透到医疗业务的方方面面，如何有效加强医疗从业人员的安全意识、减少因弱口令等问题带来的安全隐患，是保障医院信息安全必须关注的问题。

> 数据治理是非常难的一件事情，是一个很大工程，需要建立一套比较完整的体系，才有可能慢慢把这个数据的治理做好；此外，数据利用需要树立好的理念，大家对数据都要有比较深刻的认识，才能推动数据应用持续发展。
>
> —— 傅昊阳
>
> 广东省中医院信息处处长

> 整体来说，有一件事情需要我们坚持不懈坚持去做，那就是普及医院职工数据思维的理念，无论是管理者、信息人员，还是临床医护，都应该具有数据思维的概念，才能更高效高质的不断提升数据治理能力。
>
> —— 史亚香
>
> 东南大学附属中大医院信息化建设总工

此外，高质量发展的格局下，医院信息系统正在迎合互联网化趋势，向整合化、平台化、智能化进阶，安全建设的趋势也正在随之发生转变：互

联网化趋势下，面对线上支付、核酸检测申请及报告下载、云胶片等应用需求，用户量激增带来的系统压力成为医院亟待解决的痛点；越来越丰富的智能化应用，给医院相关系统和设备的安全性带来新的威胁；越来越丰富的软件和设备进入医院后，可能会因源代码漏洞等自身携带的安全问题威胁到医院的信息安全；迈入数据时代，系统相互之间的互联互通、数据的治理对于提升医院运营管理能力尤为重要，实现一体化监管的重要性日益凸显；面对持续快速增长的海量医疗数据，如何进行分级分类管理、数据资产如何进行梳理、梳理后如何落实责任，都是医院需要关注的问题。

因此，医院的安全防护固然重要，但在建设过程如何关注信息安全建设与服务便捷性、系统性能和使用体验、各业务科室间的认知协同、系统可建可运维可监管等方面的平衡，也是亟待解决的关键问题。

总之，医院信息化建设需要回归业务目标导向，以业务实现效果为建设目标，从全局架构高度，全面考虑生产系统、备份系统、容灾系统的集成性和融合能力，将医院信息化建设作为一个整体施行规划和设计。

> 在医院高质量发展的新要求下，医院信息系统建设呈现了互联网化、整合性应用、智能化应用建设的趋势。在医院信息安全规划方面，应该更关注医院信息化发展的新特征。安全建设的侧重点转变到互联网应用安全防护、数据安全管理等。不论是安全还是其他的工作，都要有一个体系化管理思路，做好整体规划，覆盖安全人才的培养、安全管理制度建设、安全策略设计、安全检查流程设计等，完成阶段性建设后仍需持续改进。
>
> —— 田宗梅
>
> 首都医科大学附属北京世纪坛医院信息中心主任

4.2 医院信息安全建设趋势

当前，科技与行业的不断融合让医院面临更多样的信息安全挑战，尤其在互联网诊疗快速落地后，对于医院信息系统安全的要求变得更高；加之，医学影像技术的持续发展下，CT、核磁、PET等精细化程度不断加深，导致影像数据量飞速攀升，数据管理和应用面临更艰巨的挑战。

基于上述背景，在医院开展信息安全建设有关工作时，医院应先进行体系化的规划，再进行实践和持续优化。聚焦信息安全规划方面，则应该广泛覆盖到医院业务的方方面面，化被动为主动、把静态防护调整到动态防护，把关注点从事后逐渐转移到事前。具体方式可参考如下：

1.集约化管理

例如针对数据安全，首先要确保信息系统和数据

存在环境的安全性，查看清楚信息系统存在的安全风险，再进行有针对性的修复；

2.数据资产梳理

然后摸清保护对象，对重要敏感的数据进行标记；

3.安全保护

也就是制定安全保护的策略，如访问控制、行为审计、数据脱敏、数据加密等；

4.建立信息安全数据安全监测体系

需要注意的是，实际建设过程中，基于不同医院的发展现状差异，应先进行差距分析或自评或自测，从而发现医院信息安全建设中的不足，根据医院当下安全问题的轻重缓急进行分级，再规划出最适合医院当前发展需求的建设周期，逐渐建设和完善。

> 安全工作既要面面俱到，也要精雕细琢。安全是短板效应，所以要化被动为主动、把静态防护调整到动态防护，把关注点从事后转移到事前和过程的实施监管。
>
> —— 包国峰
>
> 山东第一医科大学附属省立医院信网办副主任

对于行业科技企业而言，在医院面对发展需求和挑战时，应该站在医院用户角度切实帮助医院进行匹配医院现状的分析和规划、再进行落实，最终赋能医院信息安全能力的提升。

面对医院复杂的应用场景，如何捋清系统之间千丝万缕的联系、满足互联网应用中的对外防护？这需要科技企业能够具备足够能力的安全服务人员、并精准掌握医院安全建设需求，针对不同医院的特点和现存的主要安全问题制定解决方案，快速定位到医院的痛点难点，并有效推动信息安全工作的实施和完善。

> 医院信息安全建设，要结合网络安全管理部门承载能力。现状下，绝大部分医院安全工作难以到位。现有的方案往往都是针对某一个点，最后造成执行过程碎片化、各类安全数据孤岛化的现象，同时安全监督检查工作难以执行，难以到位。监督不到位又导致日常的安全工作执行不到位。如何将这些碎片化的解决方案整合好，实现网络安全管理的全面性、准确性、易用性的一体化管理的解决方案是非常关键的。
>
> —— 徐红兵
>
> 安徽医科大学第一附属医院医疗大数据办公室主任

此间，由于医院信息安全建设是一个漫长的发展过程，在解决不断出现的发展问题的过程中，已经产生很多碎片化的解决方案。如何将这些碎片

> 加强网络信息安全的目的是为了确保业务应用安全稳定、不间断，因此在网络安全建设方面，除了关注网络信息安全相关技术的应用和发展，还应该注重业务应用的场景化，即从信息系统的业务视角分级划定核心、关键和一般，梳理各类业务角色保障其开展业务工作所需要的从终端、网络、业务应用系统、应用中间件、数据库高可用等一整套体系的安全、可靠及可用性。
>
> —— 左秀然
>
> 武汉市中心医院信息中心主任

化的解决方案整合好，交付完整的结果非常关键的。在当前发展现状下，比起提供多样化的工具，一个完整全面、可落地交付的解决方案更能够满足当前医院的发展需求。

THANK YOU
FOR READING

【报告编撰】

组织策划

HC3i 调研与报告中心

内容编辑

HC3i 调研与报告中心

参与撰写

娄辛研 | 联想凌拓科技有限公司

林佑声 | 联想凌拓科技有限公司

李　欣 | 联想凌拓科技有限公司

致谢

诚挚感谢为本次调研报告展开深入研讨、分享实践经验、提供宝贵建议并把控内容方向的以下专家：傅昊阳、衡反修、包国峰、史亚香、田宗梅、王力华、徐红兵、谢颖夫、赵前前、左秀然；

诚挚感谢联想凌拓科技有限公司对本次报告的大力支持与专业建议；

诚挚感谢参与本调研活动的351位医院代表；

诚挚感谢在报告撰写过程中积极参与和提供建议与意见的所有医信同仁。

HC3i数字医疗网将继续在广大医信同仁的支持和关注下，坚守行业媒体使命，砥砺奋进、不忘初心，为医信行业发展持续赋能！

联想凌拓科技有限公司

联想凌拓科技有限公司（以下简称“联想凌拓”）是由联想和NetApp在中国共同出资、共同注册的合资公司。公司总部设立于天津空港经济区，并在北京，上海，深圳，广州，成都设有分公司。作为独立管理、独立运营的公司，联想凌拓专注于提供智能数据管理解决方案及服务，以中国客户需求为导向，依托领先的技术基因，结合本地化人才优势、研发创新实力、业务覆盖和服务网络，致力于不断推出领先的智能化数据管理技术，帮助中国客户释放数据的惊人潜力，全面打造现代化IT架构，加速企业实现数字化转型。

凭借在中国市场研发、生产、销售基于NetApp先进技术的存储与数据管理相关产品，增强中国数据存储市场的生态先进性，保持可持续发展的存储和数据服务产业，为中国客户提供先进的，差异化的数据管理和服务。同时，联想凌拓提供独有的Data Fabric混合多云解决方案战略，使企业可以跨覆盖内部部署和多种公有云服务平台的多维度IT基础架构无缝管理数据，赋予 IT组织充分发掘数据价值潜力所需的灵活性与一致性。

通过实行双品牌策略，联想凌拓为中国企业提供NetApp品牌的全线产品和解决方案以及联想品牌的OEM产品组合，为市场带来包括IT基础设施、云计算、数据中心、大数据等在内的领先技术服务，让中国客户拥有全面的一站式、全方位产品和解决方案选择范围，并仍然与全球企业一样，同步享受到世界一流的高性能数据管理解决方案。

智慧数据构建智能世界。作为中国专业领先的智能数据管理解决方案与服务商，联想凌拓将通过全球领先技术建设一个由数据智能驱动的未来。

销售热线：400-116-0099

服务与技术支持：400-828-3001

官方网站:www.lenovonetapp.com