

智慧医院建设中个人信息保护策略

李邦邦

(盱眙县人民医院 江苏盱眙 211700)

【摘要】智慧医院建设是新时期互联网技术发展与管理融合后形成的一种建设方式,在现有医院建设管理工作调研过程中发现,智慧医院建设为医院管理工作实施提供了帮助,并且也在加强医院管理的同时突出了医院建设地位。对于智慧医院管理而言,个人信息保护是整个管理工作实践的重点,也是在管理工作实践过程中的难点之一。如何在现有医院建设管理过程中,提高个人信息保护安全已经成为智慧医院建设的重点建设内容之一。鉴于此,本文针对智慧医院建设中个人信息保护策略进行了研究,旨在为智慧医院建设过程中个人信息保护策略推广及实施提供依据,提高智慧医院建设水平,也为智慧医院建设中的个人信息保护提供参考,降低个人信息泄露风险。

【关键词】智慧医院;个人信息;数据安全;隐私保护

Information Protection Strategies for Homo Sapiens in the Construction of Smart Hospitals

Li Bangbang

(Xuyi County Homo sapiens People's Hospital Jiangsu Xuyi 211700)

[Abstract] The construction of smart hospitals represents a new approach formed by the integration of internet technology and hospital management in the modern era. Research on current hospital construction and management practices reveals that smart hospital development aids in enhancing hospital administration while simultaneously elevating the status of hospital infrastructure. For smart hospital management, the protection of Homo sapiens information is both a focal point and a challenge in operational practices. Improving the security of Homo sapiens information has become a critical aspect of smart hospital construction within existing management frameworks. In light of this, this paper investigates information protection strategies for Homo sapiens in smart hospital development, aiming to provide a foundation for the promotion and implementation of such strategies. The study seeks to elevate the standards of smart hospital construction and offer references for safeguarding Homo sapiens information, thereby mitigating the risks of information leakage.

[Key words] smart hospital; Homo sapiens information; data security; privacy protection

所谓的智慧医院就是在医院建设和管理过程中,通过互联网技术、物联网技术以及人工智能技术等进行医院的智能化建设和管理,在该过程中能够实现传统医院管理的转型及创新,满足医院自身的管理要求,并且符合医院的自身管理情况。但是由于在智慧医院建设和管理过程中还存在着诸多的阻碍因素,如个人信息保护就是目前必须要解决的一项难题,如何在加强智慧医院管理的同时,同步落实个人信息保护工作成为了智慧医院当前建设管理所面临的重要问题之一。

1 智慧医院建设中个人信息保护的相关法规要求

我国当前信息化建设工作推广过程中,人们对于信息化技术的建设认识要求在不断提高。如何在加强智慧化建设与医院协同建设过程中,突出医院建设特色应成为医院建设的

重点建设内容之一^[1]。在卫生健康管理部门出台的相关政策法规中,要求对医院建设管理进行严格监管,并且应该在医院运行管理过程中,完善相关管理方案和策略。同时也需要以医院个人信息防护安全管理为目标,逐渐落实相关策略和要求。然而在智慧医院建设后,医院个人信息已经从传统的纸质档案记录转变为信息化记录,而这种情况下出现信息泄露的情况显著增加,所以有必要及时做好个人信息保护管理应对方案。如《医疗机构病历管理规定》以及《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《患者隐私保护管理办法》等都要求了个人信息保护,所以智慧医院建设管理过程中,需要以相关法律法规建设为前提,做好个人信息保护工作及方案。

2 智慧医院建设中个人信息保护的策略

2.1 从管理层面应对风险

2.1.1 建立制度与落实管理措施应对信息泄露风险

医院运营和管理过程中担负着保护患者个人信息安全的职责和义务,也是所有员工在日常工作实践过程中应该重点推进的一项管理工作。对于现有医院管理工作实施而言,管理制度方面的应对能够从根源上锁定医院个人信息泄露风险,能够在管理制度上加强信息安全防护,并且在该过程中需要加强患者个人信息核对及管理,也应该加强信息的监督和管理力度,从相关制度约束上着手,做好信息泄露风险管理和评价^[2]。与此同时,也应该培养医护人员的网络安全意识,同时根据《中华人民共和国医师法》第五十六条规定,医师在执业活动中泄露患者隐私或者个人信息的,将依法承担相应法律责任,该条款更加有助于加强个人信息安全管理力度,为医院个人信息管理提供帮助。

2.1.2 改善医院的患者告知方式满足个人信息保护要求

伴随着医院个人信息安全保护工作的逐渐推进,人们对于医院个人信息安全防护管理有了更高的认识。要知道很多医院在患者信息记录和管理过程中,仍是采用纸质病历。这种患者信息管理形式存在信息易损毁、检索效率低下、院际共享困难等突出问题,如果协调不好将会严重影响到患者的个人信息安全,所以在患者个人信息安全保护过程中,应该转变个人信息告知方式,采用多层次、智能化的管理体系。措施包括:(1)动态知情同意机制,采用分层级、分场景的电子化告知模式,通过医院 APP 或小程序推送交互式告知书,允许患者自主选择信息共享范围和使用期限。例如,在电子病历系统中嵌入“详细条款”功能,关键条款(如科研用途)需单独勾选确认。(2)可视化告知,设计将传统文字条款转化为信息图表、短视频等易理解形式,重点标注敏感信息(如身份信息)的处理规则。在挂号、检验等关键环节设置弹窗提醒,并保留“再次查看说明”入口。(3)实时权限管理,向患者开放个人信息访问日志查询功能,患者可随时查看哪些科室调取了其数据,并能即时撤回授权或提出异议。系统应在医生工作站显示当前患者的授权状态提示。(4)多语言及无障碍适配,针对老年、残障等特殊群体,提供语音播报、大字版界面等无障碍告知方式,少数民族地区医疗机构应配备双语告知选项加强个人信息防护管理力度,以此提高个人信息管理水平。

2.1.3 患者信息及医疗数据共享需求应对

随着智慧医院建设工作的逐渐推进,人们已经意识到医院患者信息化管理的必要性和价值,并且已经结合智慧医院信息化建设要求完善了相关应对方案。在现有智慧医院建设管理过程中发现,医疗数据共享需求在不断提高。因此我们需要通过技术、法律以及道德等诸多规范形式,寻求数据共

享与隐私保护之前的平衡^[3]。目前很多城市医院建设管理过程中都已经将病例、检验、检查信息管理融入到医院日常管理中。通过相关研究分析发现,患者就诊之后医院应该通过医院 APP 或者微信公众号管理了解到患者的就诊需求和意愿,应该以更加高效的解决方式确定限定范围,完善患者就诊管理方案,也需要通过个人信息管理加强患者就诊信息监管力度,提高患者个人信息共享安全,防范个人或者机构通过数据共享而造成对个人信息安全的损害。

2.2 从技术层面应对风险

2.2.1 医疗信息系统被非法访问风险防范

在信息化技术发展过程中信息手段保护也成为了安全管理的重要举措之一。在保障信息安全管理措施构建过程中,应该采用数据加密、人脸识别、双因子认证等技术手段和防护措施,确保数据的安全流转。在应用建设中,坚持“患者知情、授权调阅”的原则。比如我们在检查检验结果互认的应用中,患者有自主开放和关闭共享调阅的权限,医生在调阅患者医疗数据时,采用医务人员身份认证和患者手机端动态授权码双重认证,“一次就医、一次授权”确保安全。在管控过程中,应该按照患者认证需求,以用户认证管理为前提,做好相关信息录入管理。在加强智慧医院信息化管理实践过程中,应该做好信息的录入管理方案,并且要求用户在数据管理过程中做好相应的认证及管理,例如实施基于角色的访问控制,医院将数据分为核心、重要、一般三级,医生仅可访问分管患者完整病历,也应该采用一些物理手段进行认证管理,如装载数字证书的 UKey,手机二维码或者指纹等生物认证手段,以此提高个人信息防护管理能力^[4]。同时医疗行业更加需要遵循 HIPAA 规范限制医护人员访问范围,保护个人健康信息不被滥用或未经授权地披露。

2.2.2 互联网环境下数据传输风险的防范

互联网环境下,数据传输安全面临严峻挑战。数据在互联网内外传输,易引发泄露、篡改和丢失等问题^[5]。在加强互联网技术背景下的智慧医院建设管理过程中,需要以互联网技术管理为前提,并且做好互联网医疗管理机构,完善个人信息防护管理策略。同时也应该结合智慧医院管理要求,做好数据传输协议,实施数据加密传输,禁用弱加密算法(如 SSLv2、RC4),强制使用 AES-256 等强加密标准。然后在数据传输之前进行两端系统 HTTPS 认证。也应该在每次连接数据传输过程中加入密钥传输控制。在传输通道上也可以通过 VPN、专线等传输方式以保证传输过程的安全可靠,以此突出互联网传输控制优势。

2.2.3 互联网环境存储数据泄露风险的防范

智慧医院建设管理过程中,患者服务系统和互联网诊疗系统利用互联网服务器来存储医疗数据,并且运用云环境进

行存储管理。但进行云环境存储选择云服务商时,应优先考察其安全资质(如是否通过ISO 27001认证、是否符合国家数据安全法要求),并在合同中明确数据安全责任,要求服务商定期提供安全审计报告,约定数据泄露后的赔偿标准。同时,企业需保留对云端数据的控制权,通过加密密钥自主管理、定期数据拉取备份等方式,避免过度依赖单一服务商。对于智慧医院管理而言,数据存储环境的安全防护与服务器提出的安全防护要求也在不断提高。比如对数据存储环境,现在不光要防外部黑客偷数据,还得防内部人员乱删改。所以很多医院会给存储系统加“细粒度权限控制”,比如谁能看数据、谁能改、谁只能备份,分得清清楚楚。而且存储的数据本身也得层层保护,静态数据要加密,连备份的数据都得单独加密,怕备份盘丢了或者被人破解。通过强化数据存储环境防护措施应对能够加强访问鉴别认证管理能力,也可以防止数据被非法窃取。在智慧医院建设背景下的医院管理过程中,应该以互联网信息安全技术防护为前提,注重数据存储安全管理,加强个人信息数据防护安全,以此提高信息存储安全管理特色。

2.2.4 医院科研数据安全风险的防范

科研数据是医院科研成果管理过程中比较重要的管理内容之一,对于医院自身的管理工作实施而言,临床医学研究数据是检验医院自身管理成果的基础。医院科研数据在实际使用中,常见的风险问题可以从两个主要方面来看:一方面,在数据日常使用环节,可能由于网络防护存在漏洞(比如系统未及时修复的安全缺陷),或是工作人员操作不当(如误将数据发送至非授权邮箱、使用不安全设备存储数据),导致数据被未授权获取或外泄。另一方面,在针对具体科研场景的应用过程中,由于安全考量不够全面(比如对不同场景下的数据保护需求评估不足),或是业务流程设计存在逻辑漏洞,容易引发一系列安全隐患。例如,数据系统可能被恶意攻击破解,科研项目核心代码(如数据分析算法、试验模型代码)可能被非法窃取,甚至可能遭遇恶意代码注入(如在数据处理程序中植入病毒),进而威胁数据安全与科研活动的正常开展。在针对科研数据管理应对评价过程中,

基于《数据安全技术数据分类分级规则》、《卫生健康行业数据分类分级指南(试行)》等多项标准和信息安全防护管理为前提,做好相关的信息防护管理策略。在该部分安全防范管理工作处理过程中,应该从以下几个方面着手:首先,将患者敏感信息剔除,运用其他信息代替。其次,将管理数据拆分,做好医院科研数据防范管理策略,提高防范针对性,同时医疗机构工作人员应当对其执业行为产生的后果承担相应责任,并在涉及医疗数据再利用时主动接受监管,以此推动智慧医院建设和管理。

2.2.5 健康医疗数据技术保护的一些参考规则

在智慧医院数据建设管理过程中,人们对于个人信息防护管理有了更高的认识和追求。同时在医疗健康数据管理过程中,人们也已经加强了《网络安全法》、《数据安全法》、《信息安全技术—个人信息安全规范》(GB/T 35273-2020)、《信息安全技术—网络安全等级保护基本要求》(GB/T 22239-2019)等法规的建设和管理。同时在该过程中也需要以个人信息安全管理为目标,加强个人信息防护管理评价力度,也应该对数据划分进行评价。作为智慧医院管理人员,应该以医疗数据技术管理为前提,做好相关保护规则的运用及管理,也应该加强相关规则的运用和管理研究,注重相关参考规则的控制和管理。

结束语:

综上所述,在当前信息化技术发展实践过程中,人们对于智慧医院建设的培养及认识越来越高。与此同时,智慧医院建设中的个人信息保护越来越重视。通过个人信息保护工作实践提升了智慧医院建设质量,并且在推进智慧医院建设过程中,人们也已经逐渐意识到个人信息保护的地位和意义。在加强智慧医院建设的同时,应该从管理层面和技术层面着手做好个人信息保护策略,旨在个人信息保护策略实施过程中,能够提高智慧医院建设质量,为智慧医院建设工作的实践提供帮助,推动智慧医院建设工作转型。

参考文献:

- [1]刘海一.智慧医院建设中个人信息保护方式的探讨[J].中国数字医学, 2022, 17(03): 122-125.
- [2]刘同柱,王德斌,徐兵,等.智慧医院建设标准体系研究及实施策略[J].中国卫生信息管理杂志, 2020, 17(06): 6-7.
- [3]田海平,刘程.大数据时代隐私伦理的论域拓展及基本问题——以大数据健康革命为例进行的探究[J].伦理学研究, 2018(3): 67-72.
- [4]李楠楠.浅谈物联网技术在智慧医院建设中的应用[J].信息系统工程, 2020(3): 134-135.
- [5]李永军,刘倩.云计算环境下数据传输安全技术分析[J].信息与电脑, 2025, 37(05): 86-88.