“互联网 +”背景下医疗行业信息安全策略探讨

陈心怡 吴 翔 洪紫映

（华中科技大学同济医学院医药卫生管理学院 武汉 430030）

〔摘要〕 针对“互联网 +”背景下医疗行业存在的信息安全和隐私保护问题，结合中美两国在医疗信息安全方面有关政策和法律法规，探讨我国医疗行业信息安全未来发展方向并提出建议。

〔关键词〕 “互联网 +”；健康信息管理；信息安全；政策研究

〔中图分类号〕R - 058 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2022. 02. 012

Discussion on Information Security Strategy of Medical Industry under the Background of “Internet +” *CHEN Xinyi, WU Xiang, HONG Ziying, School of Medicine and Health Management, Tongji Medical College of Huazhong University of Science and Technology, Wuhan 430030, China*

〔**Abstract**〕 In view of the problems of information security and privacy protection in the medical industry under the background of “Internet +”, combined with the relevant policies, laws and regulations on medical information security in China and the United States, the future development direction of information security in the medical industry in China is discussed and suggestions are put forward.

〔**Keywords**〕 “Internet +”; health information management; information security; policy research

1 引言

互联网技术很大程度上能解决现有行业中存在的开放性、兼容性等问题，为多个行业的全面智能化提供助力。在医疗行业中“互联网 + 医疗健康”正在成为新的发展方向。随着互联网科技产业及大数据技术的飞速发展，卫生信息和卫生保健服务的提供和接受方式正在改变。在“互联网 +”时代强有力的信息安全政策是保证医疗行业信息化服务平稳有序开展的重要前提。网络技术的发展使医疗行业能够为从业者和客户提供更好的服务、更丰富的信息资源和更高的可用性。医疗保健是文档密集型行业，为了顺应行业发展需求医疗行业正在逐步向无纸化、智能化转变，与此同时面临问题与机遇[1]。此外在医疗保健智能化全过程中，患者个人隐私等敏感数据会在卫生保健组织之间流转，需要高度重视数据完整性与安全性。解决医疗保健领域安全风险和隐私保护问题的前提是制定有力的信息安全政策，本文着重探讨“互联网 +”背景下医疗行业所采取的信息安全策略。

〔修回日期〕 2021 - 09 - 27

〔作者简介〕 陈心怡，硕士研究生；通讯作者：洪紫映，博士，讲师。

2 医疗行业信息安全和隐私保护问题

2.1 概述

医疗信息是指在医疗过程中所产生的个人信息，包括患者身心健康、医疗状况等信息[2]。对纸质媒介而言，保存的信息只存在于一个物理空间内且复制信息成本较高，信息保护较容易，即使发生信息泄漏其影响范围相对较小。电子信息媒介的特点在于短时间批量信息处理效率较高、信息传播速度较快、信息复制成本较低，在信息保护方面面临较大风险和挑战。“互联网 +”背景下对于用户面临的医疗信息风险，一般可以从安全性和隐私性两个角度考虑。

2.2 医疗行业安全性和隐私性

安全和隐私概念不同，为了全面考虑用户信息安全问题必须对二者进行区分。美国《健康保险可携带与责任法案》（Health Insurance Portability and Accountability Act，HIPAA）定义了医疗行业安全问题和隐私问题。安全问题指医疗信息通过技术手段进行存储和传输过程中，保障信息保密性、完整性和可用性的相关问题。安全问题主要针对数据收集、保护和传播过程。隐私问题是通过不同形式、由不同用户对患者医疗信息进行保护[1]。安全问题更多地关注组织安全，而隐私问题更为关注个体保护。

2.3 医疗行业安全问题

2.3.1 网络安全 与一些大型企业相比，国内医院在网络安全建设、运营和保障方面存在不足，整体抵御威胁攻击能力较弱，这是因为医院信息化建设历程存在特殊性。在医院信息化建设初期主要考虑内部医疗业务需求，较少考虑为患者提供信息化医疗服务，此时网络建设主要是为满足院内局域网使用需求，不需要与外部系统互联互通[3]。随着“互联网 + 医疗”时代的来临医院信息化建设越来越多地考虑患者信息化服务需求，包括在线预约、挂号、诊疗、手续办理、缴费、查看检查结果等。此外医院还将从医疗、医保、医药“三医联动”角度推动互联网与医疗健康服务相融合并制订、完善相关配套政策，加快实现医疗健康信息互通互享，提高医院管理和便民服务水平[4]。推进业务线上化需要打通医院局域网和互联网，实现数据传递与共享，医院网络开放程度提升，为网络安全带来巨大挑战。虽然近年来医疗行业针对网络开放性带来的风险采取了相应措施，医院日益重视网络安全，但我国医院网络安全依然存在一些问题。在硬件设备方面，许多医院交换机等网络核心设备老化，更新换代不及时，难以匹配较为先进的安全防护技术。在软件方面，医院信息系统底层技术架构普遍较老旧，存在大量安全漏洞，无法充分防御网络入侵。在管理方面，部分医院网络安全管理制度不规范、不健全，并未根据院内实际情况制定网络安全管理制度；部分医院制定相关管理制度落实不到位。在人员方面，大部分医院重视医学人才引进，对信息化特别是网络安全人才重视不足，现有人才技术能力水平普遍偏低。医院网络安全建设落后于“互联网 + 医疗”发展速度是导致医院网络安全问题的主要原因。

2.3.2 数据安全 除医疗信息外医疗行业数据还包括医院财务、管理信息等，其中任何一种数据被破坏或泄露都会造成难以估量的后果[5]。在“互联网 +”背景下医院信息化程度日益加深，医院信息系统所产生数据如果得不到有效保护可能造成巨大损失。因此保障医院信息系统数据保密性、完整性和可用性是信息化建设过程中需要解决的重要问题。在实际医疗情境中由于医院信息系统间数据交互存在隐患，医院信息化建设在数据安全方面仍有较大风险。医院网络开放带来的数据交互共享存在于医疗机构信息化流程中的各个环节。纵向来看，国家卫生健康委员会、县级医院、村级卫生院等不同层级单位信息终端点多面广，安全防护能力参差不齐，数据泄露出口众多。横向来看，医保系统需要与医院系统、有关主管部门和医保定点药店对接，数据传输需经过银行、运营商等行业外部机构，进一步增大了数据安全风险[6]。

2.4 医疗行业中的隐私问题

2.4.1 概述 医疗行业中，用户隐私是指在不对

其他人以及社会造成利益影响的情况下，不愿意让他人和社会了解的信息[7]。由于医疗行为的特殊性，隐私信息被不当使用的风险较高，同时存在医疗信息隐私与医方知情权之间的矛盾。

2.4.2 隐私不当使用 医疗信息化使敏感隐私信息被不当使用的风险提升。医疗保健服务提供者保存和共享、维护大量敏感医疗信息，用于诊断和治疗、支付保健服务费用、公共卫生研究，甚至用于营销和媒体宣传。从管理角度来看，目前我国医疗领域关于隐私保护法律文件中存在薄弱点，部分领域存在空白，导致隐私不当使用的成本较低。此外当医疗机构对从业人员进行考评时较重视医疗质量，较少将患者隐私保护纳入评价体系内，导致部分医疗行业从业者对患者隐私保护重视程度不足。从技术角度来看，虽然传统基于纸质媒介的信息系统存在缺陷，但其限制了信息收集者共享和传播信息的行为，在一定程度上避免隐私信息不当传播。随着医疗保健行业数据收集、存储和传输信息化程度日益加深，医疗信息可以轻松被定位、收集和传输，如果不对信息技术使用加以规范，将会大幅提升敏感隐私信息被不当使用的风险。

2.4.3 隐私权与医方知情权之间存在矛盾 在许多医疗场景下患者隐私权与医方知情权之间存在矛盾。医方知情权是指医方在使患者恢复健康过程中，知晓患者本次病情中所有相关医疗信息的权利。医疗过程中医方知情权与患者隐私权之间存在一定冲突。为了使患者恢复健康，医方只有得到足够的医疗信息才可以对病情做出正确诊断，难免会触碰到患者医疗隐私[8]。由于“互联网 +”背景下信息化技术在医疗领域广泛应用带来信息安全风险，患者担心健康信息被不当使用或泄露进而造成危害和损失，有时会采取极端措施来保护个人健康信息隐私。有调查显示近 1/6 的美国成年人采取极端措施保护个人医疗信息隐私，例如向医生隐瞒信息或提供不准确、不完整信息，导致医生无法给予最佳诊断和治疗。同时不准确的健康信息影响下游用户信息利用，医疗保健体系可能遭到破坏[1]。在保证患者恢复健康的同时如何最大程度减少对患者医疗隐私的侵犯是医疗从业者必须思考的问题。

3 我国医疗行业信息安全政策分析

3.1 有关政策

3.1.1 2011 - 2015 年 2011 年原卫生部发布《卫生行业信息安全等级保护工作的指导意见》和《关于全面开展卫生行业信息安全等级保护工作的通知》，提出通过等级保护方式保障医疗行业信息安全。2015 年 3 月国务院办公厅发布《全国医疗卫生服务体系规划纲要（2015 - 2020 年）》，提出要依托国家电子政务网构建与互联网安全隔离，联通各级平台和各级各类卫生计生机构，高效、安全、稳定的信息网络[9]。同年 5 月国务院办公厅发布《关于城市公立医院综合改革试点的指导意见》，提出加强区域医疗卫生信息平台建设，完善技术标准和安全防护体系，强化信息技术标准应用和数据安全管理。

3.1.2 2016 - 2018 年 2016 年国务院办公厅发布《关于促进和规范健康医疗大数据应用发展的指导意见》，提出加强健康医疗大数据保障体系建设策略，要求加强对涉及国家利益、公共安全、患者隐私、商业秘密等重要信息的保护，加强医学院、科研机构等方面的安全防范[10]。同年《网络安全法（草案）》对外征求意见，针对保障网络空间主权安全、产品应用和服务网络安全、网络数据信息安全、网络安全监测预警以及突发事件应急处置预案等内容进行规定。2017 年《网络安全法》实施，将网络安全领域相关要求上升至国家法律层面。2018 年 4 月国务院办公厅发布《关于促进“互联网 + 健康医疗”发展的意见》，提出“互联网 + 医疗健康”发展需要加强行业监管和安全保障，即强化质量监管和保障数据信息安全；同时要求研究制定健康医疗大数据确权、开放、流通、交易和产权保护法规，严格执行信息安全和健康医疗数据保密规定，建立完善个人隐私信息保护制度。同年 7 月国家卫生健康委员会发布《国家健康医疗大数据标准、安全和服务管理办法（试行）》，其进一步明确了各级卫生健康行政部门、各级各类医疗卫生机构、相关应用单位及个人在健康医疗大数据标准管

理、安全管理、服务管理中的责、权、利，对于统筹标准管理、落实安全责任、规范数据服务管理具有重要意义[11]。

3.1.3 2019－2021 年 2019 年 9 月国家发展改革委发布《促进健康产业高质量发展行动纲要(2019－2022 年)》，提出建立健全健康医疗大数据的信息共享、数据安全、隐私保护政策和应急保障机制；推进健康医疗大数据的安全共享，深化健康医疗大数据在医学科研、教育培训、临床诊疗、产品研发、行业治理、医保支付等方面应用。同年 12 月我国颁布卫生健康领域第 1 部基础性、综合性法律《中华人民共和国基本医疗卫生与健康促进法》，明确规定国家应采取措施推进医疗卫生机构建立健全信息安全制度，保护公民个人健康信息安全，对医疗信息安全制度、保障措施不健全，导致医疗信息泄露和非法损害公民个人健康信息的行为进行处罚[12]。2020 年 10 月工信部和国家卫健委联合发布《关于进一步加强远程医疗网络能力建设的通知》，提出进一步加强远程医疗网络能力建设需要加强组织保障，建立协同工作机制，完善“互联网＋医疗健康”网络标准体系，重点推进包括网络安全在内的总体性标准，加强远程医疗网络质量监测管理。2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，该法对行业数据安全管理、个人数据隐私保护等方面进行明确规定，成为我国数据安全治理体系的重要基础[13]。同年 8 月十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，该法明确要求处理生物识别、医疗健康、金融账户、行踪轨迹等敏感个人信息应取得个人单独同意。

3.2 存在的不足

3.2.1 安全法规体系不健全 我国医疗行业现行的信息安全政策主要聚焦安全性问题，对隐私性问题关注不足。首先，医疗行业隐私性问题立法较晚。自 2011 年首次在医疗卫生行业发布相关政策以来，我国通过等级保护在技术层面对医疗行业的信息安全问题进行保障并通过一系列政策规范安全性层面的管理问题。2016 年首次从国家层面对医疗行业的隐私保护问题提出要求。其次，对医疗行业隐私问题的全流程管控不全面。虽然已从国家层面颁布针对个人信息保护的有关法律，但缺乏针对医疗行业的隐私保护法规体系。现有对医疗行业隐私保护的要求和规定散落在不同法规中，缺乏从医疗行业隐私信息的产生、流转、保存、消亡的全流程建立完整的法律制度和管控体系。最后，对患者隐私权和医方知情权的矛盾缺少法律规范，没有定义医疗行为过程中患者与医方在隐私保护领域的权利范围，权责划分不清晰。

3.2.2 政策对行业信息安全管理支撑不足 我国医疗行业信息安全立法滞后于行业信息化建设进度，难以为行业信息安全管理提供支持。我国医疗行业信息安全立法开始于“十二五”时期，在立法初期相关法规较不完善，大量领域存在空白。进入“互联网＋”时代后，虽然我国加快了医疗行业信息安全立法速度，但总体进度仍然滞后于信息化发展速度，难以满足信息化、数字化、智能化建设过程中对网络及信息安全的管理需求。

3.2.3 政策可落地性不足 目前我国相关政策和法律法规条文对于具体权利、义务和责任划分有待进一步明确，实际操作中存在一定困难，也影响医疗行业政策落实效果。例如《网络安全法》中规定网络运营者不得泄露、篡改、损毁其收集的个人信息，但对于违规行为将处以何种形式的惩罚并没有进行明确规定。在医疗信息隐私保护方面，对于医疗信息中的敏感信息和隐私信息也没有专门制定统一的定义和标准[14]。

4 美国医疗行业信息安全法律体系借鉴

4.1 HIPAA 法案

美国医疗健康信息安全立法多以隐私权保护作为基础，HIPAA 法案是美国健康医疗信息安全保护体系的核心。经过 20 多年的修订与完善 HIPAA 及其补充法案已成为一套相对完善、系统并具备较强可操作性的健康医疗信息保护专门法。其要求采用健康信息和患者信息电子传输的国家统一标准，规

定在记录和传输医疗信息的过程中最基本的信息安全要求。HIPAA 安全要求涉及对象广泛，包括生成或以其他方式处理电子病历和医疗数据的任何组织。

4.2 其他法律

2009 年美国颁布《经济和临床健康信息科技法案》（Health Information Technology for Economic and Clinical Health Act，HITECH），该法案是对 HIPAA 的进一步扩展，增加对违反 HIPAA 的处罚规定[15]。随着互联网覆盖范围不断扩展，医疗行业健康类 APP 的广泛使用带来严重的信息安全问题。对此美国国会提出《停止销售和披露可穿戴设备、追踪器中消费者健康数据法案》《信息透明于个人数据控制法案》《保护个人健康数据法案》等多项关于公民健康信息安全的综合性立法建议，以构建医疗信息传输、出售、共享的监管框架[16]。

4.3 行业监管

美国通过一系列立法加强和促进医疗行业信息安全政策的实施和落地。美国卫生与公共服务部（United States Department of Health and Human Services，HHS）修订《个人信息隐私保护标准和实施指南》，从国家层面制定法规保护医疗信息的完整性、机密性和可用性。2016 年美国联邦贸易委员会（Federal Trade Commission，FTC）发布《FTC 针对移动健康应用程序开发人员的最佳实践指南》，对移动健康应用程序能获取的用户数据和权限进行规定。2018 年美国食品药品管理局（Food and Drug Administration，FDA）发布《医疗器械网络安全管理上市前提交内容指南草案》，通过加强医疗行业网络与信息安全管理，在网络安全攻击事件中保障患者免遭延迟治疗的伤害[16]。

5 我国医疗行业信息安全发展建议

5.1 完善医疗行业信息安全立法保障

我国尚缺乏关于医疗行业信息安全和隐私性问题的相关法律法规，亟待建立医疗行业信息安全保障的专门性、常态性法规体系。现行法律文件中虽然规定了医疗行业机构必须保障患者健康信息安全，但处罚机制尚不明确，医疗信息不当使用的成本较低，政策及法律震慑性不足。对于责任主体，不仅要规范医疗行业从业人员行为，还需对健康信息化平台信息收集、使用、存储、传输等行为进行规范，对从业人员和患者责任范围进行明确划分。同时应加快我国医疗行业立法相关进程，紧跟时代特点，聚焦行业问题，实现对行业信息安全管理的有效支撑。

5.2 健全医疗行业信息安全监管政策

我国医疗行业监管为上级监管部门对医疗机构信息安全的管理提供一定指导，目前尚缺少针对医疗行业信息安全政策实际落地的监管机制。首先，应完善并明确现有政策及法规中部分权利和责任划分、界定，使落实行业监管工作有据可依。其次，应在现有政策及法规基础上制定细化、专门化的指导性实施细则并指定相关风险评判工具，使医疗行业信息安全管理工作真正落到实处。

5.3 加强组织管理和文化建设

良好的组织和安全文化是使信息技术发挥其潜力的重要因素。目前医疗卫生行业从业人员更多关注的是医疗信息使用，而对医疗信息安全管理重视不足。行业信息安全措施能否真正有效落地取决于医疗从业人员信息安全意识水平。增强医疗行业全员信息安全意识，需要在行业内形成安全和保密文化，持续开展信息安全培训和意识宣贯，医疗行业管理组织需通过持续教育、奖励等手段加强相关人员的信息安全意识。

5.4 优化医疗行业信息安全技术手段

目前我国绝大部分医院仅靠网络防火墙保障医疗信息安全，新一代网络安全设备及技术应用率低于 50%[17]。提升医疗行业信息安全防护整体水平是“互联网 +”背景下信息化、数字化、智能化建设中的重要一环。医疗行业应按照等级保护 2.0 要求持续开展等级保护工作，针对不同信息系统制定

科学保护措施。同时广泛推广网闸、防入侵系统、防毒墙、上网行为管理等设备和系统，从网络层面增强网络及信息安全保护能力。此外在数据方面要实现医疗信息转码和加密并隐匿个人基本信息。

6 结语

自“十二五”以来我国医疗行业信息安全管理体系建设取得了一定成效，但相对于发达国家而言仍存在一定差距。在“互联网 +”时代背景下，分析我国医疗行业存在的信息安全与隐私性问题以及有关政策现状，借鉴美国医疗行业信息安全法规体系建设经验，以期为我国医疗行业信息安全管理未来发展提供有益参考。

参考文献

1 Deshmukh P, Croasdell D. HIPAA: Privacy and Security in Health Care Networks [M]. Hershey: IGI Global, 2008: 2770 – 2781.

2 李国红. 论医疗领域个人信息及民法保护 [D]. 苏州: 苏州大学, 2013.

3 胡新龙, 李怀成. 互联网 + 医疗健康模式下的医院网络安全防护 [J]. 中国卫生信息管理杂志, 2019, 16 (4): 462 – 466.

4 国务院办公厅. 国务院办公厅关于促进“互联网” + 医疗健康发展的意见 (国办发〔2018〕26 号)[EB/OL]. [2018 – 04 – 28]. http://www.gov.cn/zhengce/content/2018 – 04/28/content_ 5286645.htm.

5 陈卓. 县级医院数据安全管理的典型应用 [C]. 杭州: 中华医院信息网络大会, 2011.

6 袁琛. 医疗行业数据安全探析 [J]. 医学信息学杂志, 2016, 37 (2): 43 – 46.

7 高玉玲. 医疗行为中患者隐私权保护存在的问题和对策 [J]. 中国卫生事业管理, 2003, 19 (12): 738 – 739.

8 陶爱军. 论个人医疗信息的隐私保护 [D]. 重庆: 西南政法大学, 2010.

9 国务院办公厅. 全国医疗卫生服务体系规划纲要 (2015—2020 年) [J]. 中国实用乡村医生杂志, 2015, 22 (9): 1 – 11.

10 红梅, 宗慧娟, 王爱民. 计算机网络信息安全及防护策略研究 [J]. 价值工程, 2015, 34 (1): 209 – 210.

11 周君怡, 陈敏. 医疗 App 数据泄露防范策略研究 [J]. 中国医院管理, 2020, 40 (8): 71 – 72.

12 国家卫生健康委员会. 中华人民共和国基本医疗卫生与健康促进法 [J]. 中国实用乡村医生杂志, 2020, 27 (10): 1 – 9.

13 全国人民代表大会常务委员会. 中华人民共和国数据安全法 [J]. 中华人民共和国全国人民代表大会常务委员会公报, 2021 (5): 951 – 956.

14 王乐子, 母健康, 朱翀, 等. 国外医疗信息化领域隐私数据保护现状及其启示 [J]. 医学信息学杂志, 2019, 40 (2): 40 – 46.

15 杨朝晖, 简雅娟, 李树荣. 美国和欧盟基于个人健康记录隐私和安全的法律框架比较及对我国的启示 [J]. 医学与社会, 2019, 32 (11): 129 – 132.

16 徐文轩, 刘博言, 张雪. “互联网 +” 视域下美国健康医疗信息安全管理对我国的启示 [J]. 中国医学伦理学, 2021, 34 (3): 302 – 308.

17 中国信息通信研究院安全研究所, 腾讯科技 (深圳) 有限公司, 卫生信息安全与新技术应用专业委员会. 数字医疗网络安全观测报告 (2020) [R]. 深圳: 中国信息通信研究院安全研究所, 2020.