“互联网 + 医疗服务”体系下患者隐私权保护研究*

张宇清

（湖北中医药大学人文学院 武汉 430065）

〔摘要〕 分析我国“互联网 + 医疗服务”体系的构成，比较其与传统医疗服务模式下患者隐私权保护的不同，在对国内外立法现状进行调研的基础上提出“互联网 + 医疗服务”体系下患者隐私权保护面临的挑战，从完善立法、加强监管、改进技术等方面提出具体建议。

〔关键词〕 “互联网 + 医疗服务”；患者隐私权；个人信息

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2019. 01. 002

Study on the Protection of Patients´Right to Privacy under the System of "Internet + Medical Service"

ZHANG Yuqing, *Humanities College of Hubei University of Traditional Chinese Medicine*, *Wuhan 430065*, *China*

〔**Abstract**〕 The paper analyzes the composition of the system of "Internet + medical service" in China, compares differences of the protection of patients´right to privacy with the traditional medical service mode. It also comes up with the challenges confronting the protection of patients´right to privacy under the aforementioned system on the basis of study on the legislative situation home and abroad, proposes specific suggestions in the aspects of improving legislation, enhancing supervision and advancing technology, etc.

〔**Keywords**〕 "Internet + medical service"; patients′ right to privacy; personal information

1 引言

2018 年 4 月国务院发布《关于促进“互联网 + 医疗健康”发展的意见》，明确指出要健全“互联网 + 医疗健康”服务体系，完善“互联网 + 医疗健康”支撑体系，同时加强行业监管和安全保障。医疗健康往往涉及个人隐私，“互联网 + 医疗服务”体系下更需要面对严肃的隐私安全问题。

2 “互联网 + 医疗服务”概述

2.1 概念

“互联网 + 医疗”是以互联网技术为手段，用虚拟的方式组织医疗资源，将部分可以通过非现场方式进行的服务转移到互联网平台，为不同消费群体提供医疗、保健服务。

〔收稿日期〕 2019 - 01 - 16

〔作者简介〕 张宇清，讲师，发表论文 10 余篇。

〔基金项目〕 2016 年度四川医事卫生法治研究中心资助一般项目“‘互联网 + 医疗’相关法律问题研究”（项目编号：YF16 - Y10）。

2.2 体系（图 1）

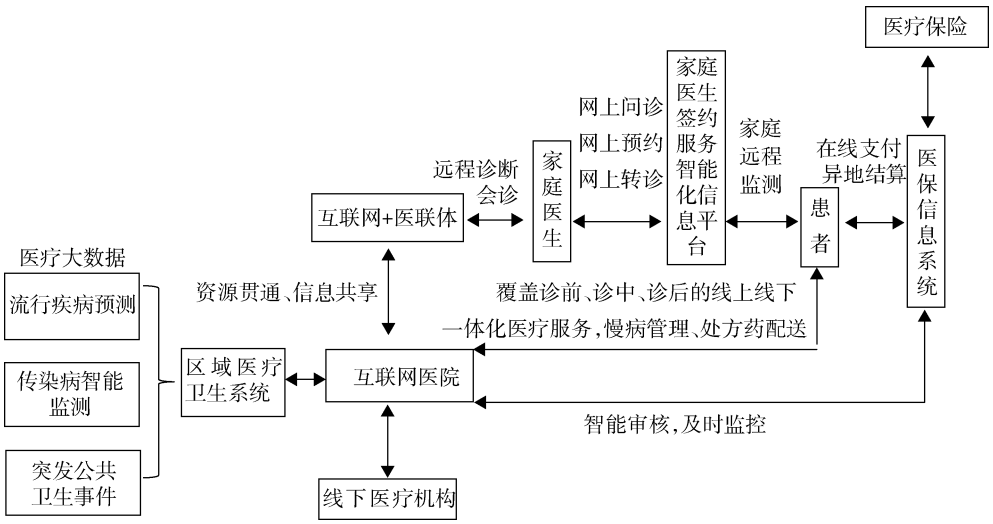

图 1 “互联网 + 医疗服务”体系

2.3 类型（图 2）

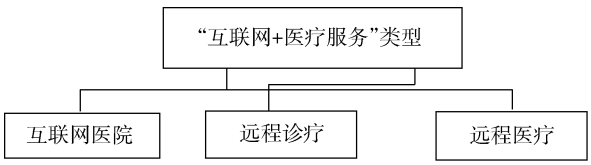

图 2 “互联网 + 医疗服务”类型

2.4 相关政策梳理（表 1）

表 1 2017 – 2018 年“互联网 + 医疗服务”相关政策

发布时间	文件名	发布机构
2017. 02	《电子病历应用管理规范（试行）》	原国家卫生计生委
2017. 11	《关于加强互联网药品医疗器械交易监管工作的通知》	国家食品药品监督管理局
2018. 04	《全国医院信息化建设标准与规范（试行）》	国家卫健委
2018. 04	《关于促进“互联网 + 医疗健康”发展的意见》	国务院办公厅
2018. 07	《关于深入开展“互联网 + 医疗健康”便民惠民活动的通知》	国家卫健委、国家中医药管理局
2018. 08	《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》	国家卫健委医改医管局

续表 1

2018. 09	《互联网诊疗管理办法（试行）》	国家卫健委、国家中医药管理局
2018. 09	《互联网医院管理办法（试行）》	同上
2018. 09	《远程医疗服务管理规范（试行）》	同上
2018. 09	《国家健康医疗大数据标准、安全和服务管理办法（试行）》	国家卫健委
2018. 11	《进一步改善医疗服务行动计划（2018 – 2020 年）考核指标》	国家卫健委

3 “互联网 + 医疗服务”体系下患者隐私权概念体系

3.1 隐私权

3.1.1 概念 指自然人所享有的生活安宁与信息秘密依法受到保护，不被他人非法侵扰、知悉、收集、利用和公开的一种人格权。权利主体对他人在何种程度上可以介入个人私生活，对是否向他人公开隐私以及公开的范围和程度等具有决定权。

3.1.2 隐私与个人信息 个人信息是指与特定个人相关联、反映个体特征、具有可识别性的符号系统，包括个人身份、工作、家庭、财产、健康等各方面的信息[1]。而隐私包含的内容大多是具有私密

性的个人信息，对隐私的侵害主要是非法披露和骚扰。关于个人隐私和个人信息两者关系，理论界有两个主流观点：一种观点认为个人信息与个人隐私既相互重合又有所区分；另一种观点认为个人信息中包含个人隐私。若将个人信息分类，笔者认为可根据是否具有隐私价值进行分类：一类是不具有隐私价值的个人信息，另一类则相反，如个人医疗信息等具有一定的私密价值，应该受到隐私权制度的高度关注与保护。

3.2 患者隐私权

指患者所享有要求医疗机构及医务人员保护合法掌握的涉及患者个人各种隐私以及不被非法侵犯的权利。患者隐私权的保护范围主要包括信息和空间隐私权，具体指的是隐私部位、个人诊疗信息、个人信息、私人空间等。

3.3 “互联网 + 医疗服务”体系下的患者隐私权

“互联网 + 医疗服务”体系下的患者隐私权在主体、客体、内容、性质方面都有独特之处，是指患者对与个人健康、身份有关，以大数据形式储存在电子媒介上，具有医疗和经济价值，经权利人或医疗健康机构采取保密措施的个人敏感信息和健康信息等所享有的自由支配、控制、不被他人非法侵扰的具体人格权[2]。

4 国内外患者隐私权保护立法现状

4.1 国外

4.1.1 单独立法 在隐私保护基本法的框架下对患者隐私权单独立法，制定执行标准。1974 年美国制定隐私保护的基本法《隐私权法》。1996 年《健康保险流通与责任法案》（Health Insurance Portability and Accountability，HIPPA）颁布，对医疗信息化中的交易规则、医疗服务机构及从业人员的识别、医疗信息安全、医疗隐私、健康计划识别、患者识别等问题有着详细规定，有效地保护医疗数据安全和患者隐私权。HIPAA 中确立保护患者隐私权的相关制度，包括最小程度披露、知情同意、管理简化、患者医疗记录查看权制度等。2000 年美国卫生和福利部（Health and Human Service，HHS）制定《个人可识别健康信息的隐私标准》，基本建立完整、操作性强的隐私保护法律体系。澳大利亚的《健康记录与信息隐私权》（2002 年）有效平衡电子健康记录的发展和维护以及个人信息隐私之间的冲突。法国颁布《医疗隐私法》和《医疗保险法》等。

4.1.2 综合保护 将个人医疗隐私信息纳入个人信息，对其加以综合保护。欧盟 1995 年的《关于在个人资料处理和个人资料自由流通过程中对个人资料进行保护的指令》要求成员国务必在 3 年内完成个人信息保护法的修改以保持与该法令的一致性，该法案还特别提出对敏感信息的使用与保护规则。英国的《数据保护法》（1998 年）将健康、基因等医疗信息归属到个人私密信息予以严格保护。加拿大的《个人信息保护与电子文件法》（The Personal Information Electronic Documents Act，PIPEDA）中禁止跨省或跨国商业机构使用个人健康信息数据。

4.2 国内

4.2.1 涉及隐私权保护的法律法规 包括《宪法》（第 38 条、第 39 条、第 40 条），《民法总则》（第 110 条），《侵权责任法》（第 2 条、第 62 条），《刑法修正案（九）》（第 245 条、第 252 条、第 253 条），《民事诉讼法》（第 68 条、第 134 条、第 156 条），《刑事诉讼法》（第 52 条、第 150 条、第 183 条），《行政诉讼法》（第 32 条）、《网络安全法》（第 4 章），《传染病保护法》（第 43 条）等。

4.2.2 涉及患者隐私权的法律法规 《侵权责任法》首次提出保护患者隐私，“医疗机构及其医务人员应当对患者的隐私保密。泄露患者隐私或者未经患者同意公开其病历资料，造成患者损害的，应当承担侵权责任。《执业医师法》规定“医师应当保护患者隐私”。《护士管理办法》要求“护士在执业中得悉就医者的隐私，不得泄露”。《网络安全法》要求“网络运营者应当对其收集的用户信息严格保密并建立健全用户信息保护制度”。强调“网络运营者应当采取技术措施和其他必要措施，确保个人信息

安全，防止信息泄露、毁损、丢失”。第 45 条针对“依法负有网络安全监督管理职责的部门及其工作人员”提出“不得泄露、出售或者非法向他人提供知悉的个人信息、隐私”。以上法律中患者隐私权都有所涉及，但是法条较为分散，多为原则性规定，缺乏相关的行业规范和标准，适用性不强、缺乏现实操作性。这种分散的立法模式已经无法满足我国“互联网 + 医疗健康”发展的法治需求。

5 “互联网 + 医疗服务”体系下患者隐私权保护面临的挑战

5.1 数据监测与收集——隐私无处躲藏

远程无线医疗监护通过无线传感器网络，在医疗健康监测领域的应用颇为广泛。患者足不出户就可以将个人相关健康监测数据传送给医院或其他医疗机构，医方对数据进行专业化处理和分析后告知患者或其家属诊断结果，实现患者在家就诊。但同时存在患者的医疗隐私信息会在未知情况下被暴露的危险。一些互联网医疗平台存在多个漏洞（登录绕过、未授权访问、平行越权等），攻击者甚至仅通过手机号就可以获取到患者姓名、身份证、就诊卡信息及挂号记录、化验检验报告单以及其他个人健康生理和医疗信息。对于网络犯罪分子来说，医疗隐私信息可能比财务数据更有价值。新加坡卫生部近期披露在 2015 年 5 月 1 日 – 2018 年 7 月 4 日期间访问 SingHealth 的患者，其个人数据均被黑客窃取，其中包括新加坡国家总理李显龙的医疗信息。被盗数据包括姓名、身份证号、家庭住址、性别、种族等，还有约 16 000 人的配药信息遭到泄露。美国《医疗机构面临的网络犯罪和其他威胁报告》称被盗的医疗保险身份证在黑色网站上至少售价 1 美元，医疗档案价格从每个 5 美元起。除来自外部的威胁，根据《受保护健康信息泄露报告》，遭遇医疗信息数据泄露事故的医疗机构中 57.5% 是内部人士所为，外部攻击者只有 42%。财务收益是内部威胁的主要动机，达到 48%。一方面，有些内部人员有权限获取用户的大量健康信息，但如果隐私权保护意识不强有可能致使大量医疗健康信息泄露甚至丢失；另一方面，少数内部人员受金钱利益驱使，复制、贩卖医疗健康信息，造成患者隐私泄露及滥用。

5.2 数据分享——隐私被滥用

在“互联网 + 医疗服务”服务活动中医疗大数据信息交流更加密集，使得区域性平台的电子病历系统得到更加迅速的推广。电子病历系统最初投入使用时是以各医疗机构为单位形成单独的数据集。目前一些地区通过与网络运营商合作，将医疗机构、保险公司以及医疗科研组织的相关数据整合后构建以电子病历数据为载体的共享平台，使得医疗数据和相关健康卫生数据信息的区域性共享成为可能。区域性医疗信息共享平台弥补基于医院信息系统（Hospital Information System，HIS）的局域网电子病历系统的不足，数据共享从医疗卫生机构内部扩展到其他的区域性医疗平台。然而电子病历系统网络化发展迅速，人们的医疗隐私数据有时会被有目的的人或机构作为商品进行贩售。如网络营销组织可以通过分析整合个人医疗信息数据对其投放量身定制的广告；一些单位或企业通过进入电子病历数据库而知晓其员工的健康状态，从而以此为由对员工进行筛选甚至解雇等。

5.3 数据挖掘——隐私被二次利用

“互联网 + 医疗服务”体系下无时无刻都持续产生着海量医学数据信息，在增进数据交互和共享的同时患者隐私面临被二次利用的侵权风险。患者隐私的一次使用是指直接获得患者隐私信息的过程，如互联网诊疗平台注册的账号、填写的个人信息等都是一次使用。二次使用则指对上述信息进行加工、分析、处理之后得到的结果并加以利用的过程。而隐私信息的二次使用大多未获得患者知情或许可，这就可能导致侵权风险。即便已经获得患者知情同意后使用隐私信息有时也无法确保语境在使用过程中的完整性，所以在挖掘数据其他潜在价值时这种方式很难落实。正如信息技术专家亨特所说：革新将不会是在收集数据方面——不是在卧室

安装电视摄像机，而是在分析已被同意共享的信息方面[3]。

5.4 数据预测——隐私被预测

在“互联网 + 医疗服务”时代背景下，患者隐私权保护所面临的挑战不仅限于隐私的直接泄露，还可能是通过有目的性地对这些隐私数据进行分析，从而预测信息主体的状态和行为。人们可以利用数据分析挖掘技术搜索相关数据信息，对信息主体所处的状态或喜好做出预判，以此来向其推销符合个人喜好的服务或产品而获取利润。如孕妇近期的搜索、浏览和购买记录都可以使人轻松推断出其可能怀孕，甚至可以判断出怀孕的状态和时间，而向其提供孕婴产品，这就可能引起一系列的推销诈骗问题。又如获取就医者的某些检查结果，即可对其当前的健康情况和下一步的行为做出推断。所以不能简单认为只要有数据隐私匿名处理技术和对高敏感重要信息的保护就足以确保患者隐私安全。

6 “互联网 + 医疗服务”体系下患者隐私权保护对策

6.1 构建层级保护模式

在“互联网 + 医疗服务”活动中，患者隐私被采集、整理、加工和处理，以数据的形式被记录下来。而这些信息必须区分保护，如果保护程度过高，虽全面有效，但会加重公共机构管理的负担；保护程度过低，公共机构负担虽减轻，但也增加隐私被侵害的风险。依据信息敏感程度、人身性以及对患者人格影响程度，从 3 个维度（患者身体、隐私、环境）来考量，通过隐私信息的经济价值和社会价值进行规整，可以将患者隐私信息分为 3 个层级。见表 2。在“互联网 + 医疗服务”体系下，应针对不同分类在对隐私信息的储存和使用中采用不同程度的保护方案。如对于敏感信息应区别于其他信息重点保护。另外患者对其医疗隐私信息享有支配权和控制权，在对隐私的使用和共享时应当进行深层次的授权同意。不同层级的隐私信息应实现不同的授权行为，如性功能障碍、流产记录、艾滋病病毒携带者等高敏感信息，不管是否出于医疗范畴内的目的，都应采取特别明示同意的方式予以授权，再配合一些数据技术手段对信息加以保护。

表 2 “互联网 + 医疗服务”体系下患者隐私信息层级结构

信息层级	具体内容	特点
敏感信息	电话号码、网络识别信息（qq、微信）传真号码、疾病诊断书、检查影像报告、生物识别符号（血型和指纹）、个人病史、个人基因信息、基因信息、性取向信息、家族病史等	医疗价值、商业价值较高，人身性较强。此类信息受侵害的可能性极大，且侵害后果严重，会造成严重的消极影响，所以应当受到重点保护
特殊信息	家庭地址、社会福利编号、医疗保险信息、证件号码、汽车牌照等	具有一定的医疗价值，受侵害的可能性较低，受侵害后对患者的伤害程度较低
一般信息	患者姓名、出生日期、与医疗活动相关的日期、个人账户、身高、体重信息等	与医疗活动无关，人身性不强。基本上没有医疗价值，受到侵害可能性低或受侵害后损害程度不高

6.2 重视直接保护，加大违法成本

《民法总则》已经确立隐私权作为一项具体人格权的独立地位，民法典各分编也已确定，其中人格权独立成编备受瞩目。在人格权编中应细化患者隐私权保护标准，明确患者隐私权的概念、范围、相关主体权利和义务，以列举的形式确定侵犯患者隐私权的行为，详细规定侵权责任的认定及举证责任。另外由于违法成本较低，处罚力度不足，导致个人隐私极易被泄露及滥用，贩卖个人隐私信息已形成完整的灰色产业链。所以应加大违法成本：其一，增加惩罚性赔偿的制度设计。此类惩戒或许不能威慑其他潜在的侵害人，但至少社会通过其法律制度宣告发现一定的非犯罪行为是应受谴责的[4]。

欧盟的《一般数据保护条例》中根据不同程度的违法行为有数额较高的罚款制度，最高可达数千万欧元。其二，对非法获取大量个人信息的黑客、数据管理人员内外勾结泄露个人信息的从严从重处理，对侵犯个人信息、电信网络诈骗等新型网络犯罪持续加大打击力度。其三，积极推进法律适用和落实执行等配套机制，提升犯罪成本，实现法律的指引与预测功能。

6.3 构建与完善医疗信息保护技术手段和数据管理体系

腾讯智慧安全在 2018 年底发布的《医疗互联网服务敏感数据泄露风险调查报告》中指出目前我国线上医疗服务系统普遍存在业务漏洞、敏感端口开放等安全问题，给未授权访问和不法黑客入侵带来便利，增加医疗数据的安全风险。国内有多家三甲医院接入的第 3 方医疗服务平台存在严重逻辑漏洞，这将导致平台就诊患者的个人信息包括姓名、手机号、身份证号以及就诊信息和医疗诊断数据等多达 10 余种敏感信息存在泄露风险。此外有 71% 的三甲医院存在高危端口开放情况，以近几年不法黑客攻击事件中出现频率较高的端口为参照，有超过 1/3 的医院将 SSH 登录、MySQL 数据库服务等高危端口直接开放于外网，易于不法黑客入侵以及未授权访问，增加医疗信息数据泄露风险。互联网医疗服务平台和医疗机构应建立标准化的患者隐私保护支撑体系。第一，设置专门防火墙，着力加强访问控制、加密、安全监控等技术手段的应用。第二，对数据存储设备及场所等进行必要的物理隔离和访问控制，有效防止隐私信息扩散和泄露。第三，制定严格的患者隐私保护规章制度，提高从业人员的保护意识，配备专门人员负责患者隐私保护工作，建立风险应对机制，妥善处理数据泄露等突发事件。

6.4 加强监管，建立协同联动执法机制

《关于促进“互联网 + 医疗健康”发展的意见》明确提出创新监管方式，切实防范风险，建立完善、有章可循的监管体系将是未来一项重要且艰巨的任务。首先，可借鉴国外做法，设立个人信息（包括隐私信息）保护的专门机构（如日本的个人隐私信息保护委员会、欧盟的数据保护官），主要工作范围包括接待投诉、投诉处理、落实赔偿和处罚等。该机构在必要时可以作为独立诉讼主体，代表公民利益，提起公益诉讼。其次，应强化消费者权益保护协会及检察机关公益诉讼的力度和广度，畅通患者隐私权的救济渠道。第三，加快制定与完善行业标准规范，确保各类医疗信息在收集、储存、开放、传输和共享过程中的风险可控，明确数据开放范围、权利、义务和责任。最后，多部门联动配合，一旦发生患者隐私泄露等信息安全事件，卫健委、网信、工信等应协同执法。建立常态化的巡视机制，重点巡视患者隐私保护情况。

参考文献

1 林亚婷. 人工智能时代下的个人信息保护［J］. 云南社会主义学院学报，2018（3）：15.
2 蒋言斌，李响. 我国医疗大数据患者隐私权保护及其模式选择［J］. 医学与法学，2018，10（1）：2.
3 吕耀怀. 当代西方对公共领域隐私问题的研究及其启示［J］. 上海师范大学学报（哲学社会科学版），2012，41（1）：25.
4 爱德华·怀特. 王晓明，李宇译. 美国侵权行为法：一部知识史［M］. 北京：北京大学出版社，2014：251.