

移动医疗 APP 隐私政策可读性及内容分析研究^{*}

李 为 沈 黎 吴 滢 刘 炜

(华中科技大学同济医学院附属协和医院计算机管理中心 武汉 430021)

〔摘要〕 分析我国移动医疗 APP 隐私政策的可读性及内容,指出存在的问题并提出建议,包括改善隐私政策的可读性、落实隐私保护相关法律法规、加强健康信息共享过程中隐私信息保护等。

〔关键词〕 移动医疗; 隐私政策; 个人信息保护; 内容分析

〔中图分类号〕 R-058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2022.09.005

Analysis and Study on the Readability and Content of Privacy Policy of Mobile Health APPs LI Wei, SHEN Li, WU Qing, LIU Wei, Computer Management Center, Union Hospital Affiliated to Tongji Medical College of Huazhong University of Science and Technology, Wuhan 430021, China

〔Abstract〕 The paper analyzes the readability and content of privacy policy of Mobile Health (mHealth) APPs in China, points out the existing problems and puts forward suggestions, including improving the readability of privacy policy, implementing relevant laws and regulations on privacy protection, strengthening privacy information protection in the process of health information sharing, etc.

〔Keywords〕 Mobile Health (mHealth); privacy policy; protection of personal information; content analysis

1 引言

世界卫生组织对移动医疗 (Mobile Health, mHealth) 的定义为通过使用移动通信技术如掌上电脑 (Personal Digital Assistant, PDA)、移动电话、移动式穿戴设备等无线设备提供医疗信息和服务^[1]。延伸到移动互联网领域,移动医疗 APP 是指基于安卓、iOS 等移动终端系统提供移动医疗

健康类服务的软件。近年来随着“互联网+医疗健康”的发展和推进,各行业主管部门、健康医疗机构、医疗服务提供商开始通过移动 APP 提供移动医疗保健服务。然而移动 APP 网络安全相关法律法规和标准体系发布较晚,导致人员安全意识薄弱、开发流程不规范等问题显著^[2-3]。目前国内学者针对移动医疗 APP 隐私安全进行研究,主要聚焦在以下领域:隐私视角下的用户研究^[4]、基于数据安全视角的移动医疗 APP 行业监管^[5]、数据安全相关的隐私保护技术^[6]等,但缺乏移动医疗 APP 背景下关于隐私问题的实证研究。本文分析、评估移动医疗类 APP 隐私政策可读性及内容,发现其存在的问题,以期移动医疗 APP 行业监管、用户隐私保护提供参考。

〔修回日期〕 2021-09-30

〔作者简介〕 李为,硕士,初级工程师,发表论文 4 篇;通信作者:刘炜,中级工程师。

〔基金项目〕 国家重点研发计划项目“医养结合服务模式与规范的应用示范”(项目编号:2020YFC2006000)。

$$Y=0.8\times X1+X2$$

2 资料与方法

2.1 研究对象

选择移动医疗类 APP 时，以应用商店官方数据提供商排行榜“蝉大师”作为数据源。该排行榜主要基于应用商店下载量、关键词覆盖率等指标建立综合指数，计算移动 APP 获取搜索流量的能力，能够反映 APP 受欢迎程度^[7]。研究以“医疗”为关键词，检索获得移动医疗类 APP 共 247 个。经人工筛查和核验抽样选择排名前 20% 的移动医疗类 APP 约 50 个，见表 1。

表 1 移动医疗类 APP 样本情况

分类	APP 名称
问诊咨询类	医鹿、丁香医生、智云健康、微医、春雨医生、小荷、好大夫在线、健康 160、左手医生、小鹿中医、平安健康、泰康医生、妙手医生、百度健康、京东健康、心理咨询壹点灵、智慧好医院
资讯文献类	医脉通、腾讯医典、全球医、梅斯医学
预约挂号类	健康云、慧医、预约挂号网、健康之路、金医宝、华医通
医药服务类	用药助手、药房网商城、叮当快药、人卫用药助手、1 药网、快速问医生
健康管理类	禾连健康、爱康、新氧医美、医联、BOE 移动健康、泓华医疗、薄荷健康、糖护士、医护到家、小豆苗、杭州健康通、优健康、大家中医、美柚
经验交流类	觅健、禾医助、云鹊医

2.2 研究方法

2.2.1 可读性分析 主要是从读者角度衡量文本阅读难度。中文文本目前尚无较为权威的可读性计量指标，部分研究者根据领域、使用场景设计不同计算方法，主要包括陈世敏公式^[8]、荆溪昱公式^[9]、李萍公式^[10]等。根据移动医疗隐私政策特点，本研究在陈世敏中文可读性公式基础上，结合秦克飞提出的针对简体中文所做的修正^[11]，通过可读性分数评估移动医疗 APP 隐私政策的可读性。具体计算公式为：

其中 Y 表示可读性分数，X1 表示每句平均字数，X2 表示难字百分比。计算总字数时汉字、中文标点、英文单词计 1 字；计算句子数时任意两个中文标点（书名号、括号、引号不计）之间的内容为 1 句；统计难字时参照《现代汉语常用字表》2 500 个常用字^[12]，不属于常用字的汉字计为难字。最终得到可读性分数表示具有相当于对应年限教育背景的读者可以理解文本内容。此外参考徐雷的研究选择是否有名词解释、是否有目录、是否标记重点内容等指标进行定性评估^[13]。

2.2.2 内容分析 主要是对抽样 APP 隐私政策内容进行标注和定性分析。依据国家标准《个人信息安全规范》个人信息保护政策模板开发基础编码指南^[14]。包括个人信息收集使用规则、个人信息保护措施、用户权利、儿童信息处理、个人信息转移、隐私政策更新、服务提供商联系方式 7 个方面。在此基础上基于 10% 的数据集随机样本试点分析，对编码指南进行修订，形成最终数据采集表单^[15]。根据表单对所抽取 APP 隐私政策进行分类、内容抽取和编码构建数据集。整个编码过程由两名编码员完成，遇到分歧时通过讨论解决，直到达成共识。最终采用描述性统计方法对数据集进行统计分析。

3 结果

3.1 可读性分析

根据移动医疗 APP 隐私政策的可读性分数分布情况，样本中可读性分数最高值是 12.48，为医护到家；可读性分数最低值是 8.23，为小豆苗。可读性分数平均值为 10.39，表示需要接受 10.39 年教育的人群才能够理解，其文化水平在我国相当于高中 2 年级水平。其中隐私政策的难字百分比均值为 0.85%，整体而言难字比例不高。每句平均字数均值为 11.95，如果以句号、惊叹号、问号作为 1 个完整语句的判断标准，隐私政策文本平均完整句句长为 68.25 字，说明隐私政策长句较多。长句阅读时间长、内容多、层次复杂，加大了用户理解的难度，见表 2。此外从定性分析中发现 48% 的隐私政

策提供名词解释，但均不涉及健康信息界定。70% 的应用提供目录，不具备链接到具体页面的功能，同时也未提供具体页码。62% 的应用标记重点内容，重点标记方式包括加粗、下划线、标红等。

表 2 移动医疗 APP 隐私政策可读性分数

序号	移动医疗 APP 名称	每句平均 字数 (X1)	难字百分比 (X2)	可读性 分数 (Y)
1	医护到家	14.54	0.85	12.48
2	健康云	14.34	0.68	12.16
3	糖护士	14.61	0.44	12.12
4	禾连健康	14.06	0.72	11.97
5	杭州健康通	13.24	1.31	11.90
6	药房网商城	14.03	0.64	11.87
7	禾医助	13.81	0.72	11.77
8	大家中医	13.54	0.79	11.62
9	快速问医生	13.68	0.58	11.52
.....				
50	小豆苗	9.54	0.60	8.23

3.2 内容分析

3.2.1 隐私信息收集 隐私信息收集分析包括对收集信息的功能、目的、内容的分析。功能分析研究结果显示 72% 的应用列举了所有需要收集个人信息的业务功能。在描述收集个人信息内容时，60% 的应用分别使用“例如”“等”以及省略号这些概括性词语或符号。目的分析中发现 52% 的应用需要通过所收集信息进行用户画像，80% 的应用需要根据数据改进功能，66% 的应用需要对用户信息进行分析和研究，78% 的应用需要利用用户数据进行机器学习或模型算法训练，66% 的应用则为了广告服务或商品推广而收集用户数据。此外 56% 的应用提出为了安全保障而使用或整合用户信息以判断用户账号风险，检测及防范安全事件。根据所收集内容分析结果，国家标准将敏感信息定义为财产信息、健康生理信息、生物识别信息和身份信息，结果显示所有 APP 均涉及收集用户的敏感信息。其中 86% 的应用会收集个人身份信息；28% 的应用表示会收集用户生物识别信息，如用户指纹或面容等数据；

64% 的应用明确表示需要收集用户银行卡或支付宝等信息。

3.2.2 隐私信息共享、公开与转让 结果显示样本中所有移动医疗 APP 均具备与第 3 方共享信息的功能，其中 70% 的隐私政策提到共享信息范围，而仅有 42% 的应用具体描述共享信息内容。此外 70% 的应用提及共享前会对个人信息做去标识化处理，62% 的移动医疗 APP 明确在共享前会与第 3 方签订用户信息保密协议。96% 的移动医疗 APP 提到公开披露用户个人信息的条款。84% 的移动医疗 APP 表示存在个人信息转让的情况，在得到用户授权同意或涉及服务提供商合并、收购或破产清算时会转让用户个人信息。

3.2.3 隐私信息保护 94% 的移动医疗隐私政策声明对用户个人信息会采取一定保护措施；80% 的应用明确描述所采取具体措施或技术，例如在用户浏览器与服务器交换数据时采取安全套接层协议 (Secure Sockets Layer, SSL) 加密保护、使用超文本传输安全协议 (Hyper Text Transfer Protocol Secure, HTTPS) 安全浏览方式、对用户数据进行加密等；仅 34% 的应用明确指出其通过的安全认证，见表 3。

表 3 移动医疗 APP 安全认证情况

安全认证名称	通过认证的 APP 数量
网络安全等级保护标准 3 级	16
ISO27001 信息安全管理体系认证	7
第 3 方支付行业数据安全标准 (Payment Card Industry Data Security Standard, PCI-DSS)	2
可信云服务认证	1

3.2.4 用户权利 结果显示 80% 的移动医疗 APP 明确提出用户享有访问、更正、删除个人信息以及改变应用内授权同意范围的权利。24% 的 APP 表示用户可以选择推广或广告信息的偏好。仅 20% 的 APP 指出用户可以通过应用获得个人信息副本。

3.2.5 政策更新及联系方式 研究结果显示 72% 的移动医疗 APP 标识隐私政策的更新时间，但只有 8% 的 APP 标识更新内容，30% 的应用具备历史政

策查阅入口。此外 86% 的移动医疗 APP 提供联系方式, 其中 44% 的 APP 明确给出专门处理个人信息安全问题的反馈渠道。

4 结论

4.1 隐私政策可读性较低

中国互联网络信息中心 (China Internet Network Information Center, CNNIC) 第 47 次互联网络发展状况统计报告显示, 截至 2020 年 12 月网民学历结构中具有初中及以下学历人数占比 59.6%, 具有高中、中专及以上学历占比 40.4%^[16]。对照结果中需要读者文化水平达到高中 2 年级的要求, 显然其难度超过了大多数网友水平, 可读性较低。文本长句较多、结构层次复杂, 无形之中造成读者理解障碍。此外移动医疗 APP 隐私政策缺乏对健康信息术语、名词的范围说明和意义解释, 所提供辅助读者理解的形式功能简单、结构单一, 缺少表格、图片等表达形式, 所提供目录仅提取 1 级标题, 缺乏页码和导航功能, 并没有提高移动医疗 APP 隐私政策可读性, 最终可能导致读者误解信息, 从而影响到用户的健康信息行为^[17]。

4.2 用户知情同意权受到侵犯

在个人医疗数据利用中, 所谓知情是指数据主体对数据利用中收集、分析以及共享各环节都明确了解; 所谓同意则涉及数据主体自主权, 数据利用者不得以引诱、哄骗甚至欺诈的方式征得同意^[18]。研究中大多数移动医疗 APP 在描述所收集信息时运用概括性词语, 并没有完全列举所收集信息内容, 并且相当一部分 APP 未说明需要收集信息的功能, 在数据收集环节用户知情权受到侵犯。此外绝大多数移动医疗 APP 在用户首次登录时选择是否同意隐私政策, 并未直接显示政策内容, 用户可以选择不阅读而直接同意。这在一定程度上促使用户跳过阅读过程, 妨害用户同意权, 该情形下即使用户点击同意也并不能证明用户具备理解、接受、承担隐私条款的能力。

4.3 移动互联网络安全等级保护不足

国家卫生健康委员会在《关于加强全民健康信息化标准化体系建设的意见》中指出要完善医疗卫生行业网络安全标准体系, 推进网络安全等级保护。网络安全等级保护明确提出移动互联安全的扩展要求, 其中包括移动应用管控、移动应用软件开发等重要内容^[19]。但移动医疗 APP 对该政策的执行力度远远不够, 绝大多数没有取得任何信息安全相关的权威认证, 未按照网络安全等级保护的要求开展网络安全保护工作。

4.4 健康信息共享缺乏保障

2021 年 8 月 20 日发布的《中华人民共和国个人信息保护法》明确指出个人信息处理者向其他个人信息处理者提供其处理的个人信息时, 应当向个人告知接收方名称、联系方式、处理目的、处理方式和个人信息的种类。而绝大多数移动医疗 APP 在其隐私政策中没有明确指出共享的第 3 方名称, 也没有提到具体共享内容, 这意味着用户无法获知个人信息流向。此外存在不少应用共享时未与共享方签订保密协议, 也未对共享数据做任何处理, 违反了《个人信息保护法》中关于个人信息处理者有义务采取相应的加密、去标识化等安全技术措施的要求, 这将直接导致健康信息共享过程缺乏安全保障。

5 建议

5.1 改善并提高隐私政策可读性, 加强用户理解

隐私条款是用户能够明确获知移动医疗 APP 个人隐私信息处理策略的有效来源, 是服务提供商与用户交互、获取用户信任的桥梁, 不应人为设置障碍。从结构编排上, 隐私政策需按照国家标准《个人信息安全规范》进行编排设计, 尽可能采用规范、清晰的框架结构。从语言运用上减少非常用字、专业词汇、模糊表达的使用, 尽量不要使用过长完整句表达, 降低用户阅读难度。从辅助阅读上, 对于含义复杂、内容丰富的内容采用名词解

释、重点标记、图表等形式加强用户对文本的理解。从内容指引上,设置目录索引提高导航性,通过点击目录标题能够实现跳转到相应内容,便于用户阅读。

5.2 落实隐私保护相关法律法规,建立行业审查机制,保护用户权利

国家已出台《网络安全法》《数据安全法》《个人信息保护法》,通过立法形式强调信息安全和个人隐私保护的重要性。同时国家卫生健康委员会也强调建立以网络安全等级保护为核心的医疗卫生行业安全认证体系。但从结果看移动医疗服务提供商并未完全按照法律要求和行业准则执行。因此应进一步在移动医疗行业加大相关法律法规和网络安全等级保护认证的执行力度,并将执行情况作为应用市场准入的标准和依据,严格对上架应用的资质审查。对于隐私政策设置不符合要求、非法侵犯用户知情同意权和隐私权的移动医疗应用,责令其下架整改。同时建立隐私政策整改、执行情况的监督机制,杜绝隐私安全风险,保护用户合法权利。

5.3 加强健康信息共享过程中隐私信息保护

随着医疗大数据的发展以及互联互通的深度应用,移动医疗应用除了现阶段与软件服务提供商进行集成及数据交互外,将来可能会与医院信息系统、区域医疗信息平台等进行对接。如果按照移动医疗服务提供商目前关于健康信息共享条款设置共享策略,患者隐私数据在跨系统、跨平台、跨业务流通时将面临巨大挑战。因此移动医疗服务提供商除了进一步明确所有共享数据的内容和范围外,还需对其进行安全处理,保障数据流动过程中不被盗取、篡改,并通过保密协议明确共享方之间的职责,做到所有共享行为可追溯、可管控、可追究。

参考文献

- 1 World Health Organization. MHealth: New Horizons for Health Through Mobile Technologies [EB/OL]. [2021-09-14]. https://www.who.int/goe/publications/goe_mhealth_web.pdf.
- 2 张绍婵,冯国忠.移动医疗 APP 监管问题探究 [J].现代商贸工业,2019,40(11):90-91.

- 3 国家互联网应急中心.2019 年中国互联网络网络安全报告 [EB/OL]. [2021-09-14]. http://www.cac.gov.cn/2020-08/11/c_1598702053181221.htm.
- 4 朱光,刘虎,杜欣蒙.隐私忧虑背景下的移动医疗 APP 使用意愿研究——基于三方博弈的视角 [J].数据分析与知识发现,2019,3(5):93-106.
- 5 梁列全,余昌鸿.移动医疗 APP 的发展与应用监管研究 [J].科技和产业,2017,17(5):85-89.
- 6 孟大程,罗恩韬,王国军.移动医疗中基于机会计算的安全和隐私保护模型 [J].小型微型计算机系统,2016,37(12):2643-2648.
- 7 蝉大师.数据白皮书 [EB/OL]. [2021-09-14]. https://cds0.static.chandashi.com/Public/static/cds_data_white_paper.pdf.
- 8 陈世敏.中文可读性公式试拟 [J].新闻学研究,1971(8):181-225.
- 9 荆溪昱.中文国文教材的适读性研究:适读年级值的推估 [J].教育研究资讯,1995(5):113-127.
- 10 李萍.我国上市公司年报中“管理层讨论与分析”的可读性分析 [J].时代金融,2018(9):225-226.
- 11 秦克飞.手机 APP 隐私政策的可读性研究 [J].情报探索,2019(1):18-23.
- 12 傅永和.现代汉语常用字表的研制——附录:常用字、次常用字 [J].语文建设,1988(2):24-33.
- 13 徐雷,徐润婕.移动 APP 隐私条款可获得性及内容分析研究 [J].现代情报,2020,40(7):82-91.
- 14 国家市场监督管理总局,国家标准化管理委员会.GB/T 35723-2020,信息安全技术个人信息安全规范 [EB/OL]. [2020-04-01]. <http://www.ahstu.edu.cn/wlzx/info/1011/1478.htm>.
- 15 Robillard J M, Feng T L, Sporn A B, et al. Availability, Readability, and Content of Privacy Policies and Terms of Agreements of Mental Health Apps [J]. Internet Interventions, 2019(7):1-7.
- 16 中国互联网络信息中心.第 47 次中国互联网络发展状况统计报告 [EB/OL]. [2021-09-27]. <http://www.cnnic.net.cn/hlwfzyj/hlwxbzg/hlwtjbg/202102/P020210203334633480104.pdf>.
- 17 王蕾,汪秋伊,李星,等.网络健康信息可读性评估研究现状及展望 [J].医学信息学杂志,2020,41(12):20-25,40.
- 18 王欢,李雅琴.个人医疗数据利用中知情同意的伦理探讨 [J].中国医学伦理学,2021,34(7):830-834,843.
- 19 何占博,王颖,刘军.我国网络安全等级保护现状与 2.0 标准体系研究 [J].信息技术与网络安全,2019,38(3):9-14,19.