健康医疗可穿戴设备数据安全与隐私保护意识实证分析研究*

何晓琳 钱 庆 吴思竹 修晓蕾 崔佳伟 孙小康

(中国医学科学院/北京协和医学院医学信息研究所 北京 100020)

〔摘要〕 采用问卷调查北京协和医学院在校师生对健康医疗可穿戴设备的数据安全与隐私保护意识，从设备数据保障能力认知、数据权利主体认知、数据共享意愿认知、尊重他人隐私意识及数据保护和维权意识 5 个方面对调查结果进行分析，阐述存在的主要问题并提出应对措施。

〔关键词〕 医务工作者；健康医疗可穿戴设备；数据安全；隐私保护

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2018.06.003

Empirical Analytic Study on Data Security and Privacy Protection Awareness of Health Care Wearable Devices *HE Xiao-lin, QIAN Qing, WU Si-zhu, XIU Xiao-lei, CUI Jia-wei, SUN Xiao-kang, Institute of Medical Information, Chinese Academy of Medical Sciences/Peking Union Medical College, Beijing 100020, China*

〔**Abstract**〕 Through a questionnaire that surveys the data security and privacy protection awareness of health care wearable devices of teachers and students from Peking Union Medical College, the paper analyzes the investigation results from the five aspects of cognition of data security ability of the devices, cognition of right subject of data, cognition of willingness to share data, awareness of respecting other people's privacy and awareness of data protection and legal right maintenance, expatiates on the main existing problems and sets forward the countermeasures.

〔**Keywords**〕 Medical staffs; Health care wearable devices; Data security; Privacy protection

1 引言

近年来在全球范围内移动通信技术已与健康行业紧密结合，广阔的应用前景成为国际共识，为健康服务带来革命性的改观[1]。健康医疗可穿戴设备是健康互联中重要的网络节点，在 2015 年 3 月国务院印发的《全国医疗卫生服务体系规划纲要（2015-2020 年）》[2] 和 2015 年 9 月美国国立卫生研究院（National Institute of Health, NIH）发布的《精准医疗项目集群——建立 21 世纪医学研究基金会》白皮书[3] 中都提到要充分利用可穿戴设备推动健康医疗事业的发展，健康医疗可穿戴设备成为新型智慧医疗中的重要组成部分。

健康医疗可穿戴设备作为新型健康医疗数据载体，近几年相继被爆出数据泄露的丑闻，如 Fitbit 存在网络连接状态下易被他人获取数据以及网络地址易被识别等安全漏洞，小米、华为、Jawbone 等厂家也纷纷出现数据泄露的问题，其中有些可穿戴

〔修回日期〕 2018-01-26

〔作者简介〕 何晓琳，硕士研究生；通讯作者：钱庆，研究员。

〔基金项目〕 北京协和医学院青年基金项目（项目编号：332016119）。

设备因为侵犯个人隐私阻碍自身产品发展而被迫退出市场。除设备和网络、数据传输等技术原因，隐私保护意识和隐私尊重的伦理道德也是影响健康医疗可穿戴设备数据安全与隐私保护问题的重要因素。医学院的师生作为健康医疗可穿戴设备的使用者、研究者及采集数据的使用者之一，调查其数据安全与隐私保护意识能较好地反映普通用户对健康医疗可穿戴设备的数据安全与隐私保护意识。因此笔者就北京协和医学院开展社会调查，在对调查数据进行研究分析的基础上，总结现存问题并结合我国国情提出数据安全与隐私保护对策，为健康医疗可穿戴设备发展提供借鉴。

2 健康医疗可穿戴设备数据安全与隐私保护意识实证调查分析

2.1 对象与方法

2017 年 5－6 月，对北京协和医学院在校师生进行健康医疗可穿戴设备数据安全与隐私保护意识的问卷调查。根据调查对象职称不同，采用分层抽样的方法，共发放问卷 126 份，回收 117 份，回收率为 92.86%。其中有效问卷为 116 份，有效回收率为 92.06%。调查对象中男性共计 30 人（占 25.9%），女性 86 人（占 74.1%）；调查对象的年龄多在 20～29 岁之间，占 68.8%，30～39 岁（占 23.3%）27 人；其中硕士研究生 81 人（占 69.8%），本科 21 人（占 18.2%），博士研究生 12 人（占 10.3%）；调查对象所学专业较分散，除未填写的 12 人外，所学专业共有 18 个，其中公共卫生（占 18.1%）、情报学（占 16.4%）和社会医学与卫生事业管理（占 16.4%）的调查对象较多；除学生外，高级、中级、初级职称的调查对象分别为 12 人（10.3%）、19 人（16.4%）和 28 人（24.1%）。

2.2 调查问卷统计结果分析

2.2.1 设备数据保障能力 为了解调查对象对健康医疗可穿戴设备数据保障能力的信心，分别对健康医疗可穿戴设备连接未知网络及设备丢失后是否应该具备丢失提醒、远程清空的能力进行调查。对于将健康医疗可穿戴设备连接未知网络的问题，47.4% 的调查对象表示非常担心，因为未知网络安全很难判断，设备较易受到攻击，存在篡改设备数据或隐私泄露的风险；38.8% 的调查对象对该情况比较担心，但不知如何去避免此类情况发生；只有 13.7% 的调查对象表示不太担心或不担心，认为设备有保障数据安全的能力或抱有侥幸心理。对于设备丢失后，86.2% 的调查对象认为应具备丢失提醒、远程清空能力，以便合理保障数据安全；11.2% 的调查对象认为只要设备具备远程数据清空能力即可满足自身需求；2.6% 的调查对象表示会时刻佩戴可穿戴设备，无需具备这些能力。

2.2.2 数据权利主体（图 1） 69.0% 的调查对象认为数据应属于用户自身，远高于负责对接的医疗服务机构和国家相关政府部门等选项。此外，本研究对查看、修改健康医疗可穿戴设备采集数据的权利主体进行了调查，33.2% 的调查对象认为权利主体应为用户自身，25.3% 和 13.2% 的调查对象认为是权利主体可分别为诊疗的专科医生和负责对接的医疗服务机构管理人员，国家卫生决策者占 9.2%。由此可知，大多数调查对象认为健康医疗可穿戴设备的数据拥有者为用户自身，其享有数据查看和修改的权利，极少数调查对象认为数据的拥有者为国家相关政府部门，若国家相关政府部门想查看、修改用户的数据，应事先征得用户许可。在数据泄露责任主体的认知方面，调查对象的认知有较大差异。具体结果，见图 2。

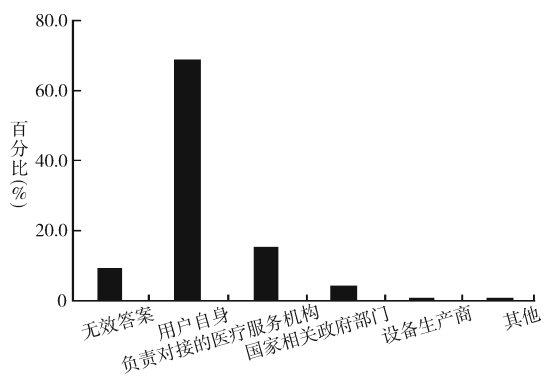

图 1 健康医疗可穿戴设备数据所有权认知情况

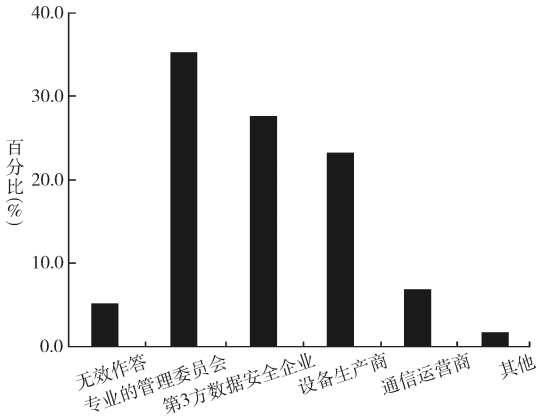

图 2 数据泄露责任主体认知情况

2.2.3 数据共享意愿 针对健康医疗可穿戴设备数据共享意愿，本研究共设置 3 道题目，分别为是否希望将采集的自身数据同步到云端、是否希望采集的自身数据实时上传，共享自身的行为数据与环境数据是否合理，调查结果，见表 1、图 3。多数调查对象比较愿意共享自身数据，认为共享个人行为数据和环境数据比较合理，但应在自身知情同意情况下或授权情况下进行数据共享。

表 1 数据共享与隐私保护选择倾向

调查对象意见内容	愿意（%）	比较愿意（%）	不太愿意（%）	不愿意（%）
是否希望将采集的自身数据同步到云端	16.4	49.1	21.6	12.9
是否希望将采集的自身数据实时上传	16.4	54.3	11.2	18.1

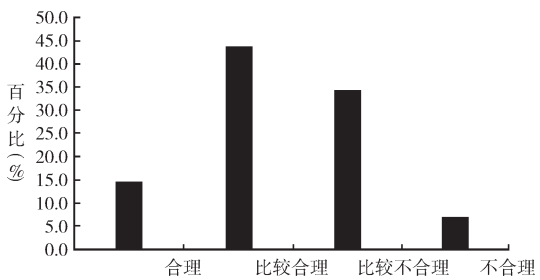

图 3 调查对象对共享行为与环境数据合理性观点

2.2.4 尊重他人隐私 为了解人们对他人隐私尊重的意识，本问卷设计如下题目：当他人在查看个人健康医疗可穿戴设备的数据时，是否会靠近；若知道健康医疗可穿戴设备会搜集周围环境的数据，是否会将设备带入公共场所。针对是否会主动靠近了解他人的健康情况，69.8% 的调查对象表示如果是家人会主动靠近，如果是同事会征得同意后再靠近；20.7% 的调查对象表示无论对方与自身是什么关系，都不会主动靠近，除非他人主动分享；8.6% 的调查对象表示可能会主动靠近，认为了解他人的健康情况并不代表会泄露他人隐私。若知道健康医疗可穿戴设备会搜集周围环境的数据，37.1% 的调查对象表示可能会将设备带入公共场所，但会提前征得周围人的同意后再使用；27.6% 的调查对象表示为保证自身健康状况的实时监测，会将设备带入公共场所使用；也有 27.6% 的调查对象表示基本不会带入，因为存在泄露隐私数据的风险；另有 6.9% 的调查对象表示不会带入公共场所使用，以避免引起不必要的恐慌。

2.2.5 数据保护和维权 对于保护和维权意识，本研究对调查对象是否遭遇过健康医疗可穿戴设备数据隐私泄露问题，在公共场合是否需要对数据进行隐匿以及在遭遇此问题后是否采取相应措施开展调查。结果显示共有 17 人遭受过隐私泄露问题，约占总调查人数的 14.7%，其中仅 9 人采取相应措施。采取的措施主要有：尽量减少不安全的网络连接、修改个人的账户密码、尽量不在公共场合展示设备和数据，无人向相关部门申诉进行维权。可以发现调查对象更倾向于从自身角度采取措施降低数据和隐私泄露的情况发生，很少采取维权措施，向相关部门申诉。在公共场合是否需要对数据进行隐匿的调查中，87.1% 的调查对象认为有必要进行部分数据隐匿，有助于减少隐私暴露的可能性；8.6% 的调查对象表现出无所谓的态度，认为个人设备在公共场所并不会引起他人的关注；3.4% 的调查对象则表示没有必要。

3 主要问题

3.1 概述

从调查问卷的分析结果中可以看出，调查对象对于健康医疗可穿戴设备数据授权、数据共享和尊重他人隐私的观点差别较大，主要存在隐私自我保护意识薄弱和未形成对他人隐私尊重观念两方面问题。

3.2 隐私数据范围模糊不清

健康医疗可穿戴设备数据内容涉及健康、临床诊疗、运动行为以及环境、社交等多维度，用户难以界定何种数据属于隐私内容范围。某些用户往往为保证个人能够得到全面的健康医疗服务而忽略隐私保密问题，这为牟取商业利益的行为提供盗取用户隐私数据的机会。

3.3 缺乏数据保密常识

用户对数据保护的知识了解很少，账户密码或解锁图案经常为方便记忆或容易操作而设置地较为简单。调查对象对健康医疗可穿戴设备连接未知网络的警觉性较低。WIFI、蓝牙、红外的网络连接和数据上传方式都是安全性极低的网络连接方式，且有研究指出可穿戴设备媒体访问控制（Media Access Control，MAC）地址基本都是固定的[4]，他人很容易与设备连接获取隐私数据。另外对于不同数据用户应该设置不同的数据权限，但用户往往因为缺乏保密意识或懒惰侥幸心理而忽略这些问题，使个人数据或隐私容易被他人破解获取。

3.4 维权意识薄弱

近些年我国公民的法律意识不断增强，但由于法律专业语言晦涩难懂，且在健康医疗服务中用户对隐私数据的保护措施与数据共享、使用条件的法律法规缺乏了解，健康医疗可穿戴设备数据属于在新型应用场景中产生，用户对健康医疗可穿戴设备数据隐私泄漏的维权意识薄弱，多采用自我救助的办法规避风险。

3.5 尊重他人隐私观念较差

使用健康医疗可穿戴设备的用户不仅缺乏隐私保护意识，也很容易忽略对他人隐私的尊重。设备在采集数据时不仅采集个人体征数据，也会采集周围环境的数据，设备带有录音和照/录像功能，那么周围人的隐私数据也将在此过程中被获取；另一方面，当数据由健康医疗可穿戴设备采集并传输到云端数据库后，数据管理公司的员工、医院的数据管理者、健康管理者很有可能出于好奇心或者利益冲动而擅自获取他人隐私数据，给用户带来隐私泄露风险。

4 应对措施

4.1 加强隐私数据保护宣传

4.1.1 概述 隐私数据保护宣传的对象不仅只针对健康医疗可穿戴设备用户，用户家属、健康医疗服务机构的医务人员以及第 3 方数据管理者对数据安全与隐私保护的知识很难保证有全面、深入的了解。加强用户及其家属、医务人员以及数据管理者的数据安全与隐私保护知识尤为必要，可通过开展隐私保护和隐私伦理尊重意识的教育培训，加强隐私数据保护宣传。

4.1.2 用户及其家属 可以制作科普视频投放于各社交网站进行分享，或通过详细的健康医疗可穿戴设备数据采集与传输政策说明书并链接至为用户提供数据安全与隐私保护服务的官方网站，同时应引导用户拿起法律的武器维护自身权益免受侵害，防止造成经济、精神损失以及人格遭到破坏。

4.1.3 医务人员及数据管理者 健康医疗服务机构的医务人员及健康医疗可穿戴设备数据管理者应通过加强法律与准则细节解读，对隐私数据泄露带来的风险与承担的法律责任予以说明。此外应增加数据使用与授权机制培训课程，定期开展相关主题讨论会，促进行业间互相交流等方式开展加强健康医疗可穿戴设备数据安全与隐私保护知识宣传。

4.2 遵循最小化共享原则

最小化原则是指受保护的敏感信息只能在一定

范围内被共享，履行工作职责和职能的安全主体在法律和相关安全策略允许的前提下，为满足工作需要仅被授予其访问信息的适当权限。在保障自身健康医疗服务可以正常开展情况下用户应遵循最小化数据共享原则，共享自身健康医疗可穿戴设备采集与反馈的数据，减少社交圈的互动数据和频率。此外用户应在采集数据前确认所采集的数据共享对象、共享数据内容等以减少不必要的数据发布。在最小化分享原则中用户可以将所采集的健康生命体征数据共享给主治医生，但应避免共享给整个医疗服务机构，可只授予其拥有保存的权利，而无权查看、获取数据；对个人行为数据应尽量只分享给能为其提供健康服务的主体和较为亲密的家人，降低分享对象数据泄露致使自身数据和隐私也遭到泄露的可能性。

4.3 注意未知环境中设备使用

健康医疗可穿戴设备现有数据格式编码复杂度较低，多使用较为简单的数据格式，如 JSON 等，将采集的数据值或图片直接进行交互传递，加密措施简单，设备使用不安全的网络连接协议，黑客容易破译，进行数据攻击、篡改。因此未知环境特别是公共场所 WIFI 未加密的情况下，用户将健康医疗可穿戴设备连入网络时数据安全遭到破坏的风险极高。所以在未知网络环境中用户应尽量减少网络连接，蓝牙在配对结束后立刻调回不被其他设备扫描到的状态，减少设备被攻击的可能性。此外在公共场合中使用设备时应尽量遮挡设备屏幕或使用第 2 屏幕等视觉阻塞方式减少数据与隐私泄露风险。

5 结语

在健康医疗可穿戴设备数据安全与隐私保护中，单纯依靠任何一方力量或某一方面的突破都很难取得有效成果，需要健康医疗服务机构、政府相关部门以及健康医疗可穿戴设备生产商和第 3 方数据管理方彼此合作、达成一致，从多个层面实施数据及隐私保护，用户也需要主动提高隐私保护意识，共同保障健康医疗可穿戴设备数据和隐私安全。

参考文献

1 于广军，杨佳泓. 医疗大数据［M］. 上海：上海科学技术出版社，2015，1：181.

2 国务院办公厅关于印发全国医疗卫生服务体系规划纲要（2015—2020 年）的通知［EB/OL］.［2017－03－02］. http：//www. gov. cn/zhengce/content/2015 － 03/30/content_ 9560. htm.

3 NIH 发布“精准医疗”白皮书，呼吁所有人共享基因数据［EB/OL］.［2017－03－03］. http：//www. biodiscover. com/news/politics/122097. html.

4 Security Analysis of Wearable Fitness Devices（Fitbit）［EB/OL］.［2017 － 11 － 10］. https：//courses. csail. mit. edu/6. 857/2014/files/17 － cyrbritt － webbhorn － specter － dmiao － hacking － fitbit. pdf.