健康信息化背景下医护人员医疗信息安全风险识别与应对策略

徐王权,姚乐融,李 锐,柴 静
(安徽医科大学卫生管理学院,安徽 合肥 230032)

摘要:医疗信息安全是我国医药卫生信息化的前提与保障,医护人员在医疗信息安全中扮演着极为重要的角色,其对医院的正常运转和社会形象具有重要影响。本文主要阐述了健康信息化背景下医护人员职业场景、职业角色、使用工具及职业环境,分析了医护人员在不同的职业场景中面临的医疗信息安全风险,并针对性的提出了应对策略,旨在为我国医药卫生信息化提供安全保障。

关键词:医护人员;信息安全风险;应对策略
中图分类号:R197 **文献标识码**:B DOI:10.3969/j.issn.1006-1959.2021.06.007
文章编号:1006-1959(2021)06-0025-04

Risk Identification and Coping Strategies of Medical Information Security for Medical Staff Under the Background of Health Informatization

XU Wang-quan,YAO Le-rong,LI Rui,CHAI Jing
(School of Health Management,Anhui Medical University,Hefei 230032,Anhui,China)

Abstract:Medical information security is the prerequisite and guarantee of China's medical and health informatization. Medical staff play an extremely important role in medical information security, which has an important impact on the normal operation of hospitals and social image.This article mainly elaborates the occupational scenes, occupational roles, tools and occupational environment of medical staff under the background of health informatization, analyzes the medical information security risks faced by medical personnel in different occupational scenes, and proposes targeted countermeasures.It aims to provide safety guarantee for China's medical and health information.

Key words:Medical staff;Information security risk;Coping strategies

信息化是我国卫生事业发展的重要内容,也是发展的工具之一[1]。“十三五”时期,医疗卫生行业将是国家信息化发展的重点,已纳入国家网络安全和信息化建设重点规划[2]。《健康中国 2030 规划纲要》《国务院促进大数据发展行动纲要》《国家信息化发展纲要》等系列文件将全民健康信息化建设提升到国家高度[3]。医药卫生领域的信息化迎来了前所未有的发展机遇,并进入高速发展期。与此同时,医疗信息安全越来越成为政府和卫生行政部门关注的焦点。本文主要阐述医护人员在不同的职业场景中面临的医疗信息安全风险,并针对性的提出了应对策略,旨在为我国医药卫生信息化提供安全保障。

1 医疗信息安全是卫生信息化的前提和保障

1.1 信息安全已经上升到国家层面 2014 年美国斯诺登事件以后,信息安全受到世界各国的高度重视,已经上升到了国家安全的高度。同年,我国成立了以国家主席为组长的中央网络安全与信息化领导小组,全面负责国家信息安全工作。2015 年国家主席习近平在互联网大会上指出,没有网络空间的安全,就没有国家的安全。信息安全是信息化社会重要的保障,没有信息安全,就无法真正实现信息化。至此,信息安全和网络空间安全已经上升到国家层面。

1.2 医药卫生领域信息安全形势严峻 在医药卫生领域,医疗信息事关患者的生命健康、个人隐私及伦理道德,直接影响医院的正常运转和社会形象,因而其安全性极为重要。根据美国电信 Verizon 的数据泄露调查报告显示,全球医疗卫生行业的数据泄露威胁从 2014 年开始逐渐呈现飞速上升的趋势:2014 年行业排名第 6,到 2016 年已仅次于金融行业排名第 2,2017 年排名第 1。2019 年占比为 15%,远超金融行业 10%[4]。国内医疗安全事件层出不穷,2014 年某妇幼保健院医生贩卖产妇信息,造成了极其恶劣的社会影响,2018 年全国有 247 家三甲医院检测出勒索病毒。为此,国家卫健委出台了医疗机构信息安全等级保护条例,要求医疗机构于 2015 年 12 月完成医疗机构等级保护测评工作。2018 年出台了《国家健康医疗大数据标准、安全和服务管理办法》,其中第十七条规定:责任单位应当建立健全相关安全管理制度、操作规程和技术规范,落实“一把手”责任制,加强安全保障体系建设,强化统筹管理和协调监督,保障健康医疗大数据安全[5]。2019 年《中华人民共和国基本医疗卫生与健康促进法》第九十二条规定:国家保护公民个人健康信息,确保公民个人健康信息安全。推进医疗卫

基金项目:1.安徽省教育厅高等院校质量工程教学研究项目(编号:2018jyxm0164);2. 安徽省教育厅人文社科重点项目(编号:SK2018A0168);3. 安徽医科大学博士科研资助基金项目(编号:XJ201638)
作者简介:徐王权(1979.7-),男,安徽芜湖人,博士,副教授,主要从事卫生信息管理研究

生机构建立健全医疗卫生信息交流和信息安全制度。这些条列和法规对医疗机构的医疗信息安全都提出了明确的目标和要求。

1.3 医护人员在医疗信息安全管理中扮演着重要角色 在信息安全管理过程中，人是其中最为活跃的因素，也是绝大部分(80%左右)信息安全事件的源头[6]。作为医疗信息的生产者和使用者，一线医护人员在医疗信息安全工作中扮演着极为重要的角色，他们的行为将直接影响医疗信息的安全程度。因此，减少医护人员面临的信息安全风险，规范其日常操作行为，是医疗信息安全管理的重要举措之一。

2 健康信息化背景下医护人员执业场景变化

2.1 传统环境下医护人员的行为场景 传统环境下，医护人员的职责是在执业医院进行日常诊疗活动，主要工作场所包括门诊部诊室、住院部医生办公室及手术室。与信息有关的主要工作内容包括：病历撰写(大病历、病程记录等)、医嘱开设(检查、检验及用药医嘱等)、查阅检查及化验报告等。所采用的工具为医护工作站信息系统或者手工纸质病历材料。工作场所稳定，角色相对单一，因而面临的医疗信息安全风险较少。

2.2 健康信息化背景下医护人员的行为场景 2013年11月20日，《关于加快推进人口健康信息化建设的指导意见》中明确了健康信息化的总体目标是：以业务和管理需求为导向，全面建成实用、共享、安全的人口健康信息网络体系。在此背景下，催生出了基于互联网+医药卫生的多种新模式、新业态和新技术，如区域卫生信息平台、移动医疗、互联网医院、医疗网站、远程医疗、医联体和医共体及专科联盟等[7]，大大提升了医疗机构的工作效率，也极大的方便了患者。在此过程中，医护人员将面临更多、更复杂的工作场景，承担的角色也呈现多元化的特征，见图1。医护人员在不同的场所扮演的角色和使用的工具均不相同，工具本身有纸质和信息系统之分，信息系统也有是否联网及登入方式的区别，医护人员在这些场景中行为方式也不尽相同。因此，其面临的信息安全风险种类和性质也存在较大差异。

3 健康信息化背景下医护人员信息安全风险识别

医护人员面临的医疗信息安全风险主要受三个因素的影响：工作环境、职业角色及使用工具。工作环境主要是指公共网络或是局域网络或是单机系统；职业角色主要指对医疗信息的访问权限；使用工具是指信息化工具或手工纸质工具。依据上述三个因素及具体的内容，本文对医护人员可能面对的风险进行了研判，见表1。

4 信息安全风险应对策略

4.1 规范账户信息管理，提升医护人员口令的安全级别

4.1.1 妥善维护个人口令 医护人员的工作环境偏向于公共场合，或多或少都有旁观者存在，个人账号泄露的可能性较大。另外，部分医护人员存在将账号和密码写在纸条及记录本上的习惯，也容易导致口令泄露，且长时间使用同一口令泄露的可能性将成倍增加[8]。因此，为保障口令不被“有心人”窃取和利用，医护人员应定期更新口令，尽可能的减小因口令泄露带来的风险。

4.1.2 部署弱口令检测系统 口令失窃另一个重要的原因是口令设置过于简单，即弱口令，如采用生日、姓名的拼音、电话号码、简单数字组合、键盘特定形状字母或数字组合等作为口令，很容易通过猜测或者简单的密码破解软件等识破。因此，有条件的医院可以通过部署弱口令检测系统来解决这一问题，通过扫描系统中账号的口令，识别出弱口令，并提醒医护人员进行修改。

4.2 严格医护人员系统权限分配，降低由于账户泄露造成的危害程度 针对医护人员的角色和级别，严

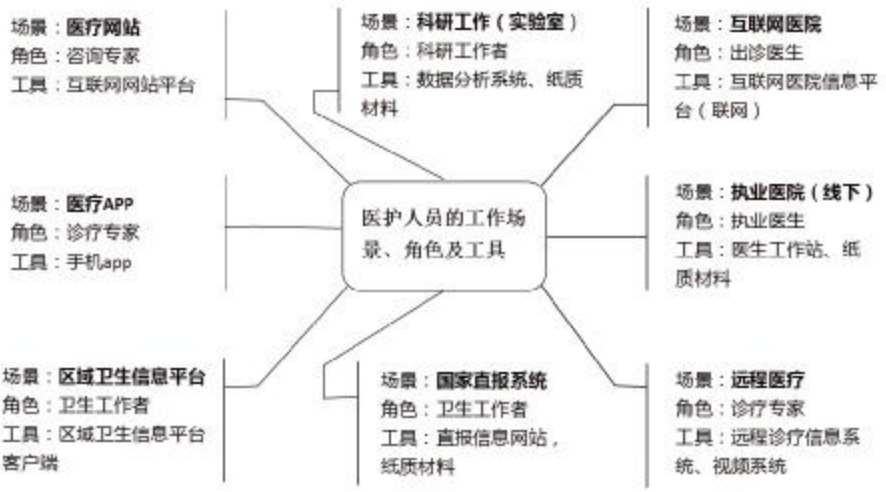

图1 健康信息化背景下医护人员工作场所、角色及工具

表 1 健康信息化背景下医护人员执业场景及可能面临的医疗信息安全风险

序号	职业场景	职业角色	使用工具	工作环境	面临的信息安全风险
1	执业医院（实体医院）	执业医生	信息系统及纸质材料	院内诊室，院内局域网络，有限性与互联网连接或 VPN	用户口令失窃 纸质材料遗失 作废病历纸张未正确销毁
2	互联网医院	出诊医生	互联网医院平台	互联网环境	账号口令失窃 网络黑客入侵致数据被盗 电脑植入木马病毒致数据泄露
3	远程医疗	会诊专家	远程诊疗平台	VPN 或互联网	远程诊疗平台支撑等无关人员泄露 账户口令失窃 遭遇钓鱼网站
4	医疗网站	咨询专家	网站平台	互联网开放环境	网络黑客入侵致数据被盗 电脑植入木马病毒致数据泄露 账号密码失窃
5	手机医疗 APP	诊疗专家	手机	互联网开放环境	面临的信息安全风险 Wifi 入侵 手机病毒
6	科研工作	科研工作者	数据分析工具、纸质材料（如调查表）	单机系统或联网电脑	手机失窃或淘汰手机未能正确处理数据未脱敏 调查数据使用后未及时销毁
7	卫生信息直报	卫生工作者	直报平台	互联网开放环境	口令失窃 上报原始资料泄露
8	医联体	卫生工作者	医疗体信息平台	卫生专线、VPN 或互联网	电脑植入木马病毒 口令失窃 发布未经许可的文件

格确定其系统访问权限及可访问的内容。同时，在医护人员角色和级别变动的情况下，动态更新其访问权限和访问内容，在满足其日常工作的前提下，尽量赋予其最小访问权限和有限访问内容。此举的目的是一旦医护人员账号泄露，可将其对系统造成的影响限定在可控范围之内。另外，对于已经离职的医护人员，应及时注销其各系统的账户信息，消除医疗信息泄露的隐患。

4.3 加强医护人员的信息安全培训，提高医护人员的信息安全素养 医护人员的信息安全培训可以依据信息安全素养的理念[9]，从信息安全意识、知识、能力及执行和维持等五个方面进行系统性培训，见图 2。信息安全意识：主要是建立信息化工作必须安全的观念，保持对信息安全风险的一种戒备和警觉的心理状态；信息安全知识：主要是对信息安全基本知识的了解，如病毒、密码、防火墙、钓鱼网站等；信息安全能力：主要是基本的处理信息安全事件的方法或者预防信息安全风险的措施等，如安装杀毒软件的方法、杀毒、对特定文件设置密码等；信息安全执行：主要涉及是否落实了信息安全的规章制度，将信息安全工作落实到日常工作中等；信息安全维持：主要将信息安全措施作为常态化的工作，持续保持。

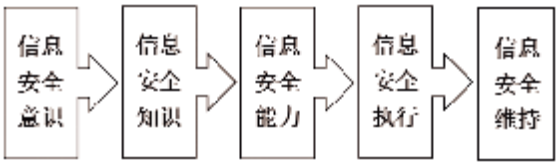

图 2 医护人员信息安全培训内容及递进关系图

医护人员的信息安全培训还可根据不同的场景设立培训主题，如诊室医生工作站、互联网平台、手机 APP 及科研平台等，针对不同场景中存在的风险，有针对的进行培训。需要说明的是，医护人员的信息安全培训不是一蹴而就，需要定期或者不定期持续进行，不断强化其信息安全意识，提升安全防护能力。另外还需做好日常的宣传工作，使医护人员时刻保持警惕。

4.4 完善工作场所规章制度，规范医护人员的医疗信息安全行为 针对不同工作场景可能面临的信息安全风险，制定针对型的日常行为制度，如作废的病历用纸应及时粉碎销毁、不得将病历资料拍照留存上网（发朋友圈等）、不得擅自将工作资料内容拷贝及拍照私自留存、不得使用未脱敏的医疗信息进行科学研究等。将相关的制度和要求印成医护人员工作

手册，便于医护人员日常查阅及落实。同时，医院还需建立相应的惩罚措施，对违规行为进行处罚，确保信息安全规章制度落到实处。

5 总结

在全民健康信息化的背景下，医护人员将进入更多的职业场景，面临的医疗信息安全风险也在不断变化，这一现象应该引起医院和卫生主管部门的高度重视。及时准确识别医护人员面临的医疗信息安全风险源，有针对性的进行规避与提前应对，尽可能将风险消除在萌芽状态，使医护人员的职业场景更加规范与安全，以为医疗行业的信息安全管理工作奠定基础。

参考文献：

[1] 中共中央国务院关于深化医药卫生体制改革的意见[EB/OL]. [2020-10-13].http://www.gov.cn/gongbao/content/2009/content_1284372.htm.2009-3-17/2020-9-7.

[2] 国务院关于印发“十三五”国家信息化规划的通知[EB/OL]. [2020-10-13].http://www.gov.cn/zhengce/content/2017-01/10/content_5158488.htm.2016-12-27/2020-9-7.

[3]孟群.互联互通促进人口健康信息化建设科学发展[J].中国卫生信息管理杂志,2016(4):323-323.

[4] Data Breach investigations Record [EB/OL].[2020-10-13]. https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf.

[5]关于印发国家健康医疗大数据标准、安全和服务管理办法(试行)的通知[EB/OL].[2020-10-13].http://www.cac.gov.cn/2018-09/15/c_1123432498.htm?from=timeline.2018-9-15/2020-9-7.

[6]马勇,张晓林,胡金伟,等.“互联网+医疗健康”中的个人信息保护问题探讨[J].中华医院管理杂志,2019,35(1):19-24.

[7]宋杰,孙国强,马琏,等.医院移动医疗安全挑战及思路探索[J].中国数字医学,2019,14(1):94-96.

[8]陈文亮,庄绍燕,杨保卫.基于我院HIS的统一用户管理的设计与实现[J].中国医疗设备,2016(8):89-90.

[9]罗力.上海市民个人信息安全素养评价研究[J].重庆大学学报,2013,19(3):95-99.

收稿日期：2020-10-13；修回日期：2020-10-23
编辑/成森