# “互联网 +”背景下医院信息系统风险管理研究

谭太昌 王甲甲 王加强 舒 朗 袁 红

（四川省医学科学院/四川省人民医院 成都 610072）

〔摘要〕 从人员不安全行为、设备及软件不安全状态、环境不确定因素和管理缺陷 4 方面分析医院信息系统风险来源，提出应对策略，包括重视教育培训、加大技术投入、加强日常维护、完善管理制度等。

〔关键词〕 “互联网 +”；信息系统；信息安全；风险管理

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2018. 11. 008

**Study on the Risk Management of Hospital Information System against the Background of "Internet +"** *TAN Taichang, WANG Jiajia, WANG Jiaqiang, SHU Lang, YUAN Hong, Sichuan Academy of Medical Sciences & Sichuan Provincial People's Hospital, Chengdu 610072, China*

〔**Abstract**〕 The paper analyzes the sources of information system risk in the hospital from four aspects such as unsafe behavior of personnel, unsafe condition of equipment and software, uncertain factors in environment and defect in management, and comes up with coping strategies including attaching importance on education and training, increasing technological investment, strengthening daily maintenance and improving management system, etc.

〔**Keywords**〕 "Internet +"; information system; information security; risk management

## 1 引言

“互联网 +”利用互联网平台为传统行业提供便捷高效的思路与解决方案。随着互联网技术的迭代发展，“互联网 +”技术无疑提升了医院的核心竞争力，使医患双方在诊疗过程中都得到极大便利的同时也给医院带来信息安全隐患。由于医院信息系统中储存着大量重要信息，这些信息关乎医院的运营发展、规划布局等，丢失或者损坏会造成难以挽回的损失，医院信息系统风险管理尤为重要。

## 2 “互联网 +”背景下医院信息系统风险管理重要意义

不同于纸质档案时代，随着信息技术的不断迭代发展，信息系统已是现代医院进行信息管理不可替代的工具，显著提升医院各方面的管理效率。医

〔收稿日期〕 2018 - 09 - 24

〔作者简介〕 谭太昌，副主任技师，发表论文 16 篇；通讯作者：袁红，教授，主任技师。

〔基金项目〕 四川省科技厅资助项目“医学实验室质量和能力认可体系管理系统地建立暨推动四川省医学实验室质量和能力认可工作”（项目编号：2016Z R0080）；四川省卫生和计划生育委员会科研课题“转基因 foxp3 在肝癌增殖、转移及化疗药物敏感性的作用机制”（项目编号：18PJ120）。

院信息系统中存放的病患和健康管理资料以及医疗业务数据对于医疗服务、临床教学、运营规划、医学研究极具价值[1]。医院信息系统中的资料除与医院运作与管理息息相关外也会影响患者的医疗安全。从安全性考虑，最佳方法是将医院核心业务系统与互联网在物理上相互隔离，但“互联网 +”要求将互联网平台与医院核心业务进行高效互联，如预约挂号、自助缴费、打印检查报告等都要求医院的核心系统与互联网实时链接，由此必然加剧医院信息系统的安全风险。所以医院在利用“互联网 +”技术带来便利的同时还要注重信息风险防范。

## 3 医院信息系统风险来源分析

### 3.1 概述

医院信息系统主要包括两大类，一是临床应用类系统，如医生工作站、检验信息系统（Laboratory Information System，LIS）、药物系统、医学影像系统等；二是医疗管理类信息，如门诊挂号、病案管理、出入院管理、结算财务系统等。“互联网 +”背景下大量信息可能被获取、加工、传输、储存。有的信息如医生门诊出诊安排等必须及时公开，而有的信息如患者病案等必须对非授权人员保密。广义地讲信息获取失误、加工错误、传输出错（包括非法获取）、储存错误等都是医院信息风险，由于信息获取和加工主要涉及医疗技术，而信息传输、储存与信息系统安全密切相关，故本文只讨论后两种医院信息系统风险。

### 3.2 人员

管理学认为人是最大的风险来源，也是可变性最大的风险因素。有统计资料表明人为因素导致的事故数量占总事故数量的 70% 以上。接触医院信息系统的人员有医院相关与无关人员之分，无关人员只能浏览公开信息，而相关人员可以根据其岗位获得接触信息的不同授权，而超出其授权范围或者无关人员接触到非公开信息就是风险。相关人员的业务能力不强、防范意识不够以及无关人员的恶意攻击，如黑客可以利用非法技术手段对医院信息系统进行攻击，都会对医院信息系统造成严重损害，可能会使机密和非公开信息被窃取，造成医院严重损失。

### 3.3 设备及软件

信息设备及软件是“互联网 +”时代医院实现信息化的重要保障，需要考虑以下要点：一是设备设计问题。设备技术可靠性、性能等与信息安全密切相关。医院有时从效益和节省成本的角度出发可能有意减缓信息设备的更新。此外由于客观技术条件的限制，目前大多数计算机使用都是微软公司 WINDOWS 操作系统，如果其存在的漏洞不及时修补极易受到攻击。另外有些医院计算机中使用的盗版软件也易遭受攻击，进而影响医院信息系统的安全运行。二是设备的安全防护问题。由于医院信息系统需要与省市医保、新农合、区域卫生健康信息平台等建立网络连接，使其不能完全与外部网络隔离，易受到计算机病毒和网络黑客的入侵。近年来黑客的网络攻击技术手段不断翻新，新病毒、木马程序不断涌现。如勒索病毒事件，黑客就是利用计算机系统漏洞进行病毒攻击并勒索钱财，国外多家医院成为病毒感染重灾区[2]，造成巨大损失。

### 3.4 环境

各种环境因素包括天气、地理条件等都可能影响医院信息系统安全。如夏季暴雨雷击、超高温、意外断电等都会导致设备故障；网络线路的断裂造成信号丢失。网络设备故障对计算机网络的破坏具有隐蔽性和突然性，还会造成故障排查困难。

### 3.5 管理

管理是将人员、设备和环境有效地结合起来的手段和过程，通过规定标准、模式实施控制、指导整个医院运作活动。常见的管理缺陷包括以下内容。一是标准是否适用。医院现有的信息系统各种规章制度是否与新环境相适应是需要考虑的首要问题。如针对新型蠕虫、木马等病毒泛滥的情况，各级医院制订严格的内外网物理隔离制度，但往往执行不到位。如果系统管理人员安全意识薄弱或责任

心不强，导致系统管理账号、密码泄露或被破解，会给医院网络信息系统造成重大破坏和损失。二是控制是否适度。医院信息系统的目标是为医患双方带来便利，从而改善患者的就医体验，同时提升医院的核心竞争力和经济社会效益，这就要求医院信息系统与客户之间有极好的交互性和适当的开放性。医院信息系统的开放也给系统自身带来安全问题，可以设计信息系统分级访问机制，在安全性和便利性之间取得平衡。

## 4 医院信息系统风险应对策略（图 1）

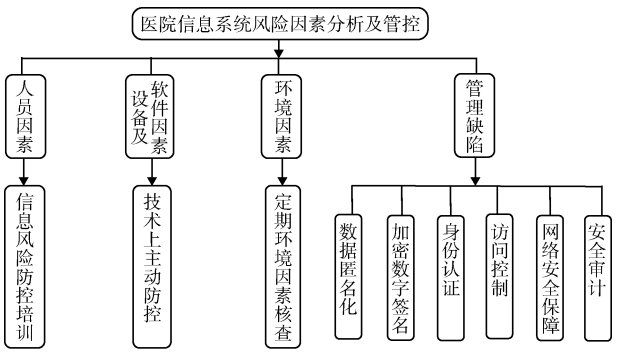


图 1 医院信息系统风险因素分析及管控

### 4.1 重视教育培训，提升人员信息风险防控意识

提升信息风险防控意识的有效途径是对医院各级人员开展有针对性的教育培训[3-4]，包括基本的信息安全知识培训和信息安全法制教育，特别是 2017 年 6 月开始执行的《中华人民共和国网络安全法》，对风险防控规定进行宣传，应用制度措施明确医院每个部门、各级岗位人员在信息系统风险管控中应尽的权利和义务，在思想和行动上统一全院的信息风险防控意识。

### 4.2 加大技术投入，做好主动防控

根据风险防控需求，做好每年医院信息化建设预算，不仅要包含采购硬件设备和网络改造的资金，还应包括购买防病毒软件和加密技术等软件、技术的资金。有计划地淘汰老旧计算机，及时更新补丁、修复操作系统漏洞。医院信息系统建立在计算机网络基础之上，而计算机网络容易受到病毒的攻击，安装防病毒软件是避免病毒侵袭的有效手段。计算机网络入侵检测系统可作为防火墙的合理补充，通过数据审计和行为分析等手段及时预警网络或系统受到攻击的可能性。

### 4.3 加强日常维护

优化设计医院网络结构主动改造旧网络，主要设备和链路采用冗余设计，留有技术余量。做好线路防护，重要节点服务器最好设置在专用机房内，专用不间断电源线路供电。

### 4.4 数据匿名化[5-6]

为切实保护患者的隐私和安全，确保在医疗信息系统中以及提供正常医疗服务以外的（如医疗保险、医疗机构的某种研究）传递中使用的患者资料不向非授权用户透漏。对数据进行分级管理，防止人为从后台查询患者敏感数据；对身份证信息等设置数据加密；对特殊患者的特殊信息（如基因信息）进行替换，如姓名用特殊字母替换等（去标识化）。

### 4.5 加密和数字签名

创建和管理数据存储的加密密钥、数据库加密，加密数据库表中的数据字段以保护患者档案和医疗信息系统处于使用状态。由医疗信息系统的用户创建数字签名，确保临床数据的不可否认性，如诊疗记录、报告等。采用 CA 电子签名系统进行身份鉴别以及对关键数据的一致性签名。

### 4.6 身份认证

根据角色级别、用户类型及其对医疗信息系统的重要性来选择是否进行身份认证，对不同用户选择恰当的身份认证手段。用户登录时进行双因素身份鉴别（USBKey + 密码）；提供用户身份唯一标识和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户，身份鉴别信息不易被冒用；提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施设置口令制度并定期强制更换。一般 8 位以上，包括数字、字符、大小写字母组合。

### 4.7 访问控制

应有具体的时间和空间条件限制，保证具有访问权限的用户只有在指定时间、空间才能访问医疗信息系统。提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；访问控制覆盖范围应包括与资源访问相关的主体、客体及其之间的操作；由授权主体配置访问控制策略并严格限制默认帐户的访问权限；授予不同帐户为完成各自承担任务所需的最小权限并在其之间形成相互制约的关系。从交换机对医院各个区域进行 IP 号段分配，防止非法随意配置 IP 来登录系统，同时各终端设备接入网络时进行网段划分，重要数据的查阅进行 IP 网段及区域的可靠隔离，防止其他区域非法登录查阅。

### 4.8 网络通信安全保障

用网络日志来记录、登录用户 IP 地址、媒体访问控制（Media Access Control，MAC）物理地址；利用虚拟专用网（Virtual Private Network，VPN）实现数据传输保密。六是安全审计。提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；保证无法删除、修改或覆盖审计记录；审计记录内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等，对日志进行统一的审计分析同时无法对日志文件进行修改。

## 5 结语

国内专家已开展一些针对医院信息安全管理方面的研究，同时可以借鉴其他行业专家的成果指导相关研究[7-8]。随着临床医学步入精准医学时代以及基因测序技术的飞速发展，测序价格的降低，人们获取个人基因组数据相对越来越便利，医疗机构除传统的医学数据外还将产生海量的基因数据，此外数据存储网络化，伦理、隐私和基因数据提供者的信息安全面临更复杂的挑战[9-12]。医院信息系统风险管理的根本目的是保障信息系统安全，从而提升医院的社会和经济效益，以便更好地服务社会。这需要从整体思维出发，从组织架构、风控意识、技术队伍、制度措施方面全方位入手，构建多重防护体系，确保医学信息和数据安全。

## 参考文献


1 华永良. 医院信息安全体系架构［J］. 中国数字医学，2016，11（6）：89－91.

2 赖勇平. 医院信息化建设中计算机网络安全管理与维护［J］. 电子技术与软件工程，2017，5（16）：214－215.

3 Park E H，Kim J，Park Y S. The Role of Information Security Learning and Individual Factors in Disclosing Patients´ Health Information［J］. Computers & Security，2017，65（3）：64－76.

4 Ki－Aries D，Faily S. Persona－centred Information Security Awareness［J］. Computers & Security，2017，70（9）：663－674.

5 陈大超. 医院计算机网络信息安全管理维护工作策略［J］. 电子技术与软件工程，2017，5（8）：225.

6 蔡雨蒙，朱一新，刘云，等. 医疗卫生行业信息安全等级保护探讨［J］. 医学信息学杂志，2014，35（9）：12－15.

7 Kiran K V D，Reddy L S S，Kumar V P，et al. Information Security Risk Management in Critical Informative Systems［C］. India：IT in Business，Industry and Government. IEEE，2015：1－5.

8 Semin V G，Shmakova E G，Los A B. A Statistical Approach to the Assessment of Security Threats Information System［C］. Russia：International Conference of Quality Management，Transport and Information Security，Information Technologies. IEEE，2017：100－105.

9 吕耀怀，曹志. 大数据时代的基因信息隐私问题及其伦理方面［J］. 伦理学研究，2018，17（2）：86－91.

10 刘辉，丛亚丽. 临床医学大数据的伦理问题初探［J］. 医学与哲学（A），2016，37（10）：32－36.

11 雷小三. 基因组数据的隐私保护技术研究［D］. 西安：西安电子科技大学，2014.

12 白晋伟，沈百荣. 健康管理与深度测序数据解析的挑战［J］. 医学信息学杂志，2018，39（1）：8－11，32.