# “互联网 + 医疗”信息安全问题及对策分析

王 洁

（北海市第二人民医院 北海 536000）

〔摘要〕 针对“互联网 + 医疗”的应用现状，分析其可能存在的信息安全问题，提出防范对策，包括增强医院信息系统安全性、建立相应管理制度、制定相关法律法规、加大监管力度以及提高自我保护意识。

〔关键词〕 “互联网 +”；医疗信息安全；信息系统安全

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2018. 03. 010

**Analysis of "Internet + Medical" Information Security Problems and Countermeasures** *WANG Jie, The Second People's Hospital of Beihai City, Beihai 536000, China*

〔**Abstract**〕 Based on the application status of "Internet + Medical", the paper analyzes the possible information security problems in it and raises countermeasures including stepping up security of hospital information system, building corresponding management system, laying down relevant laws and regulations, strengthening supervision and enhancing self - protection awareness.

〔**Keywords**〕 “Internet +”; Medical information security; Information system security

## 1 引言

“互联网 + 医疗”是以互联网为载体、以信息技术为手段，（包括移动通讯技术、云计算、物联网、大数据等）与传统医疗健康服务深度融合而形成的一种新型医疗健康服务业态的总称[1]。“互联网 + 医疗”在互联网创新技术推动下，开展健康教育、医疗信息查询、疾病在线咨询、预约诊疗、电子处方、远程医疗、移动医疗等多种形式的健康医疗服务[2]。随着网络信息技术的发展，“互联网 + 医疗”模式必将给传统医疗行业带来巨大变革，而“互联网 + 医疗”服务平台集中患者个人医疗信息、网络帐户信息等多种敏感数据信息，保护患者个人信息是“互联网 + 医疗”亟待解决的问题。因此对互联网医疗的信息安全问题必须加以重视。

## 2 “互联网 + 医疗”应用

“互联网 + 医疗”模式改变传统的就医模式，让寻医问药变得方便快捷，服务平台整合医疗资源，实时通讯、互通互联、资源共享，能实现传统医疗不能完成的服务。近年来我国各地“互联网 + 医疗”主要应用于以下几个方面：一是改善患者就医体验，实现网上预约挂号、缴费、查看检验检查报告等功能，减少患者非诊疗的就诊时间，随时随地掌握就诊信息，提高患者就医便利程度。二是推进分级诊疗，患者首先在网上问诊，确定是否需要到大医院就诊，以及就诊医疗机构级别，从而缓解大医院门诊压力，也避免患者无序就医[3]。而远程医疗是推进分级诊疗的良好举措，使患者在基层医

〔修回日期〕 2018 - 01 - 02

〔作者简介〕 王洁，工程师，发表论文 3 篇。

疗机构接受到高级别医疗机构的专家诊疗，提升基层医疗机构的诊疗能力。三是建立区域卫生信息平台，建立患者电子健康档案，实现区域内医疗机构信息互联互通，实现患者门诊处方、住院医嘱、检查报告、病历等健康信息的集中存放和共享。四是智能穿戴设备带来的健康管理。智能腰带、腕带、臂环、头盔等可穿戴医疗设备用于对个人运动和生活进行跟踪，个人健康信息都可连入互联网，随时随地采集健康数据，共享数据，为医疗大数据的应用分析提供重要支撑。

## 3 安全问题

### 3.1 医疗卫生信息

在“互联网 +”浪潮的不断推进下，各种业务和服务已信息化、移动化、网络化，而互联网的信息安全问题使人们时刻保持警惕。黑客入侵、木马病毒、手机信息意外泄露等事件频频发生，让网络信息安全问题再成焦点。在互联网医疗中，患者在网上预约挂号或填写个人信息注册网站进行医疗健康咨询、分享就诊经验时，无意中泄露了某些碎片信息，虽然看似毫无价值，但是将其与患者提供的其他信息关联后却有可能识别患者身份[4-5]。医疗机构数据库中也储存着患者个人信息，包括基本信息、病历、病史、治疗记录、检查报告等数据信息。孕产妇信息泄露最为常见，详细到孕产妇的姓名、年龄、电话、预产期、分娩时间、地点等，甚至连婴儿信息都十分清楚。造成孕产妇信息泄露有两种可能：一是内部人员倒卖信息；二是黑客入侵医疗机构网络。不管什么原因，这些隐私数据一旦泄露，可能会被不法分子用于诈骗、推销或冒用数据制造虚假身份，损害患者利益。

### 3.2 医院信息系统

传统的医院信息系统是医院内部网络，是封闭、隔离的网络系统，相对安全，但随着“互联网 +”在医疗领域的应用，医院信息系统不可避免接入互联网[6]。接入互联网后医院信息系统可能会遭遇网络攻击或入侵，而传统的医院信息系统基本没有应对策略，网络安全防护疏漏，网络内部未做安全区域划分，边界安全防护不严密，存在安全隐患，且核心数据传输缺乏均衡机制，难以应对高峰需求。医院信息系统一旦被入侵，大量的医疗数据可能会遭到窃取和篡改，给医院和患者带来巨大的安全风险。如何应对医院信息系统被入侵和窃取数据是“互联网 + 医疗”要解决的关键问题。

## 4 防范对策

### 4.1 增强医院信息系统安全性

4.1.1 概述 医院的网络分为内网和外网，外网与 Internet 直连，内网部署医院信息系统（Hospital Information System，HIS），检验信息系统（Laboratory Information System，LIS），医学影像存储与传输系统（Pictures Archiving and Communication System，PACS）等。接入互联网后，为保证医疗信息安全，医院内外网之间采用防火墙、网闸等安全措施隔离，医院网络还需具备入侵防御、互联网控制审计等功能，具体网络拓扑结构，见图 1。

4.1.2 外联区 外网为外联区，接入 Internet、专网专线，利用虚拟专用网络（Virtual Private Network，VPN）网关、Web 防火墙、互联网控制审计系统、入侵防御系统等做好安全防护。内网划分了不同安全区域：数据接入区、核心数据区、DMZ 区、安全管理区。各区域之间使用防火墙控制访问，且防火墙和核心交换机、汇聚交换机等关键设备采用双机热备，避免单点故障。

4.1.3 网闸 医院外网和内网之间使用双向网闸，隔断利用各类通用协议的攻击和入侵威胁，实现两个隔离的网络之间的数据交换。网闸是由外部主机、内部主机和专用隔离开关系统组成。外部主机连接外网，内部主机连接内网，专用隔离开关系统在任一时刻仅连接外部主机或内部主机，与两者间的连接受硬件电路的控制高速切换，保证在任一时刻仅连通外网或内网，实现对网络安全防护[7]。

4.1.4 DMZ 区（隔离区、非军事化区） 为解决外部网络不能访问内部网络服务器的问题而设立的一个非安全系统与安全系统之间的缓冲区，外网用户只能访问 DMZ 中的服务，不能接触存放在内网中的数据信息[8]。需要与互联网通信的代理缓存和 Web 服务器单独放在 DMZ 区，其他数据存放在网闸后，以保证内网数据安全。

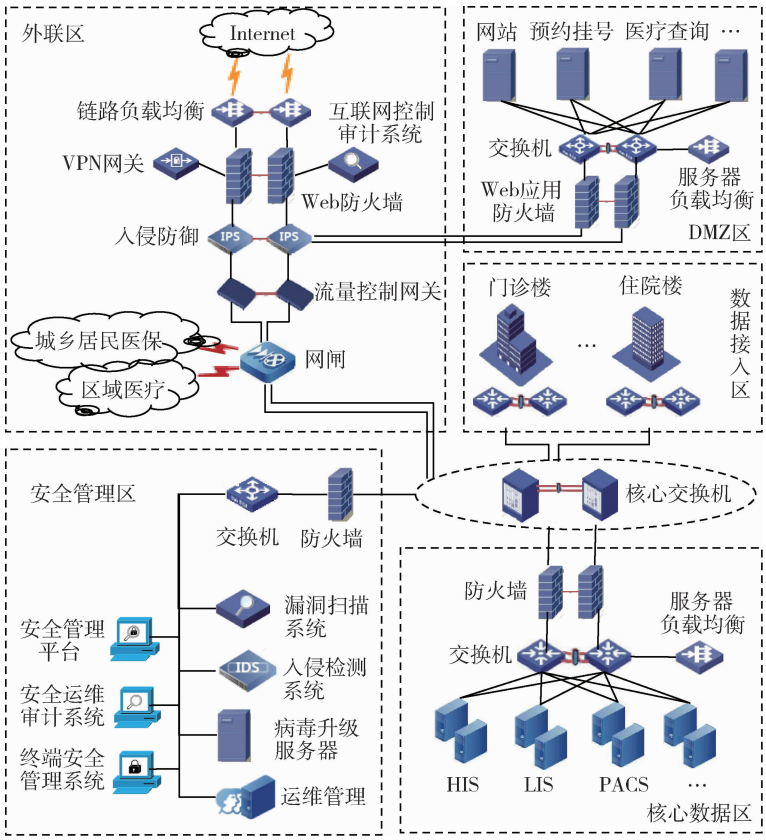


**图 1 网络拓扑**

4.1.5 核心数据区 存放 HIS、LIS、PACS 等，利用负载均衡技术，将系统服务器负载（工作任务）进行平衡、分摊到多个操作单元上执行，共同完成工作任务，从而提高网络数据处理能力，提高网络的可靠性、可用性[9]。在业务高峰期，保证网络各部分带宽满足需求，且按照业务的重要次序来指定带宽分配优先级别，在网络拥堵时能优先保护重要主机。

4.1.6 安全管理区 采用终端安全管理产品，进行终端安全管理、安全运维审计、系统漏洞扫描、病毒升级、入侵检测、运维管理，确保终端安全，提高信息系统的防范能力。

## 4.2 建立相应管理制度

建立相应管理制度是互联网医疗信息安全的重要保障。建立账号管理制度，明确医疗机构各部门人员权限，控制管理用户个人查看数据内容的权限，处理长期不使用的账号。从医院信息安全体系建设到管理、维护、安全审计等方面需要专职人员负责，定期对信息系统工作人员进行相关安全应急技能培训，提高安全防范意识和维护技能。加强互联网医疗信息工作人员的隐私保护意识培养，强化其自我约束的能力，使隐私信息得到妥善的保护。

## 4.3 制定相关法律法规，加大监管力度

立法机关应根据现有互联网和医疗方面的法律，制定出互联网医疗信息安全方面的法律法规，明确医疗卫生机构和互联网公司保证医疗信息安全的责任，规定罚则，严厉打击泄露、倒卖个人医疗信息的违法行为，为互联网医疗机构和企业提供有力的法律保障[10]。同时政府还需加强监管和服务的力度，对薄弱环节重点监管，支持互联网医疗服务企业，推动互联网医疗的发展。

## 4.4 提高自我保护意识

对患者而言，在网上进行健康咨询或分享就诊经验等行为时应谨慎，不轻易透露个人信息，不与陌生人分享信息，不访问可能存在安全风险的网站、点击不确定内容的链接或扫描来历不明的二维码。在多个网站不要使用相同的账号、密码注册并

定期修改密码、清除上网痕迹，提高自我保护意识。

## 5 结语

“互联网 + 医疗”不仅优化了医疗服务流程，使寻医问药变得方便快捷，为患者提供更好的服务，还实现医疗信息在区域医疗机构之间的共享与交换，推动医疗卫生信息化发展。而互联网医疗的信息安全问题对医疗行业至关重要，必须保证医疗数据安全，保护患者隐私信息。在互联网医疗发展中，医疗信息安全是一个综合的防范过程，利用信息安全技术加强医院信息系统的安全性，建立相应管理制度，制定出互联网医疗方面的法律法规，加大相关部门监管力度，提高患者自我保护意识，才能保障互联网医疗的信息安全。

### 参考文献


1 孟群，尹新，梁宸. 中国互联网医疗的发展现状与思考［J］. 中国卫生信息管理，2016，13（4）：356 - 363.

2 谭冲，王笑. “互联网 + ”与医疗［J］. 共产党员（辽宁），2016，68（2）：52 - 53.

3 栾运波，田珍都. 我国“互联网 + 医疗”存在问题及对策建议［J］. 行政管理改革，2017，8（3）：59 - 63.

4 马诗诗，于广军，崔文彬. 互联网医疗的隐私保护与信息安全［J］. 上海医药，2017，48（9）：14 - 16.

5 舒婷. “互联网 + ”时代的患者隐私保护［J］. 中国数字医学，2016，11（5）：41 - 43.

6 孟晓阳，朱卫国，李连磊. “互联网 + ”对医院信息系统安全的挑战与对策探讨［J］. 医学信息学杂志，2016，37（12）：38 - 41.

7 孙祥玉，孙大伟. 网闸技术在医院内外网数据交换中的应用［J］. 电子世界，2014，35（11）：64.

8 陈卫平. DMZ 区安全建设模型初探［J］. 现代电视技术，2013，24（2）：125 - 128.

9 赵峡策. 基于 Nginx 和 Memcache 的负载均衡集群架构设计［J］. 电子技术与软件工程，2017，23（5）39 - 40.

10 何博文，宁祉婷，罗维杰. 互联网 + 医疗信息安全问题探讨［J］. 价值工程，2017，35（10）：246 - 249.


（上接第 32 页）

诊量超过 3 000 ~ 4 000 人次，庞大的患者量对医院的门诊服务水平提出更高的要求。如何最大限度地减少患者在挂号、缴费、取报告等环节的排队等候时间，利用信息化手段优化门诊服务流程，是一个亟待解决的问题。医院充分发挥信息化技术优势，推出自助服务设备，用于缓解和解决就诊过程中的“三长一短”现象。在实际使用中由于自助机分流了部分患者，减少人工窗口前排长队等候的现象，随着自助机的深入推广，应用程度不断提升，必将加快患者流转速度，改善门诊秩序，提升患者满意度。患者在医院就诊的所有诊疗信息都存储在 HIS 中，可直接在自助设备上进行处方、检查检验的查询。对于医院工作人员来说，收费窗口和导医的工作压力得以减轻，采用自助设备也可避免一些人为错误的发生[10]。

### 参考文献


1 卢片，郝斐. 构建“银医通”系统优化门诊服务流程［J］. 中国医疗设备，2015，30（12）：12.

2 蒋婷婷，刘志伟，葛茜茜. 如何提高医院自助终端服务机的使用率［J］. 医院管理论坛. 2015，32（9）：55 - 56.

3 魏洋洋. 基于服务理念的医院查询交费一体机设计研究［D］. 济南：山东建筑大学，2015.

4 冯一侃. 医院门诊自助系统的对比研究［J］. 医院管理论坛，2016，33（9）：58 - 61.

5 乔刚. 医院自助一体机的管理与应用［J］. 医疗装备，2017，30（20）：57 - 58.

6 黄艳，李亚萍. 第三方支付平台“银医通”应用评价［J］. 解放军医院管理杂志，2016，23（6）：574 - 575.

7 沈静华，韩菁. 医院开展“银医通”自助结算的实践与思考［J］. 卫生经济研究，2016，355（11）：62 - 63.

8 李艳姣. 基于财务视角的医院自助挂号缴费模式研究［J］. 财会学习，2017，（21）：68.

9 郭凌菱，姜福康，郝斐. 门诊银医通系统的构建与应用［J］. 中国医学设备，2015，12（3）：52.

10 周毅. 自助设备在我院的应用［J］. 中国医疗设备，2013，28（1）：76 - 77.