互联网医院信息安全风险和应对措施分析

李建辉

长春中医药大学附属医院　吉林　长春　130021

[摘　要]近些年来，伴随着我国互联网技术的快速发展，医院对自身的医疗服务、医疗质量以及经营管理等方面也提出了全新要求，需要全面加强医院信息系统建设，以此来使互联网医院的重要信息得到有效共享与传播，全面提高医院的信息化建设水平。本文针对互联网医院信息安全风险展开分析，介绍了安全风险的类型，并提出具体的应对措施，希望能够为相关工作人员起到一些参考和借鉴。

[关键词]互联网医院；信息安全风险；应对措施

【DOI】10.12252/j.issn.2096-6288.2020.03.023

在我国进入互联网时代以来，医疗行业的整体发展水平已得到了显著提升，特别在对互联网技术进行广泛应用后，这使医疗行业内部的各个单位在许多方面都对移动互联网接口进行了开放，人们对互联网医院的信息化建设也逐渐加大了关注度。在实际建设互联网医院信息系统时，需要科学合理地利用移动互联网技术，从而改善与优化当前的医院就诊流程，有效提升医院的资源利用率，以此来为病患创造具有明显智慧特征的医疗环境，使病患满意度得到有效提高。而在医院信息平台的搭建和运行过程当中，需要针对信息安全风险采取有效的防控对策，使相关网络安全风险问题得到有效解决，进一步保障互联网医院的信息安全性，促进我国医疗行业的网络化、信息化与智能化发展。

一、互联网医院信息安全风险

对于互联网医院而言，其除了是指医院所提供的医疗服务，由原本的线下向线上进行转移以外，在诊疗流程上与实体医疗机构也存在相应的差异。而在互联网医院的实际运营过程当中，有着更为突出的数据滥用、网络安全以及隐私泄漏等威胁，这也对医疗质量的安全管理工作提出了更高要求。结合目前互联网医院的信息安全风险进行分析，可以发现其主要包括以下几个方面。

（一）信息基础设施风险

针对互联网医院的信息基础设施进行分析，其具体是指相关医疗机构在互联网医疗活动开展过程当中所必备的各项基础支撑设施，主要包括服务器、机房环境、交换器、用户终端、通信光纤以及不间断电源等。对于此类设备设施而言，其往往存在漏水、雷击、地震、火灾、被损坏、被盗窃、供电中断、温湿度超标以及通信光纤被挖断等风险问题，需要相关管理人员对此加大重视[1]。

（二）网络安全风险

互联网医院可以在互联网上暴露原本处于物理隔离的相关医院内部信息系统，并使内外网有效打通，使数据信息实现实时交互。在互联网医院的运行过程当中，可以使医院网络边界得到有效拓宽，但同时也使网络安全问题的发生概率有所增大，使受到网络攻击的安全风险点有所增加，具体表现在计算环境、区域边界以及通信网络等方面，而相关风险隐患则主要表现在恶意代码攻击、低级别访问控制、篡改、窃取、入侵、拒绝服务、泄漏、盗用等[2]。

（三）互联网医院信息系统风险

互联网医院信息系统平台具有较高的复杂性，也是互联网诊疗服务开展的重要基础。在此平台上，互联网医院监管平台、医生、患者以及第三方等，可以有效实现信息交互。从系统架构角度进行分析，互联网医院信息系统与单系统模式和线下单服务器存在区别，其通常对微服务架构以及协同模式进行采用。在信息系统运行过程当中，并非由系统来直接提供服务，而是利用网络来为用户提供服务。在此架构下互联网医院系统的应用程序编程接口、人机交互、数据分析与处理、数据采集等，都使系统的信息安全风险有所加剧。除此之外，由于不同医疗机构在互联网医疗开展程度以及信息化建设水平等方面有较大差异存在，进而使得信息系统的研发与实施能力有所不同，在系统监管方面也不够一致，容易导致互联网医院出现相关安全隐患。在互联网医院的信息系统运行过程当中还存在计算和存储瓶颈等相关风险，例如人工智能应用、可穿戴设备接入、影像数据调取以及视频问诊等都使系统的存储压力有所增加，同时其应用端并发量与访问量的剧增，也对服务器具有的计算能力提出了全新要求[3]。

（四）医患双方个人隐私风险

在互联网医院的运行过程当中，会使内外网的医疗数据具有更高的实时共享需求，这也集中了医患双方信息，减小了信息的获取难度，同时也导致信息泄漏风险有所增大。首先，注册信息泄漏风险。对于互联网医院而言，其要求医护与患者进行实名认证注册，具体要收集患者的姓名、民族、性别、人脸、身份证号、家庭住址以及手机号码等基本信息，而且还需要收集医护人员的相关信息和从业资料，并向互联网进行上传，这也使得个人隐私存在相应的泄漏风险。其次，医疗记录的泄漏风险。相关的药品企业、物流公司以及保险公司等会使用患者的就诊记录、检查检验报告、诊断书以及处方等相关医疗数据，这也产生了用户信息的滥用现象[4]。

（五）互联网医院数据风险

在互联网医院的发展过程当中，数据资产是其重要的一类资产，而大数据则是保证互联网诊疗服务精准程度的有利

依据。针对互联网医院的数据特点进行分析，其具体表现在资产不易保护、价值高、产权多元化等方面。目前，数据资产不仅未形成良好的交换市场，而且法律归属也不够明确。在实际收集、加工、使用、公开、提供、传输相关数据时，缺乏明确规定，这也增大了互联网医院的数据资产保护难度。

（六）互联网医院信息系统运维风险

针对互联网医院的运维管理进行分析，其主要是指管理运维过程具体需要涉及系统巡检管理、故障处理流程以及需求变更流程等内容，需要确保维护人员能够有效发挥自身职能，从而提高互联网医院运行的安全性和稳定性。在互联网医院信息系统的实际运维过程当中，需要涉及操作行为、网络环境、软硬件等方面，因此运维过程十分复杂，需要有效结合运维管理、运维技术以及运维人员等要素，并通过三者的相互制约，从而有效提高运维水平。一旦各部门之间的沟通不够有效，未明确划分运维责任，则容易导致系统运行期间有相关风险问题产生，对系统的运行稳定性造成影响[5]。

二、互联网医院信息安全风险的应对措施

（一）完善互联网医院信息安全管理制度

相关互联网医院需要完善自身的信息系统安全管理制度，具体包括信息系统运维管理制度、数据备份管理制度、数据中心管理制度、计算机终端使用管理制度等。在相关管理制度制定后，还需要加大对制度的执行力度，健全具体的处罚机制，以此来保证安全管理制度的有效落实，为互联网医院信息安全管理工作的开展提供指导依据。

（二）建立互联网医院信息梯度保护模式

对于互联网医院的信息安全风险防范，其目标在于使信息安全风险发生的概率得到降低，从而使互联网用户的满意度得到提升。通过有效结合安全技术模型以及管理机制，可以进一步明确互联网医院信息安全目标，并制定出科学合理的风险监管规则与处置方法，对互联网医院信息梯度保护模式进行建立。具体来说，在不同的应用场景和特征数据下，需要对强度不同的安全保护措施进行采取。除此之外，还需要将应用和数据分开，并对上云进行应用，在院内存储医疗数据。与此同时，还需要将一般信息和敏感信息区分，并对敏感信息进行加密传输[6]。

（三）提供多维度的安全服务

互联网医院信息安全为动态过程，需要持续跟踪、响应和分析全新的安全漏洞与威胁。在风险评估服务以及安全加固服务开展过程中，需要从第三方安全、人员安全、物理安全、管理制度等方面进行评估与分析，并对数据库、网络、系统以及管理策略等采取有效的安全控制措施，对安全风险问题进行及时处理。

（四）营造互联网医院安全文化

想要使互联网医院的医疗质量安全以及信息安全，不仅需要对互联网医疗有关的规范和法律法规进行出台，而且还应对使用者的安全防范意识进行提升。对此，互联网医院需要采取外训和内训、线上和线下相结合的方式，对互联网信息安全培训活动进行定期开展。与此同时，还需要对医护人员有效落实互联网诊疗法律法规以及规范操作等方面的安全培训，防止医务人员对互联网数据进行滥用。对于互联网医院技术人员，需要有效落实网络安全关键技术以及数据库操作规范等相关培训活动，使互联网医院的信息系统安全防护水平得到提升。

（五）建立信息系统应急预案

互联网医院需要对信息系统应急预案进行建立，确保相关业务的不间断运行，具体包括网络应急预案、数据灾备系统、应用系统应急预案等。在发生事故之后，需要按照最小损失使系统得到恢复，使预案实现最短时间，简单明了地制定应急预案。在应急预案当中需要对紧急事件进行说明，并要对应急预案开展预演活动，从而及时发现相关问题，有效修正预案，使预案的正确性和可行性得到保证。

（六）优化网络安全架构

在实际构建和应用医院平台时，需要合理完善网络安全架构，具有十分重要的作用。在医院的实际运作过程中，需要对与互联网时代相符合的网络架构进行设计，从而使网络架构在医院平台信息安全防护中进行合理应用，以此来保障医院内部数据的完整性和安全性。

结束语

综上所述，在互联网医院的信息系统运行过程当中还存在一些安全风险因素，进而导致在实际传播和使用信息时容易有相关的安全问题产生。对此，需要互联网医院结合信息安全风险，采取有效的解决措施，以此来维持信息系统的安全稳定运行。

参考文献

[1]连英杰，张欣，王然.刍议医院计算机信息安全风险管理策略[J].临床医药文献电子杂志，2019，7（33）：184-185，196.

[2]谭太昌，王甲甲，王加强，等.“互联网+”背景下医院信息系统风险管理研究[J].医学信息学杂志，2018，39（11）：36-39.

[3]陈旭锐.医院网络与信息安全存在的风险及应急预案处理[J].世界最新医学信息文摘（连续型电子期刊），2019，20（12）：190，192.

[4]周翔宇，王晓君."互联网+医疗"背景下医院信息安全的构建与探索[J].电脑知识与技术，2019，15（32）：61-62.

[5]陈明.掌上医院平台信息安全风险分析与控制[J].福建医科大学学报（社会科学版），2019，20（2）：22-26.

[6]刘世杰.浅析互联网时代医院移动接入的风险与等级保护的新对策[J].网络安全技术与应用，2018，12（4）：87，96.