基于“互联网 +”背景下医院网络的信息安全防护措施研究

张庆玲[1]　秦庆凯[1]　吴　波[2]
（1. 贵州省公安厅网安总队，贵州 贵阳 550001；
2. 贵州省网络与信息安全测评认证中心，贵州 贵阳 550003）

摘要：随着“互联网 +”时代的到来，信息技术在很大程度上改善了群众的生活，提升了其生产效率。随之而来的是互联网信息安全问题，例如信息安全管理制度不完善、应急方案无针对性等，这些问题使得医务工作难以顺利开展。对此，为了顺应时代发展并体现互联网 + 技术的引导价值，医院在发展中需要结合实际落实有效的信息安全防护措施，从而提升工作效果。本文就“互联网 +”背景下医院网络的信息安全防护措施进行研究，并对此提出相应看法，希望为医院信息化建设提供参考。

关键词：“互联网 +”；医院网络；信息安全防护；研究

互联网 + 主要是将传统行业以及互联网紧密结合的一种有效发展模式。此类信息化手段推动了医学领域发展，例如线上挂号、取报告单、远程问诊等方式实现线上与线下紧密结合，方便了群众生活。通常来讲，医疗机构中病人病史、治疗记录、医院资产等信息具有极强商业价值，一些不法人员借助入侵信息资料即可获取资金，且一些内部人员也可借助贩卖信息获取利益，互联网安全管理问题随之而来。对此，在互联网 + 背景下医院如何避免出现安全管理问题，成为其重点研究内容，笔者认为其在发展中需要落实制度、重视员工培训等，在最大程度上保护信息安全，推动医务工作发展。

一、互联网 + 医疗背景下医院信息安全管理发展趋势

（一）信息管理趋于复杂化

出现这一情况的关键因素在于当前医学逐渐精细化。在实际工作过程中，医院下属子系统需不断接收外部信息，同时也需要对信息进行交流、交换，此外目前很多医院内部信息传递层级要求和设备也在进一步完善，这使得内部系统面临复杂内外部环境。为了最大化满足群众需求，众多医院在发展中将科室进一步细化，且当前就诊人数不断增加，为了提升整体工作效率，医院需制定并完善合理的信息化管理制度。

（二）信息管理系统智能化

目前互联网 + 获得持续发展，其在医疗领域逐渐形成“互联网 + 医疗”体系，其主要目的在于确保用户能够在最短时间内享受便捷、优质服务，同时在发展过程中传统医疗信息会逐渐与服务资源进行整合，进而形成一个一体化的服务平台，这一平台集众多科室、管理部门于一体，这意味着医院信息安全管理系统化运作也更为普遍。

（三）信息安全涉及范围更为广泛

综合来讲很多医院医疗系统有本身数据库，不过这些数据库整体涉及面较窄，且缺少一定安全性以及稳定性。而在互联网 + 背景下，医疗机构需要联合多个部门完成服务，需要在医疗机构、市民和政府社保局之间共享各种信息，一些相应的信息和记录都可以通过物联网设备和网络云服务查阅，目前且信息和数据越来越精细化，信息安全的涉及面开始加大，探究信息安全保护措施成为众多医院研究内容。

二、互联网 + 医疗背景下医院信息安全管理存在的问题

（一）信息安全技术相对落后

多数情况下，很多医院在建设之处都有自身的信息数据库，不过相关信息数据库涉及面较窄，且不具备安全性。随着互联网 + 时代的到来，很多医院数据库系统已难以适应这一环境，在全新平台以及网络技术的支持下，患者、医院等之间的联系更为密切，信息交流也趋于精细化，这一过程中会不可避免地出现医院信息泄露情况，其中一些是人为因素泄密或者盗窃者泄密，还有可能是一些偶然性因素或者外在因素造成的信息流失等。不仅如此，一些医院积极顺应时代发展，围绕互联网 + 创设全新服务平台，但是其并未重视医护人员工作能力提升，导致互联网难以发挥其引导价值，新时期下的发展目标难以实现。

（二）信息化安全管理体制不完善

目前很多医院信息安全管理并未得到重视，对有信息查询权限的人员没有严格履行登记制度和监督制度；信息安全管理考核体制不健全，没有有效的惩罚机制和监督机制；一些管理人员并不重视信息安全管理，在制度建设方面也并未结合实际落实相应措施；部分医护人员认为医院信息安全是管理部门职责，医院在安全信息记录以及掌握方面并未制定详细规定。

三、基于“互联网 +”背景下医院网络的信息安全防护对策

（一）顺应时代发展，重视网络安全建设

在互联网 + 背景下的医院网络信息安全建设角度进行分析，前沿思想、正确发展理念是落实相关工作的关键前提。因此，在全新时代背景下，管理人员在发展中应积极顺应时代发展，结合实际强化自身思想观念建设，意识到网络安全建设对医院自身发展的影响以及必要性，这样能够为后续网络安全发展做好充分保障。笔者认为，其在发展中可以从以下几点入手：第一，医院管理人员应发挥自身引导作用，在发展中重视医院内外部网络安全问题，宣传其重要性，使更多人员参与到网络安全建设过程中。第二，针对目前网络安全管理中存在的限制性因素，管理人员应统筹规划进一步加大投资力度，同时也需要对相关的设备进行更新、完善，定期对设备进行检查，在最大程度上避免信息安全问题的出现；结合信息建设实际需求，积极组建一支网络安全管理队伍，确保网络安全检修、维修工作的专业性，这样可以进一步提升安全管理整体效果。第三，结合实际需求制定并完善相应规章制度，切实实现计算机网络安全化管理。

（二）外联网络防护安全建设

在互联网技术支持下，医院主要是结合区域卫生、银行、社保等进行互联，多元主体加入使得网络安全面临巨大挑战。不仅如此，从外联网络服务不难看出，其主要有单向以及双向调用服务，在实际发展过程中为了提升整体安全效用，前者与银行、农合等积极互联，在实际运行过程中，其主要是借助医院内部的端口向这些外联服务器发送信息，实现数据、信息的交互，双方工作人员会结合这些内容落实相应措施。为了在最大程度上避免出现相应的技术问题、信息泄露等情况，医院在全新时代下，应结合自身实际积极引入并落实安全建设防护网，其可以确保访问的方式

为由内到外，在最大程度上避免出现信息入侵的情况，例如医院内部平台、APP 等都可落实这一措施。用户在访问过程中均会与医院内部的信息进行交互，因此容易造成医院信息被泄漏的情况，甚至对正常业务造成影响。对此，医院所设立的外联网络防护安全系统，能够做到及时对漏洞进行检测，在发现其中问题时则可对其进行修复；不过结合现有资料进行分析，医院内部信息安全化问题涉及面较广，对此为了避免出现信息泄露情况医院的数据库可设置相应的信息加密装置，这样能够进一步提升管理效果，若内部人员需使用相关数据，则可借助信息化手段将其进行解密处理，切实提升整体防护效果。

（三）积极设立防火墙技术

在互联网 + 背景下，防火墙技术已经被广泛应用于网络安全防御中，其是一种智能化的形式，通过信息的处理，针对某一网络区域和用户设立相关的安全化防护措施，实现信息的有效整合以及处理，若出现未经授权的信息则会将其去除，切实来提升网络安全。同时当前科学技术趋于成熟，防火墙的功能越来越强大，经过发展其类似于一种数据隔离技术，在互联网安全管理中控制内外网的通信。此项技术较为复杂，包括信息整合技术、状态检测技术等。通过在网络层对数据进行分析、记录，再结合网络系统的需求，将信息及时呈现，从而实现全方位的数据信息监测，以免一些具有破坏性的数据通过互联网进入到用户计算机，在一定程度上避免了财产以及安全损失。相较于一般的安全防御技术，防火墙的应用更符合当下信息多元发展的现状，此项技术具有更为高效的信息筛选以及防护功能，还具有一定的安全性与灵活性，是当前我国网络安全防御系统最为常见的智能化工具，对此在互联网 + 背景下，医院在信息管理方面可积极引入防火墙技术，借此来提升信息安全管理效果，避免出现工作偏差。

（四）进一步完善风险评估机制

此种方式主要是对信息系统中不安全的因素进行管理，在发现漏洞时会结合之前记录进行修复，若遇到全新问题则会重新建立档案。结合实际进行分析，当前医院信息安全风险主要集中在技术层次以及人为因素，对此为了提升网络安全信息管理效果，医院在发展过程中需要设立专门的考核小组，结合医院实际情况制定并落实安全监测计划和方案，切实加大人员信息安全管理力度，细化行为规范，对系统的硬件基础设施、网络结构与网络环境、信息存储备份、网络安全监测以及信息应急预案等方面进行认真测试排查与考核。不仅如此，考虑到医院主要是医疗机构，其在信息技术层面缺少相应的技术，因此医院在发展中可与专业的安全服务公司合作，达到双赢的目标。

（五）强化信息安全监管考核机制

通过落实相应的制度，避免出现内部职工擅自修改计算机网络配置、盗用他人密码和 IP 地址上网情况；严禁计算机使用人员擅自安装非办公软件，信息部门做好每天的信息巡查比如网络攻击的监测。医院监管部门应充分落实保密机制，例如为了确保信息安全，内部网络系统可对信息进行备份处理；涉密文件需要使用涉密计算机对文字进行处理，在最大程度上避免信息泄露情况的出现；涉密信息不得存储在非涉密存储介质内等，严禁私自外借文档。不仅如此，医院在发展中需要从实际出发，制定信息发展工作规划，经常性地进行督促检查，检查内部的隐患，完善内部管控。

（六）设立信息防范系统

在互联网 + 背景下，针对医院内部网络信息安全，相应的管理部门则需要建立应用相应的数据库，从而将怀疑为病毒的数据与数据库的内容进行比对，以此来确保信息的安全性。为了达到最佳的判断效果，早期数据库的建设至关重要，在建设过程中，相关的单位需要将安全信息数据进行收集，才能顺利实现对病毒数据的识别。若早期数据库建设不到位或者数据不完善，当计算机受到病毒攻击的时候，数据库往往难以及时准确判别这些病毒数据，导致病毒进入电脑造成严重损失。当前很多病毒数据库建设存在诸多问题，导致针对病毒的防护效果很差，难以实现对计算机的有效保护。为而为了达到计算机信息安全的目标，有必要建设与医院实际相符的病毒防御以及甄别体系，可以定期对计算机内部文件进行扫描，及时清除危及计算机安全的病毒和木马。同时，还要针对计算机系统进行及时升级和维护，提高系统完整性安全性，避免为黑客留下可以利用的漏洞。此外，还要注重做好计算机设备配置的升级，提高计算机运行安全性。还要做好计算机机房的安全防护，要注重做好防火操作，还要规范应用计算机。

（七）重视人员综合能力提升

为了进一步实现医院内部信息管理目标，笔者认为医院在发展中应着手提升管理和工作人员的能力。通过落实必要的措施，使工作人员具备符合医院运营标准的业务能力以及职业素养，并有一定的应急能力，可以及时解决实际操作中存在问题以及突发情况。首先，部门管理人员需立足实际，结合绩效管理体系和人员素质提升体系，引导内部人员积极参与各类培训，使其掌握全新的技术以及方法，并将这些内容落实于信息安全管理以及服务过程，及时解决当前工作中存在的难点问题；医院也需同时相应的奖励机制，鼓励管理和工作人员积极参与培训过程。其次，结合人员能力发展目标制定培训方案。为了确保培训的有效性以及针对性，可以发放调研问卷，及时、精准掌握员工对内部培训体系、绩效体系存在的疑惑以及建议，并汲取其中有价值的内容将制度进一步完善，从而确保培训的针对性以及有效性。第三，选择有针对性、符合员工实际需求的培训方法，医院需围绕工作内涵、员工实际需求，结合其差异性可以落实分有效培训法，确保员工整体能力和素养的提升。这样，医院在发展中重视工作人员综合能力提升，利于后续网络信息安全管理工作的顺利开展，切实提升整体管理效果。

四、结语

综上所述，在互联网 + 背景下医院在发展过程中重视网络的信息安全以及管理，利于改善当前信息管理工作现状，提升整体管理效果。因此在发展过程中，管理部门需要深入分析目前网络信息安全管理中存在的不足，并结合医院发展实际需求落实有效措施，如提升人员综合能力、完善制度体系等，切实推动医院网络信息安全管理工作发展。

参考文献：

[1] 章俊航，王轶群，王卉，徐小林 .B/S 模式下的医院网络信息安全防护系统设计与应用 [J]. 中国医学装备，2020，17（05）：181-185.

[2] 庄一峰 . 基于大数据背景的医院网络信息安全防范分析 [J]. 网络安全技术与应用，2020（11）：138-140.

[3] 杨晓毓 . 大数据背景下医院网络信息安全防范机制构建策略 [J]. 财经界，2021（30）：19-20.

[4] 金琰 . 基于“互联网 +”背景下医院网络的信息安全防护措施 [J]. 网络安全技术与应用，2022（02）：121-123.

[5] 沈颖杰 . 分析网络信息安全防护体系及其在医院网络系统中的运用 [J]. 电子技术与软件工程，2019（03）：182.