

移动医疗应用终端综合管理平台研究与应用

陈军伟 吕佳蔚 王 宁 李 鹏 辛海燕 徐 浩

(青岛大学附属医院 青岛 266003)

〔摘要〕 分析移动医疗应用带来的挑战, 介绍移动终端综合管理平台设计与部署、技术实现、功能模块、应用效果, 指出该平台的应用能够方便医护人员开展临床工作, 提升医院管理部门对移动医疗服务的掌控能力。

〔关键词〕 移动医疗; 信息系统; 信息安全; 信息管理

〔中图分类号〕 R-056 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673-6036.2017.12.005

Study and Application of Comprehensive Management Platform for Mobile Medical Application Terminals CHEN Jun-wei, LV Jia-wei, WANG Ning, LI Peng, XIN Hai-yan, XU Hao, The Affiliated Hospital of Qingdao University, Qingdao 266003, China

〔Abstract〕 By analyzing challenges brought along by mobile medical application and introducing design, layout, technical realization, functional modules and application effect of the comprehensive management platform for mobile terminals, the paper points out that application of the platform would facilitate medical staffs with clinical work and enhance control ability of management department of the hospital on mobile medical service.

〔Keywords〕 Mobile medical; Information system; Information security; Information management

1 引言

随着信息技术的快速发展, 移动医疗已被广泛应用在无线查房、移动护理、药品管理和分发、患者标识识别、会诊管理、临床业务查询、远程诊疗、预约诊疗等领域。移动医疗的应用使得医务人员可以随时随地了解患者病情变化, 提高医务人员诊疗决策的及时性和效率, 给患者提供一个安全、简单、便捷、舒适的就医过程, 代表医疗信息化应用的发展趋势^[1-2]。

〔收稿日期〕 2017-09-07

〔作者简介〕 陈军伟, 硕士, 工程师; 通讯作者: 李鹏, 硕士, 工程师。

青岛大学附属医院在移动医疗应用方面的探索主要经历 3 个阶段, 最初以院内无线局域网应用为主, 医务人员以移动医疗推车、IPAD、PDA 等为载体, 完成查看病历、检查检验报告、病历书写、患者身份确认、医嘱核对和执行等医疗活动, 实现患者床边医疗服务。第 2 阶段推出面向患者的移动医疗应用程序, 患者通过智能手机就可以完成网上预约挂号、在线支付、在线查看检查检验报告等, 实现医疗信息服务由院内向院外的拓展。第 3 阶段推出基于移动互联网的移动医疗应用程序, 如口袋医生、青医医生等, 医务人员在个人智能手机上安装上该程序后, 无论身在何处, 只要有 4G 或网络信号就可以实时查看在院患者的病历资料, 极大地方便医生的临床工作。

2 移动医疗应用带来的挑战

基于移动互联网的医疗应用给医务人员的工作带来前所未有的便利,但也给医疗信息安全和信息管理带来巨大的挑战,主要表现在以下几个方面:第一,医务人员使用自带移动设备办公(Bring Your Own Device, BYOD),从而使得个人日常生活应用程序和医院诊疗数据混杂,必然会带来医院医患数据泄漏、隐私泄漏等风险;第二,个人智能手机中毒、丢失等情况时有发生,在手机中存储的医患数据如没有加密机制的保证,医患数据泄漏的危险系数增大;第三,移动终端通过互联网与院内信息系统交互数据,数据传输过程如不采取一定的加密机制极易造成数据泄漏或被窃听;第四,移动医疗应用的智能终端数量不断增加,终端设备的注册、使用、挂失、淘汰等全生命周期管理没有有效的解决方法,智能终端的运行状态无法了解,安全策略的调整和配置下发也无法批量进行;第五,未来将有更多的移动业务系统安装到个人手机上,对于这些移动业务系统的升级、维护和管理缺少统一的系统平台支持^[3-4]。通过对上述几个方面的分析并结合建设几代移动医疗应用过程中的经验,设计和开发医院移动医疗终端综合管理平台。

3 平台设计与部署

3.1 功能设计

从终端、管道、云端3部分入手设计移动终端管理平台,功能主要涵盖安全桌面(Mobile Security Desktop, MSD),安全容器(Mobile Security Container, MSC),设备管理(Mobile Device management, MDM),应用管理(Mobile Application Management, MAM),内容管理(Mobile Content Management, MCM)等核心模块。为保障数据传输管道的安全,设计全新的移动接入服务(Mobile Access Services, MAS),通过一定的数据加密技术保证数据和传输通道安全方案,从而解决医院移动医疗终端的设备、应用、内容管理以及接入安全等问题。

3.2 部署架构

需要从4个层面考虑移动终端综合管理平台的部署,分别为移动终端层、网络层、管理平台层和业务应用层。移动终端层主要实现医疗应用程序在客户端设备上的安全运行;网络层主要实现数据和传输通道的安全;管理平台层主要实现对设备、应用程序、内容、策略、统计等管理功能;业务应用层主要实现移动医疗应用程序对业务系统的操作。系统平台的部署架构,见图1。

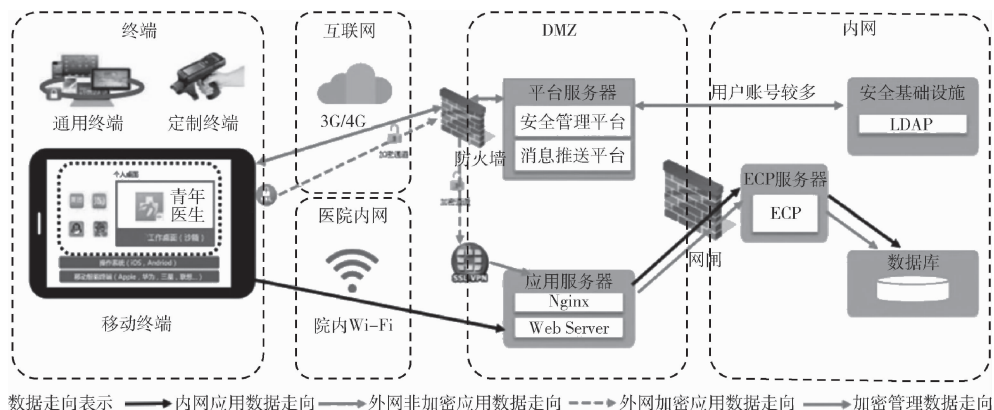


图1 移动医疗应用综合管理平台部署架构

4 技术实现^[5-6]

4.1 工作区安全保护

为实现对用户工作区的安全保护,提出安全容器的概念,采用终端沙箱隔离技术,彻底分离个人区和工作区,为用户提供一个安全的工作环境,实现对数据内容的保护,确保工作和个人生活互不影响。

4.2 数据安全保护

通过应用密钥分离技术,对安全容器中的数据、文件等内容进行加密,保证医患数据和文件的安全性。同时还建立文档水印防泄漏机制,确保在移动终端上的医患数据不被窃取和泄漏,防止患者的病历、档案等信息外流。医护人员使用移动终端打开的文件都已经采用文档水印机制,生成了和用户名一一对应的水印代码,这样就对数据泄漏有可追溯的依据。在极端情况下即使患者的信息被窃取,在特定加密算法的保护下,窃取者也无法打开加密后的数据。

4.3 传输通道安全保护

医务人员使用移动终端访问业务系统主要分为院内和院外两种情况。当医护人员在医院内部时,大都通过医院内部无线网连接网络,医院内部网络是一个相对安全的网络环境,所以在这段管道内数据传输可以应用非虚拟专用网(Virtual Private Network, VPN)传输。医务人员外出时经常需要在线关注患者的情况,就必须通过公网连接到医院的内部业务系统进行操作,数据在传输的过程中很容易被截获,导致数据泄漏。因此设计 VPN 安全接入机制,当医护人员通过公网连接院内业务系统时,VPN 自动连接,当退出业务系统时,VPN 自动断开,无须医护人员做任何操作。在数据传输过程中,通过应用沙箱级 VPN 隧道技术、国密/AES-256 高强度加密算法以及对主流第 3 方 VPN 的支持等,确保数据在传输过程中无法被窃取和监听,传输通道安全保护过程,见图 2。

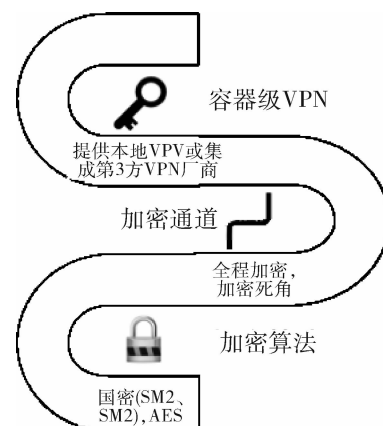


图 2 数据传输通道

4.4 移动终端管理策略

对于移动终端的管理主要从硬件准入、功能限制、软件配置等方面实现管理目标。硬件准入机制将终端设备与用户信息绑定,实现设备注册、认证、激活、使用、淘汰等全生命周期管理。功能限制机制可以将限制策略定向下发至移动终端,限制设备的某些功能如摄像头、蓝牙、声音等。软件配置管理可以将配置策略文件如密码、VPN、数字凭证等定向下发给终端,实现设备的批量管理。

5 功能模块

5.1 移动终端设备管理

通过将移动终端设备与用户个人信息在系统中绑定,实现对设备的注册、认证、激活、使用、淘汰等全生命周期管理。系统平台可以向移动终端定向推送消息、下发安全策略、获取终端设备定位、跟踪终端设备运行状态等。

5.2 应用程序管理

应用程序管理模块主要实现企业应用商店和应用管理功能,保证各应用程序的安全、可靠、可控。系统支持对 IOS 企业应用、安卓企业应用、iTunes 应用商店应用、Web 应用等 4 种类型应用程序的上架、下发、下架等应用全生命周期的管理。对于应用程序在安全容器中产生的所有数据进行加密处理,数据传输过程也进行加密保护,确保业务

数据安全。

5.3 工作区内容管理

工作区实现了对医院内部文档数据的管理,主要包括文档的上传、修改、下发和删除等,实现对所有移动终端应用文档的加密。工作区实现对音频、视频、Office 文档、图片、PDF 等多种格式文件的支持,应用过程无需调用本地的阅读器,做到个人区与工作区的完全隔离。工作区文件打开后,自动添加数字水印,防拷贝、防截屏,真正做到工作区内容的安全自主可控。

5.4 通讯录管理

移动终端管理平台上提供通讯录功能,医护人员可以在院内通讯录中方便地找到同事的联系方式,可以通过终端应用软件相互发送信息或拨打语音电话,沟通工作问题。这种内部通讯模式保障医务人员通讯的安全与便利,节约用户的通讯费用。

6 应用效果

移动终端综合管理平台自 2017 年 2 月开始运行,到目前为止已有近 1 000 名医务人员自带移动智能终端在系统中注册。在应用程序管理区已经上架青医医生、办公自动化、内部查询、医院工作日报等移动应用程序。管理平台的启用给医务人员的日常工作带来极大的便利,缓解信息技术管理部门

的工作压力,降低医院信息安全的风险,受到好评。

7 结语

移动医疗应用将医疗信息服务从院内拓展到院外,给医护人员开展临床工作带来方便,提高诊断效率,提升医护水平和服务能力。移动终端管理平台将医院的移动医疗应用程序和终端设备纳入统一的管理,提高医疗信息安全级别,增强医院信息技术管理部门对移动医疗服务的把控能力。

参考文献

- 1 陈文洁,徐腾达,阮学平,等. 自带移动设备办公在医疗机构中的应用 [J]. 中华医院管理杂志, 2016, 32 (8): 634-637.
- 2 汪鹏,吴昊. 国内外移动互联网医疗应用现状及未来发展趋势探讨 [J]. 中国数字医学, 2014, 9 (1): 8-10.
- 3 李鹏,辛海燕,苗元青,等. 工作流技术在医院办公流程再造中的应用 [J]. 中国数字医学, 2015, 10 (1): 109-111.
- 4 胡建平,高晓飞,刘娟,等. 移动互联网医院信息安全与监管平台 [J]. 中国卫生信息管理杂志, 2015, 12 (1): 14-19.
- 5 冯登国. 网络安全原理与技术 [M]. 北京: 科学出版社, 2003.
- 6 国家密码管理局. GM/T 0024-2014 SSL VPN 技术规范 [S]. 2014.

《医学信息学杂志》开通微信公众号

《医学信息学杂志》微信公众号现已开通,作者可通过该平台查阅稿件状态;读者可浏览当期最新内容、过刊等;同时提供国内外最新医学信息研究动态、发展前沿等,搭建编者、作者、读者之间沟通、交流的平台。可在微信添加中找到公众号,输入“医学信息学杂志”进行确认,也可扫描右侧二维码添加,敬请关注!



《医学信息学杂志》编辑部