医院外联平台建设解决方案

施文杰

（江苏省老年医院（江苏省省级机关医院）信息中心 南京 210024）

〔摘要〕 介绍医院外联平台架构设计，包括逻辑、网络架构，从内外网隔离、数据关联、数据传输、辅助策略等方面阐述平台安全策略，从网络环境和硬件设备方面实施准备，讨论平台效果，指出其有助于医院与患者间信息共享，提升医疗效率和服务质量，优化就医流程。

〔关键词〕 医院；外联平台；平台建设；架构设计；安全保证

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2018.11.010

Solution for Building of Outreach Platform in the Hospital *SHI Wenjie*, *Information Center*, *Jiangsu Province Geriatric Hospital* (*Jiangsu Province Official Hospital*), *Nanjing 210024*, *China*

〔**Abstract**〕 The paper introduces the structural design of outreach platform in the hospital including logic and network architecture. It elaborates on the security strategy of the platform in several aspects such as separation between intranet and extranet, data association, data transmission, auxiliary strategy and so forth. It discusses the preparation and implementation of platform building from network environment and hardware equipment and the effect of platform, points out that the platform can facilitate the information sharing between hospital and patients, improve medical efficiency and service quality as well as optimize the process to seek medical advices.

〔**Keywords**〕 hospital; outreach platform; platform building; architecture design; safety guarantee

1 引言

经过多年的信息化建设，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）、电子病历系统（Electronic Medical Records，EMR）等信息系统已在医院运行稳定且存储了海量的患者诊疗数据信息，具备数字化医院的基本特征。但是患者没有获取这些信息的快捷方式，不能直观、充分地享受到信息化带来的便利。医院外联平台借助互联网开放、互联的特性，将医院的内部接口以“互联网＋医疗”的形式提供给公众，兼顾安全性，支持第 3 方应用接入，打破医院内外网络的限制，实现院内院外业务协同，最终形成以医院为中心的医疗生态系统[1]。有效改善患者就医体验，优化诊疗流程，提升医疗效率和服务质量，从长远看还有利于建立统一的数据平台，更有针对性地提供服务，增加医疗服务附加值。

2 平台概述

2.1 技术

外联平台为医院提供快速安全的互联网接入服务，采用“防火墙＋网闸＋前置机”的方案，通过

〔收稿日期〕 2018－08－07

〔作者简介〕 施文杰，工程师，发表论文 5 篇。

认证和加密机制尽可能将安全风险隔离在平台之外，保证院内业务系统的安全。采用 Web Service、视图、存储过程等方法与医院 HIS、LIS、PACS、EMR 等业务系统进行数据交互，提供标准统一的互联网医疗服务[2]。对内封装业务逻辑，对外提供统一接口服务，方便第 3 方接入以及医院管理与统计。力求将所有对外服务进行统一封装与标准化，降低第 3 方对接医院的成本，最终形成以医院为中心的医疗生态系统。

2.2 功能

外联平台是医院信息资源共享的平台，是医疗数据流转的枢纽。患者可以通过多种接入外联平台的终端如医院官方网站、掌上医院 APP、医院微信公众号等实现信息查询、门诊缴费、预约挂号等功能，满足不同层面、需求患者的求医期望。医务人员也能实现如接收院内通知、危急值处理、患者影像资料调阅、EMR 查询等功能[3]。现阶段平台应用以方便患者为中心，优化就医流程，提升服务质量。

3 平台架构设计

3.1 概述

原则是多层隔离，最外层的公网用户与最内层业务系统数据之间必须经过多层防护和隔离，组成安全有机的整体。在保证内层业务系统安全平稳运行的前提下尽可能提高平台服务质量和用户体验。

3.2 逻辑架构

外联平台是医院对外业务的中间平台，是连接医院业务内网和互联网的桥梁。使用业务逻辑封装及统一接口服务为第 3 方应用通过外联平台对接医院业务系统提供便利，实现院内业务扩展到院外。为满足医院业务发展需要，平台功能将逐步完善，提供更多、更丰富的创新性第 3 方服务[4]。平台逻辑架构，见图 1。

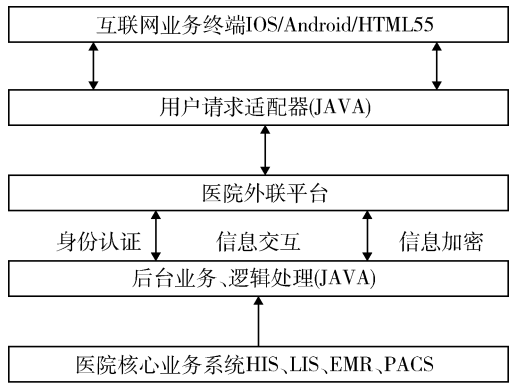

图 1 外联平台逻辑架构

3.3 网络架构

从安全性考虑外联平台最好部署在院内。医院需要借助防火墙和网闸隔离内外网，防止外网攻击影响到院内业务系统的正常运转。医院通过外联平台统一接口为患者和第 3 方提供相关医疗服务。数据库数据量大，与内网核心系统难以剥离，因此在内外网数据交换区部署前置机。当外联平台需要业务数据时向内网核心系统提交请求，由前置机获取到相应数据后再提供给平台使用[5]。平台通过网闸与医院内网前置机交互数据，前置机再将交互后得到的信息送到内网业务系统，由业务系统直接完成读、写库操作。平台网络架构，见图 2。

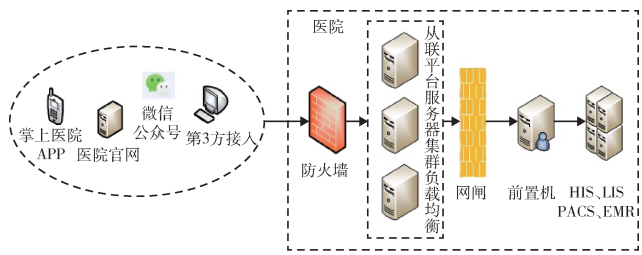

图 2 外联平台网络架构

4 平台安全保证

4.1 概述

医院外联平台作为面向患者服务的互联网开放平台，需要从 HIS、LIS、PACS、EMR 等核心业务系统获取所需服务及数据信息。医院为外部访问者建立从互联网进入内部网络访问信息系统的通道，

其面临信息安全风险不容忽视，必须建立完善的安全策略[6]。

4.2 内外网隔离

为确保医院核心业务系统安全，通过网闸将医院网络分隔为外网和内网两部分，核心业务系统部署在内网。网闸遵循单一服务、定向交换、不支持协议解析 3 项基本安全原则，从物理上实现内外网隔离。网闸通过黑白名单对交互进行限制，保证院内数据的绝对安全[7]。当外联平台需要数据转发到内网时需按照事先制定好的 IP 地址和端口号的映射规则访问内网。前置机实现业务数据的内外网隔离，外界只能访问前置机，无法直接访问医院业务信息系统，保证数据安全。外联平台服务器和前置机之间通过双向安全超文本传输协议（Hyper Text Transfer Protocol Secure，HTTPS）请求通过，此方案在保持内外网络物理隔离的同时能够在两个不同安全等级的网络之间进行实时、适度、可控的数据交换和应用服务[8]。

4.3 数据交换

医院外联平台与内网前置机采用基于网闸的数据交换方式，首先对接收到的应用数据包剥离所有传输控制协定/网际网路协定（Transmission Control Protocol/Internet Protocol，TCP/IP）网络协议和应用层协议，对数据文件进行完整性和安全性检查；随后平台立即发起对前置机 TCP/IP 协议的数据连接，将平台服务器与前置机进行连通；最后数据块文件以静态方式在内外网络间进行“摆渡”，保证内外网数据能够安全、可靠、完整地交换，实现最高级别的安全保障[9]。前置机收到数据块文件后立即进行 TCP/IP 和应用协议的封装并通过内网与业务信息系统进行数据交互。一旦数据请求完成，前置机立即中断与外网的连接，恢复到完全隔离状态。

4.4 数据传输

医院外联平台采用负载均衡服务器集群的方式部署于外网防火墙后并限定只能与被授权的第 3 方服务器进行交互。通过 IP 地址和密钥加以验证，只允许被授权的第 3 方 IP 地址数据包通过防火墙传递至外联平台服务器，阻断其他 IP 地址的数据包请求[10]。数据传输采用安全套接层协议（Secure Sockets Layer，SSL）进行加密传输，确保不被窃听和篡改，维护数据的完整性。传输敏感信息需强制使用方式保证机密性和完整性，在实施部署过程中采用 3 重数据加密标准（Data Encryption Standard，DES）高强度加密算法，加入 SSL 层的虚拟专用网（Virtual Private Network，VPN）隧道技术，降低中间人攻击风险，保证通讯完全私密，实现数据传输安全可靠[11]。

4.5 辅助策略

外联平台的安全保证来源于对系统的有效管控，主要体现在平台运营的过程安全、权限管理、安全审计、日志分析、业务复核、数据安全以及多维度安全措施的应用。安全建设是一个持续过程，要配有专职网络安全管理员，通过例行检查、漏洞扫描及时发现问题并补救。还应建立相应管理制度、流程，定期演练，常态化管理，才能在出现安全异常时有效解决问题，保证网络安全。

5 平台建设实施

5.1 网络环境

医院对外需提供百兆互联网专线接入服务，平台专有互联网域名；对内保证平台服务器与内网前置机交互网络带宽不小于 20 兆。提供每台外联平台服务器内网、外网 IP 地址各 1 个并开放相应端口通过网闸与前置机做端口映射。

5.2 硬件设备

医院需准备 4 台 DELL R940 高性能服务器，将其中 3 台构成具有负载均衡能力的外联平台服务器集群，1 台作为内网前置机使用。为确保平台良好的用户体验，每台服务器均配置 128GB 内存、1TB 高转速硬盘。还应准备华为 USG6600 硬件防火墙，金电网安 FerryWay 网闸，包括内端机、外端机和独立硬件隔离信息交换区。内部数据交换速率大于

1Gbps，并发连接会话数大于 5 000，系统延时小于 2ms，支持 HTTP/HTTPS、POP3、SMTP、FTP、SAMBA、NFS、DNS、TCP、UDP、SOCKS、RTSP、MMS 等主流网络协议。

6 应用效果

6.1 信息共享化

平台围绕患者和医生两大主体，有效改善其信息不对等的情况。以医院现有业务信息系统为基础，利用网络以及无线终端设备实现医务人员移动工作，医疗服务从院内到院外的全流程信息化服务新模式。通过外联平台统一接口接入的相关医疗服务，以诊前挂号、医疗咨询、健康服务以及诊后收费、报告查询等作为基本入口，将医院信息系统延伸到患者移动终端。患者可以利用移动终端获取各项信息，如医嘱、病历以及检验报告等，实现医院与患者间信息共享，提升医院服务质量，提高患者满意度，在一定程度上增加用户粘度。还应考虑逐步从诊前、诊后服务向诊疗核心方向进行探索，更好地推进医疗服务体系建设。

6.2 提高工作效率，降低成本

传统模式下患者的每个就医环节如咨询、挂号、缴费、取报告等均需要医院工作人员参与。而现阶段整体就医流程中门诊咨询、挂号、收费等都为数据和资金的传递，均可通过外联平台来实现。患者通过移动终端进行这些操作。平台可同时为多名患者服务，单位时间内的业务处理能力显著高于人工操作。医院现已减少相关部门 25% 的工作人员，提高工作效率，降低人力成本支出。

6.3 优化就医流程

缩短患者等待时间，在外联平台投入应用前医院患者平均每次就医等待时间为 2 小时，挂号、收费、检查、领取结果都需要患者在现场等待。平台上线应用后患者通过移动设备进行操作，平均等待时间缩短为 1 小时。缩短患者在医院内的非诊疗时间，注重患者就医体验。

7 结语

医院外联平台基于现有核心业务信息系统，借助无线网络通讯技术和智能移动终端实现患者与医院间的信息互动，优化就医流程，提高患者满意度，提升医院医疗质量和市场竞争力[12]。未来还要在平台现有基础上拓展在线问诊、随访、慢病管理等新功能。尤其是慢病管理方向，将来会有非常好的应用前景，这部分数据的利用价值也较高。

参考文献

1 王淑，于广军，蒋蓓，等. 基于移动在线技术的全流程医疗服务平台建设与应用［J］. 中国数字医学，2015，10（9）：49－51.

2 孙国强，由丽孪，陈思，等. 互联网＋医疗模式的初步探索［J］. 中国数字医学，2015，10（6）：15－18.

3 傅廷君，吴庆斌，钟军锐. 基于微信平台的移动医疗应用［J］. 中国数字医学，2015，10（9）：61－63.

4 史嘉兴，丁绍平，任静，等. 掌上医生平台的设计与临床应用［J］. 中国数字医学，2017，12（4）：64－67.

5 程瑶，应凌云，焦四辈，等. 移动社交应用的用户隐私泄漏问题研究［J］. 计算机学报，2014，37（1）：87－100.

6 刘雨，包国峰，王玮，等. 移动互联网医疗数据安全机制的设计与实现［J］. 中国医疗管理科学，2015，5（5）：55－59.

7 刘锋，吴东东，姬晓波. 医疗网络与外部网络信息安全交互方案设计［J］. 中国数字医学，2015，10（10）：96－98.

8 温海燕，穆卫农，胡华，等. 区域卫生信息化环境下信息安全策略与实践［J］. 中国卫生信息管理杂志，2013，10（2）：157－162.

9 葛小玲，郭罗军，刘枭雄，等. 基于移动互联网的掌上医院信息安全策略与实践［J］. 中国数字医学，2015，10（6）：12－15.

10 罗永刚，孙军，司子瑾. 移动医疗应用中的信息风险分析［J］. 中国数字医学，2013，8（10）：15－17.

11 卞松，帅梅，高黎，等. 移动医疗系统在医院中的实现［J］. 中国医疗设备，2015，5（5）：76－78.

12 王立准，王春雨，魏瑜帅. 无线移动技术在数字化医疗中的研究和应用［J］. 医学信息学杂志，2015，36（4）：25－28.