医院电子病历电子签名需求分析及实施方案*

史森中

(陆军军医大学大坪医院野战外科研究所信息科 重庆 400042)

〔摘要〕 以陆军军医大学大坪医院为例，分析电子病历面临的安全问题以及使用电子签名的必要性，从网络架构、电子签名工作流程等方面阐述电子病历 CA 认证实施方案，指出该方案有助于实现医院医疗管理流程优化，提高安全保障。

〔关键词〕 电子病历；电子签名；CA

〔中图分类号〕R-056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673-6036.2019.03.009

Requirement Analysis and Implementation Plan of Electronic Signature on Electronic Medical Records in Hospitals

SHI Senzhong, *Department of Information*, *Institute of Surgery Research*, *Daping Hospital*, *Army Medical University*, *Chongqing 400042*, *China*

〔**Abstract**〕 The paper analyzes the security issues of Electronic Medical Records (EMR) and the necessity of utilizing electronic signature by taking Daping Hospital, Army Medical University as an example. It also elaborates on the implementation plan of CA authentication from the aspects of network architecture and the electronic signature procedure, etc., points out that such a plan facilitates the optimization of management process in hospital and improves security level.

〔**Keywords**〕 Electronic Medical Records (EMR); electronic signature; CA

1 引言

近年来电子病历（Electronic Medical Records，EMR）在各大医疗机构得到广泛应用，陆军军医大学大坪医院也上线该系统，这顺应医疗信息化发展趋势，也符合信息化应用向临床发展的迫切需求。但是 EMR 为临床工作开展提供便利的同时也带来新的挑战，由于系统应用前期医院更注重其功能性，较少关注其数据安全，没有统一的标准规范来管理，致使许多患者及家属往往对 EMR 数据的真实性、安全合法性存在诸多疑问[1]。近年来医院信息系统在医疗机构得到很好的发展及应用，管理层更加重视运用电子签名来取代手写纸质签名，从而减少纸质文档、病历存储的同时还能增强患者合法权益的保护、提升法律效应。

2 电子病历面临的安全问题

2.1 身份验证

此前医院信息系统的身份验证相对薄弱，EMR 也不例外，二线、三线医师将账号和密码交予一线医师，导致存在冒用他人账号、密码登录查看病历

〔修回日期〕 2019-01-28

〔作者简介〕 史森中，工程师，发表论文 24 篇。

〔基金项目〕 2018 重庆市社会科学计划普及项目“患者科学就医的宣教与普及”(项目编号：2018kp08)。

记录，甚至修改病历内容的情况。此外医师大多使用简单设置的数字密码，极易被猜测识别，一旦出现医疗问题及纠纷，病历内容极易被篡改，很难追究具体相关责任人，更加难以定责和取证。

2.2 数据存储安全

以往 EMR 数据直接存储于医院数据存储服务器，数量巨大，难以进行加密，也容易遭到不法入侵，而医院信息系统中没有相应措施进行验证，无法甄别 EMR 文件是否被篡改过。

2.3 实时性

每台计算机终端内的系统时间可以任意设置，并非与当前时间一致，可能出现每台终端计算机时间都不一致的情况。而国家相关标准中对电子病历中患者各类诊疗记录、各流程环节都有十分严格的要求，特别是实时性。因此在这样的情况下难以达到电子病历实时性的要求。

2.4 合法性

未实行签名的医疗电子文书不具备法律效力，此前的医院信息系统没有可行的技术或方案解决该问题，因此电子签名实施前医疗文书以及电子病历无法核实数据真实性以及可靠性。

3 使用电子签名的必要性

3.1 概述

2004 年 8 月《中华人民共和国电子签名法》正式发布，标志着电子文书已得到法律的认可与保护。数字医疗、智慧医院的建设与发展离不开电子签名的实施及应用。医院电子病历应具备法律效应，减少数据安全风险，生成法律认可的医疗文书，普及并规范电子签名技术成为必不可少的举措。2017 年 4 月原国家卫生计生委发布《关于印发电子病历应用管理规范（试行）的通知》，指出“有条件的医疗机构电子病历系统可以使用电子签名进行身份认证，可靠的电子签名与手写签名或盖章具有同等法律效力”[2]。

3.2 实现可追溯性

电子病历系统用户参与其各个核心环节，医护人员所提交的医疗文书、诊疗记录等必须可追溯、追责。每个表单以及各项操作加以数字签名能够起到与手写签名或盖章相同效果，使操作者无法否认个人操作行为[3]。

3.3 实现无纸化管理

此前大坪医院病历保存是经医务人员人工打印装订，由医院病案管理员统一收集进行分类、核对、捡入后盖章保存。由于未实施电子签名前其文书以及数据无法得到法律认可，保存并无意义，只能采取较为原始的纸质病案流程保管。原卫生部明确指出医疗机构住院病案存放不少于 30 年，门（急）诊病案存放自患者最后一次就诊之日起不少于 15 年，因此医疗机构纸质病案日积月累、不断增加，对存放空间与环境、人力和物力资源等方面带来极大挑战，加大医院在病案管理上的投入。

4 电子病历 CA 认证实施方案

4.1 概述

数字证书及认证中心（Certificate Authority，CA）指发放、管理、废除数字证书的第 3 方权威管理机构。CA 认证对应用系统主要提供以下安全服务功能。一是身份认证。数字证书如同公民身份证，能够证明授权使用者的身份，较身份证其多出一个公共密钥（简称公钥），能够确保公钥与额定实体之间的联系。系统登录实施用户与实体之间双向认证机制，达到一人一证、一机一证、持证上岗的效果，如果没有数字证书则不能登录系统。二是数字签名。保证证书持有者身份的合法性[4]，保护数据及数据单元的完整性并签发证书，以防证书被伪造或篡改。三是可信时间戳。通过权威可靠的第 3 方公共时间服务机构以及法定时间源颁发具有法律效力的时间电子凭证，时间戳与电子签名唯一对应[5]。其中包含电子数据的 Hash 值、产生时间、时间戳服务中心信息等。必要时其可作为时间的法律公证。电子病历 CA 中心结构，见图 1。可信安全认证平台为应用系统提供安全服务，主要通过应用系统调用安全中间组件来实现，安全中间件是为应用系统调用安全平台的应用程序接口（Application Program Interface，API），所有安全机制都由该接口来实现，包括证书验证、数据库接口、加密与

解密、数字签名、可信时间戳、黑名单查询等[6]。

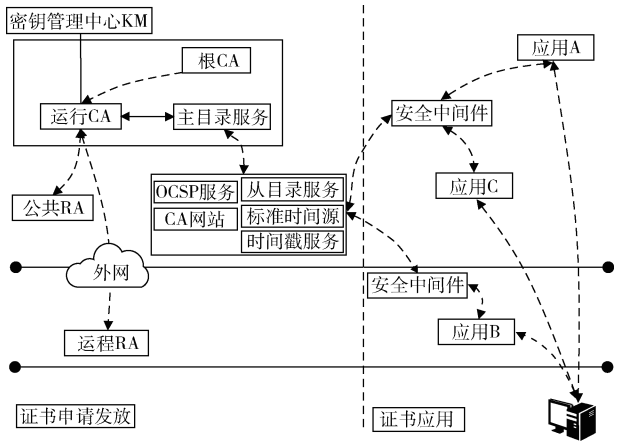

图1 电子病历 CA 中心结构

4.2 网络架构

大坪医院至今仍沿用基于客户机/服务器（Client/Server，C/S）与浏览器/服务器（Browser/Server，B/S）架构开发的“军字一号”医院信息系统（Hospital Information System，HIS），这是一套极为复杂的综合系统，在此基础上实现第 3 方可靠认证需要对系统进行改造，如通过 CA 技术来实现认证。医院在本地应用服务器前端需要架设区域 CA 安全网关，医院在进行使用者身份认证时需要将认证信息发往建立在市卫生局的注册机构（Registration Authority，RA）分中心。分中心通过双链路与区域中心进行联通。其应用结构，见图 2。

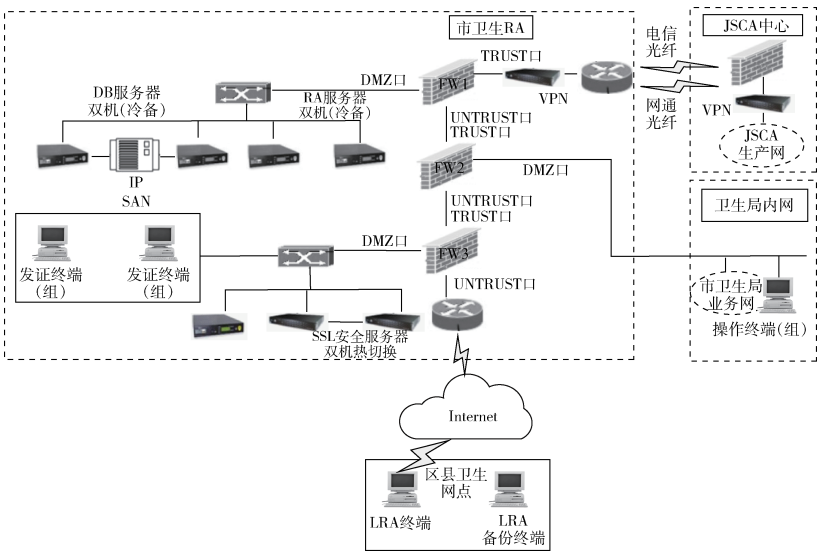

图2 电子病历 CA 认证应用结构

4.3 电子签名工作流程

4.3.1 证书申请 使用电子病历的医护人员必须申请与其身份相对应、由 CA 中心签发的数字证书。数字证书常称为密匙，其以介质（USB 接口密匙）的方式存在[7]。是网络用户身份证，主要包含身份信息和本人的两个私钥，即加密和签名私钥。用于系统网络中各类用户身份信息核实与确认，实现数字加密以及签名授权等。

4.3.2 身份认证 医务人员在使用医院电子病历系统时必须插入密钥，同时通过 EMR 登录界面输入密匙 PIN 码，系统调用安全中间件接口，读取证书资料并验证 PIN 码的正确性，再由安全平台的证书查询验证服务系统来完成对数字证书合法性的验证[8]，用户身份认证后可进入系统。数字证书身份认证过程，见图 3。

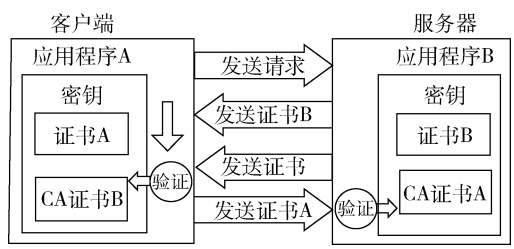

图3 数字证书身份认证过程

4.3.3 数字签名 在对电子病历进行记录、修改和保存时必须进行用户数字签名以及身份验证，以此保证电子病历的安全可靠性以及法律效力。具体包括以下几类情况。（1）医师在 EMR 系统中记录病历时的电子签名。医师完成病历记录时系统调用数字签名模块，以私匙的形式进行数字签署，同时加盖时间戳来确保时间准确性，产生的签名及时间数据保存到电子病历中，而保存后的数字签名数据将不可修改，形成可靠的病历资料。（2）采集医疗仪器数据生成电子病历签名。患者在使用医疗设备进行监护检查时会产生大量医疗数据，如影像、生化检验信息等，医护人员当场通过信息系统来确认，确认后的数据信息保存为电子病历的一部分，最后通过该医护操作人员数字证书以及私钥进行签名确认，具体过程与病历书写及修改时数字签名过程基本一致。（3）调用和查询 EMR 中的数字验签。存储于数据库中的 EMR 信息被调阅查询时，为保障 EMR 系统内病历数据的完整、准确性，系统需要验签病历信息数据。（4）对已完成的 EMR 进行修改。医师在对已完成的电子病历进行再次修改时系统会对每次修改进行数据记录，每次会产生一条修改记录，需要医师进行数字验签后才得以保存，以便为不良事件发生提供病历的质量追溯及法律依据。

4.3.4 验签服务 验证保存于 EMR 中签名数据的真实性，由明文电子病历信息验签和盖戳时间明文验证[9]。在完成对 EMR 数据信息读取后，通过数字验签中间件在医生的数字身份证对公匙进行签名后进而验签 EMR 病历信息内容，此时会生成验签数据，当签名数据与验签数据相对应时可调用 EMR 中患者信息。验证保存于数据库 EMR 的正确性，也包括明文电子病历信息验签和盖戳时间明文的验证，过程同上。时间戳验证时，可信时间戳由我国唯一专业、权威第 3 方时间戳服务机构颁发，不能被篡改和伪造。只有盖戳数据与验证数据相同（所调用和查询的电子病历时间正确）才能证明系统所调用和查询电子病历信息是正确、可靠的，保证 EMR 的不可抵赖性。对于系统登录、查询、录入、修改、删除等都有可信的操作记录日志[10]。

5 结语

大坪医院通过电子签名的实施与应用建立统一的安全认证机制，医生可以检索医师电子签名来核对病历书写时间，进而对三级查房等情况进行自动质量管控。病房护士无需再审核转抄手工签字，核对条码，由责任护士立即执行，临床医嘱执行时数字扫描查对后可实现在设备上生成电子签名。医师电子签名并非只是简单地将纸质病历手写签名转变为 CA 认证数字签名，而是从提高医院管理水平与医护诊治工作效率入手，有助于实现医院医疗管理模式中流程的优化、安全保障。大坪医院实现病历文件、医疗文书、检验单据等医疗文件的无纸化管理，为医院电子病历封存过程提供支持。

参考文献

1 瞿佳. 数字证书技术应用研究［J］. 信息系统工程，2018，26（6）：46－47.

2 李迎新，陈能太. 电子签名在医院电子病历中的实施［J］. 中国医学装备，2018，15（4）：94－97.

3 刘军，韩冬，黄家忠. 天津市疾病预防控制信息系统数字认证的实现［J］. 医疗卫生装备，2018，39（2）：56－59.

4 朱长东. 基于 CA 签章的可信电子病案无纸化建设［J］. 电子技术与软件工程，2018，129（4）：189－190.

5 毕宇. 于区块链智能合约的 PKI－CA 体系设计［J］. 金融科技时代，2018，26（7）：44－46.

6 王文明. 医院电子签名应用需求分析及解决思路［J］. 中国数字医学，2017，12（12）：67－69.

7 王颖，徐宝元，李亚丽，等. 护理病历数字认证技术的设计与实现［J］. 中国数字医学，2017，12（6）：27－29.

8 郭萍，傅德胜，朱节中，等. 轻量级可移交 CA 的 MANET 网络认证体系［J］. 计算机科学，2017，44（3）：145－149.

9 杨齐成，王锦，胡北辰. 数字证书在网络安全中的应用分析［J］. 江汉大学学报：自然科学版，2017，45（3）：278－282.

10 胡向禹，张洪亮. 中国疾病预防控制信息系统云认证服务模式的建设与应用［J］. 信息安全研究，2017，3（6）：554－559.