

云密钥及移动签署管理系统在输血信息管理系统中的应用与思考*

钟丽娜¹, 郑新波², 莫建坤^{1△}, 罗志恒¹, 陈波¹, 易哲², 黄龙², 朱伟杰¹, 冯剑锋¹, 罗焕泉¹

1. 广东省第二人民医院输血科, 广东广州 510310; 2. 广东迈科医学

科技股份有限公司, 广东广州 510320

摘要:目的 实现云密钥及移动签署管理系统在用血安全数字化、无纸化管理中的应用。方法 云密钥及移动签署管理系统与用血安全数字化、无纸化管理系统(以下简称用血安全信息管理系统)对接,建立云密钥用户认证与数字签名,使用个人身份识别码+设备绑定的模式,完成设备绑定实现扫码签名,即可在用血安全信息管理系统上用云密钥管理系统对输血相容性实验报告、发血单据等进行数字签名,同时将发血单据发送到移动签署管理系统,临床取血医护人员在平板电脑上用手写笔对发血单据进行签名确认,实现发血单据签署流程的无纸化。结果 输血科操作人员在应用用血安全信息管理系统时,通过登录云密钥管理系统实现输血相容性实验报告、发血报告合法的电子签名。使用平板电脑上的移动签署管理系统,实现医护人员取血电子签名合法化、规范化问题。结论 通过云密钥及移动签署管理系统在用血安全管理系统中的应用,有效解决了电子签名的真实性与唯一性,为确保用血安全全程质量控制信息化、数字化、无纸化管理电子签名提供了一种有效、安全、合法的方式。

关键词:云密钥管理系统; 移动签署管理系统; 输血信息管理系统; 电子签名; 认证

DOI:10.3969/j.issn.1673-4130.2021.23.025

中图法分类号:R197.32

文章编号:1673-4130(2021)23-2935-04

文献标志码:B

随着近几年移动互联网的发展,结合智能手机、5G 网络的普及,移动技术在医院输血信息管理系统中的应用越来越广泛。在网络型用血安全数字化、无纸化管理系统的建立及应用过程中发现,输血科(血库)一个人值班时,需要在不同的实验室对输血信息管理系统进行操作,使用硬件型的优盾进行数字签名认证时,则需要不同的操作电脑间对优盾进行频繁拔插,实属不便;再者如何将临床取血人的证书签名机关(CA)签名信息嵌入到输血科(血库)输血信息管理系统的发血单据上也是需要考虑的关键问题^[1-3]。本文依据《临床输血技术规范》《医疗机构临床用血管理办法》《卫生系统电子认证服务管理办法(试行)》及相关标准规范要求,采用双轨制,即按照《临床输血技术规范》要求完成用血安全工作的同时,拟在广东省第二人民医院输血信息管理系统上开展使用云密钥管理系统,并且使用移动签署管理系统在平板电脑上实现电子签章数字认证,确保输血信息管理系统运行的用血安全数字化、无纸化、数据和档案真实可信且合法有效^[4-5]。

1 材料与方法

1.1 云密钥管理系统

1.1.1 总体技术方案 根据《电子签名法》相关要求,以及中华人民共和国国家卫生健康委员会关于医疗卫生系统的相关政策要求和技术要求,搭建符合法律法规要求的电子认证服务体系,体系分为两大部分:数字证书服务体系和安全应用支撑体系,其中数字证书服务体系负责审核医护人员的真实身份,同时为其签发数字证书;安全应用支撑体系负责将数字证书认证和医疗卫生系统进行集成,形成完整、可靠、符合法律、符合政策规范的卫生系统电子认证。

云密钥管理系统使用非实物介质证书,避免出现证书的携带及保管问题,支持基于手机的强身份认证,认证方式采用数字证书,移动终端支持直接调用云端密钥,实现移动终端的可靠身份认证和电子签名;支持对应用数据或文件提供数字签名操作,支持业务端、用户端、云认证签名服务系统协同完成,并且需要用户确认;采用密钥管理云服务,支持密钥由移动终端和云认证服务协商产生。提供密钥生成、存储、销毁的云服务。云密钥管理系统整体架构见图 1。

1.1.2 云密钥用户认证与数据签名 医院云密钥使用个人身份识别码(PIN)+设备绑定的模式,医院管理部门提交医护人员资料(工号、姓名、身份证、手机

* 基金项目:2020 年度广东省档案局科研项目计划(YDK-260-2020)。

△ 通信作者, E-mail: mojiankun88@126.com。

本文引用格式:钟丽娜,郑新波,莫建坤,等.云密钥及移动签署管理系统在输血信息管理系统中的应用与思考[J].国际检验医学杂志,2021,42(23):2935-2938.

号码等)和纸质申请备案,供监管部门审查,CA 后台批量审核签发数字证书,短信发送初始密码;医护人员安装云密钥 APP,初次登录输入工号和初始密码,通过短信验证码绑定到备案的手机号码,完成设备绑定,绑定后可实现扫码签名。

输血科工作人员登录医院输血信息管理系统,输血信息管理系统通过密钥安全管理系统调用身份认

证模块进行身份校验,返回身份校验数据,中间件根据校验数据生成登录专用二维码;用户打开移动终端 APP,扫描二维码,第 1 次签名或登录时需要输入 PIN,提交签名给云密钥管理系统身份认证模块进行校验,校验完成后对提交医疗数据进行电子签名并加盖时间戳。

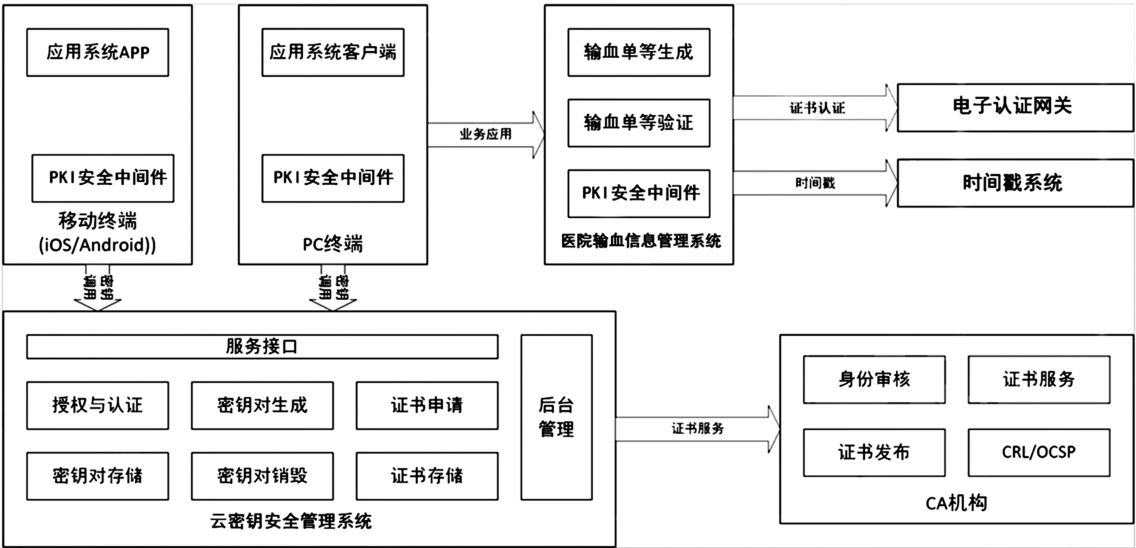


图 1 云密钥管理系统整体架构

1.1.3 数字签名与验证的关键步骤 见图 2。(1)首先检查操作人员是否登录输血信息管理系统。(2)如果已经登录输血信息管理系统,则检查是否过了登录有效期,登录有效期可以由输血信息管理系统来设置。如果过了有效期则提示重新登录流程,没有过有效期则执行图 2 第 1、2、3 步骤。(3)操作人员完成数字签名操作。

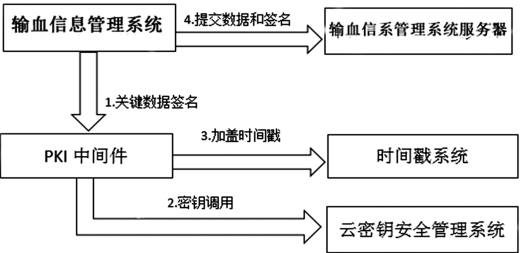


图 2 输血信息管理系统数字签名与验证的步骤

1.1.4 云密钥安全管理与密钥生成过程^[6-8] (1)云密钥管理系统产生随机 PIN。(2)使用国产 SM3 算法计算上一步产生的随机 PIN 的散列函数值。(3)使用国产 KDF 算法,利用上一步计算得到的 HASH 值作为输入,导出一个对称密钥 k。(4)云密钥管理系统调用专用密码设备产生签名密钥密文 cd1(专用密码设备使用内置密钥对签名密钥加密后的结果)。(5)云密钥管理系统使用(3)中产生的对称密钥 k,使用国

产 SM4 对称加密算法,再对上一步产生的签名密钥密文进行加密,得到双重加密的签名密钥密文 cd2。(6)云密钥管理系统销毁(3)中产生的对称密钥。(7)云密钥管理系统存储签名密钥对双重加密后的密文 cd2。

1.1.5 密钥计算过程 (1)云密钥管理系统使用国产 KDF 算法,利用用户输入的 PIN 的 HASH 值作为输入,导出一个对称密钥 k1。(2)使用上一步导出的对称密钥 k1 解密双重加密后的签名密钥密文 cd2。(3)如果用户输入的 PIN 正确,则解密后能得到 cd1,否则,解密失败。(4)云密钥管理系统调用专用密码设备提供的接口,将 cd1 和待签名的数据输入到专用密码设备中,得到正确的计算结果,即签名结果。

1.2 移动签署管理系统

1.2.1 移动签署管理系统网络拓扑 移动签署管理系统网络拓扑见图 3。

1.2.2 移动签署管理系统在输血信息管理系统上的应用 输血信息管理系统与移动签署管理系统进行对接,输血科操作人员在输血信息管理系统上用云密钥管理系统对发血单据进行数字签名,然后将该单据发送到移动签署管理系统,临床取血医护人员在平板电脑上用手写笔对发血单据进行签名确认,实现了发血单据签署流程的无纸化。

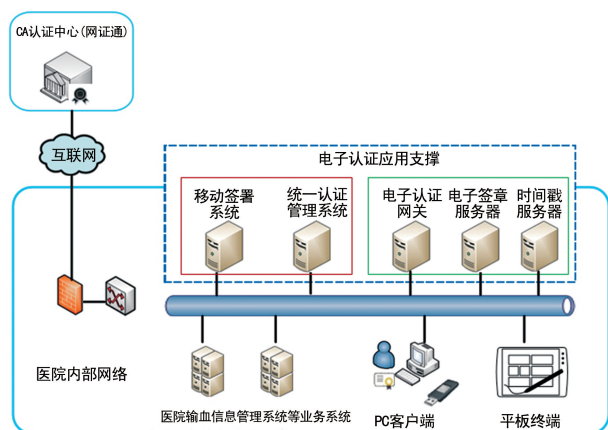


图 3 移动签署管理系统网络拓扑

2 结 果

2.1 在操作输血信息管理系统电脑终端时,插入 CA 输血信息管理系统可全程实时记录操作员动作,可确保输血信息管理系统中输血相容性各种实验报告、电子数据、档案等的安全性和合法性。

2.2 在应用输血信息管理系统时,登录云密钥管理系统实现实时电子签名,解决了输血科工作人员操作输血信息管理系统时需要携带硬件电子签章的不便、在网络型输血信息管理系统不同终端电脑操作时需要反复拔插 CA 的问题,提高了电子签名的方便性、可操作性、安全性和合法性。

2.3 通过使用 CA 签名平板,实现医务人员取血签名合法化、规范化问题。广东省第二人民医院对用血安全输血相容性相关电子报告、档案实现了规范化、标准化管理,工作流程得到了充分优化,减少了用血安全中信息数据实验报告和档案的各种缺项。

3 讨 论

随着科学技术,特别是信息化技术的发展,输血信息化、无纸化管理是用血安全管理的重要课题和必然发展趋势。根据现行《临床输血技术规范》要求,本科室尝试建立临床用血安全资料、档案纸质与数字化、无纸化“双轨制”保存管理方法:按照传统方法手工签署和保存输血相容性相关资料和实验报告,同时根据中国合格评定国家认可委员会 ISO15189:2012、纸质档案数字化规范(DA/T31-2017)、电子文档归档与电子档案管理规范、中华人民共和国档案法、无纸化病案的实施与改进的说明^[9-12],开展在输血信息管理系统建立云密钥和 CA 签名平板电子认证^[13]。

输血科工作人员操作输血信息管理系统时,插入工作人员的 CA 签名操作输血信息管理系统,输血信息管理系统可实时记录操作人员各种动作,可确保输血信息管理系统中的电子数据、档案的安全性和合法性,但是在网络型输血信息管理系统不同电脑终端操作时必须拔插操作人员的 CA 签名到正在操作的

电脑终端上,这样才能确保操作人员操作实时有效。在登录输血信息管理系统时登录云密钥管理系统,这样就可以解决输血科操作人员在网络型输血信息管理系统不同电脑终端操作电子签名问题,不存在需要操作人员再登录问题,一次登录云密钥管理系统就可全程实时监控、实现操作人员的电子签名真实可靠,并且具有法律效力。

临床取血医护人员在输血科发血单据上必须签名是临床输血技术规范要求的。本科室曾考虑临床发血时直接使用取血人员个人的 CA 签名解决取血者的电子签名合法性问题,但综合考虑后使用 CA 移动签署管理系统并将之嵌合到输血信息管理系统中更为科学合理,它可以很好地解决不同取血人员需要携带 CA 签名、忘记携带或故障等原因影响电子签名问题。使用 CA 移动签署平板电子认证,使用优盾在输血信息管理系统中进行电子签名操作,解决了取血者在输血信息管理系统上的电子签名合法性问题。

将云密钥、移动签署管理系统嵌合到输血信息管理系统上,输血科工作人员登录输血信息管理系统时插入操作人员的 CA 签名或登录云密钥管理系统,当输血科发血时请临床取血者在移动签署平板上进行电子签名,实现了在用血安全全程电子化、无纸化办公的同时,又保证了电子数据的安全性和合法性;在提高医护人员工作效率及电子数据安全保护的同时,又减少了因优盾忘记携带或故障等原因影响医疗业务正常进行的需求,同时在登陆系统的时候,增加如微信扫码、指纹识别等身份验证方式,提高了安全级别。

通过云密钥及移动签署管理系统在输血信息管理系统中的应用,有效解决了电子签名的真实性与唯一性,为电子签名提供了一种有效、安全、合法的方式。

参考文献

- [1] 莫建坤,郑新波,任勇,等.网络型医院输血管理系统的建立及应用[J].检验医学与临床,2013,10(17):2345-2346.
- [2] 钟丽娜,郑新波,杨俏兰,等. Techno TwinStation 型、iH-1000 型全自动配血分析仪在使用 ISBT-128 编码时出现的问题及对策[J].现代医院,2020,20(3):341-343.
- [3] 罗志恒.云密钥系统在门诊电子病历的应用[J].科技创新导报,2020,33(1):151-152.
- [4] 杨翰坤.全面改进数字化病案管理的实践探讨[J].现代医院,2018,18(4):521-525.
- [5] 夏祺霖.可靠电子签名技术在医院中的设计与应用[J].医学信息,2018,31(18):9-10.
- [6] 朱鹏飞,张利琴,李伟,等.基于国密算法体系的交互型电子签名[J].网络空间安全,2018,9(1):41-45.

[7] 严新成,陈越,巴阳,等.云环境下支持更新加密的分布式数据编码存储方案[J].计算机研究与发展,2019,56(10):2170-2182.

[8] 梁爽.云计算中跨域安全认证的关键技术研究[J].计算机测量与控制,2019,27(8):276-280.

[9] 程天慈.无纸化病历存储的现状与问题[J].北京医学,2020,42(1):75-76.

[10] 石斌,刘春玲.无纸化病案的实施与改进[J].中国病案,2019,20(11):1-2.

[11] 雷明德,黄学忠,郑晓聪.基于 LIS 平台提升科室设备档案管理能力[J].国际检验医学杂志,2013,34(23):3262.

[12] 康从越,王凌雪,马琳娜,等.电子病历推动临床输血科信息管理系统建设[J].中国药物经济学,2014,9(1):173-175.

[13] 彭红.云计算中密钥管理关键技术研究[J].软件,2019,40(9):212-215.

(收稿日期:2021-03-12 修回日期:2021-07-17)

管理·教学

以临床思维为导向的检验医师规范化培训模式探讨^{*}

范 超,鲁卫平[△],黄 庆,邓少丽,黎 敏,余春利
陆军特色医学中心检验科,重庆 400042

摘 要:传统的检验医师规范化培训多将培养重点集中在专业理论知识、检验技术能力及检测结果准确性的把控等方面,如何真正让临床医生和护士融入检验流程,如何科学解读检验结果并指导临床将其合理应用到实际诊疗工作中亟待提高。该文探索以专业技能培训为基础,以临床思维为导向,结合临床查房、病例讨论、教学查房、临床交流等教学模式,为培养能真正发挥检验与临床“桥梁作用”的检验医师提供一些参考,并着力于更深层次地探索检验医师规范化培训模式。

关键词:检验医师; 规范化培训; 临床思维

DOI:10.3969/j.issn.1673-4130.2021.23.026

文章编号:1673-4130(2021)23-2938-03

中图法分类号:R372;G643

文献标志码:B

现代临床医学已进入精准诊疗时代,检验医学在其中的地位和作用日渐凸显,检验科为临床疾病的快速诊治发挥着越来越关键的作用^[1-2]。因此,如何指导临床规范选择检测项目、获取合格的检测标本、科学解读和合理使用检验报告显得至关重要,而且是检验医师必须具备的能力。在检验医学专业住院医师规范化培训工作中,本科室以检验医学相关知识和技能为基础,着重培养学员对检验结果的分析和解释的能力,以及与临床的沟通、咨询和指导的能力,使其成为既具备临床检验技能,又能参与临床诊治工作的检验医师。为实现这一目标,本科室作为重庆市首批检验医学专业住院医师规范化培训基地,在实践中不断探索各种教学及培养模式,并持续改进和完善培训体系,力求打造出一条更具价值和特色的规范化培训之路。

1 依据培训大纲细化培训内容

依据检验医学住院医师规范化培训大纲要求,同时参考《检验医学住院医师规范化培训与考核》^[3]相关内容,并结合本基地的实际,各专业组制订了具备

各自特点的培训内容和细则,培训内容覆盖检验前、检验中、检验后全过程,培训计划细化到每周。除了掌握检验基本理论知识和检测技术外,还特别融入了对学员发现问题、分析问题、解决问题等综合能力及辩证思维能力的培训,从而使培训内容更具完整性,教员的讲授更具明确性,学员的学习更具目的性,培训计划的实施更具可操作性和新颖性。

2 加强师资队伍建设,确保教学质量

按照国家临床医师规范化培训的相关要求及基地的实际情况,本科室从已经获得医院教员资格认证的工作人员中遴选出具有丰富临床经验和扎实专业技能的教员组成一支强有力的师资队伍。要求每名教员掌握检验医师培训的总体目标,实现“目标教学”,掌握培训内容细则和实施方案,做到“按纲施训”,在培训过程中做到“因材施教”,定期总结培训中的问题并反馈给学员,做到“持续改进”,注重学员综合能力的培养,促进学员“全面发展”,争做“双一流”教师团队。

^{*} 基金项目:2018 年度大学教育研究立项课题(2018 B13);2019 年重庆市研究生教育教学改革研究项目(yjg193132)。

[△] 通信作者,E-mail:ronnylu@126.com。

本文引用格式:范超,鲁卫平,黄庆,等.以临床思维为导向的检验医师规范化培训模式探讨[J].国际检验医学杂志,2021,42(23):2938-2939.