看到其无形的社会效益。当价格与价值趋于协调时,便会正向激励护理事业健康积极发展。

4.3 加强成本过程管理　满足患者日益增长的护理要求人力成本,合理配置,积极培训,提高素质,物资成本做到物尽其用,杜绝浪费。关注患者住院费用管理,进行实时监控,每天核对,及时通报,三级联查,办公室护士自查、住院处收费处审查、患者确认清单。

4.4 重视人力成本价值　关注人力成本价值有助于护理成本的合理设置和体现,护理人力成本就是指在实施专项护理服务过程中所消耗的人力资源价值,专项护理服务价值的体现,需要进一步重视护理人力在从事专项护理方面的技术含量和劳动价值。从护理经济学的角度出发,价格是价值的货币表现,在制订合理收费标准时,要考虑体现出专项护理服务的价值。

因此,护理服务项目价格管理,既需要医院护理管理者的高度重视,也需要引起医疗行政主管部门、医院的高度关注,加强对护理服务价格项目的研究和管理。

参考文献

[1] Florin J, Ehnfors M, Ostlinder G. Developing a national integrated classification of health care interventions in Sweden[J]. Int J Med Inform, 2005, 74(11-12): 973-979.

[2] Frantz E. Management of the acute Coronary Syndrome under German Diagnosis Related Groups in 2005/2006 [J]. Herz, 2005, 30(8): 710-714.

[3] Borsa J, Anis A. The cost of hospital care in Canada: a comparison of two alternatives[J]. Health Manage Forum, 2005, 18(1): 19-27.

[4] 王燕. 护理成本效益对护理事业发展的影响[J]. 中国实用护理杂志, 2007, 23(7): 65-66.

[5] 王霞, 王建萍, 王小华. 护理成本核算与护理价格的调查[J]. 中华现代护理杂志, 2008, 14(15): 1711-1712.

[6] 刘则杨. 护理经济学概论[M]. 北京: 中国科学技术出版社, 2002: 3-5.

(收稿日期:2013-06-20　修回日期:2013-08-12)

医院 CA 认证系统的安全性分析

张立群,熊　剑,陈亚婕(湖北医药学院附属太和医院信息资源部,湖北十堰　442000)

【关键词】 CA 认证系统;　身份认证;　电子签名;　安全性

DOI:10.3969/j.issn.1672-9455.2013.23.087　**文献标志码:**C　**文章编号:**1672-9455(2013)23-3243-02

随着我国医疗体制的逐步改革,积极发展区域医疗卫生信息平台是当前医疗管理的趋势。而电子病历系统作为区域性医疗卫生共享信息的重要内容,其必然得到对应的完善和标准化。而电子病历信息的公信力与安全性是构建在数字证书技术的 CA 认证基础之上的。

随着 CA 认证技术的不断发展与成熟,其给数字证书的正常使用提供了技术性基础。卫生部于 2011 年 1 月 1 日颁布并实施了《电子病历系统功能规范(试行)》,其中第二章第六条就明确规定:电子病历系统在管理和使用过程中应该进行用户授权与认证,同时结合审计、数据存储、隐私保护以及数据管理等方式,确保电子病历数据的安全、可靠。因此,医院在区域医疗信息管理过程中应该更加重视网络情况下 CA 认证系统的信息安全问题。

1　CA 认证系统架构过程中的相关技术

1.1 CA 认证身份识别　CA 认证系统信息安全分析过程中需要解决的重要问题就是身份认证及信息保密问题。首先,什么是 CA 身份认证? 作为电子病历信息系统安全管理的核心内容,针对医生与患者电子身份的确认,当前主要采用基于数字证书的 CA 认证系统。CA 认证系统实施过程中,由公钥基础设施(PKI)系统中通信双方都信任的实体进行数字证书发放、删除与管理。该实体应该是一个具有政府授权的组织或者是政府机构,保证其具有对应的公信力和权威性。所以,数字证书是一种网络实体身份证,是进行信息发布与获取过程中的身份认证依据。在系统登录过程中,应该保证系统具有双向认证机制,若没有数字证书就不允许其登录系统,更不允许其非法进入系统进行诊断、开具处方、治疗等活动。另外,数字证书还应该确保所发布的共享病历信息只有发送对象及发送者才能读取,非法窃取信息者不能对信息进行解码。因此,CA 数字认证系统在构建过程中还应该将信息内容加密作为系统构建的基础。例如,可以采用公钥、私钥等进行加密,实现身份认证。

1.2 电子签章　作为电子签名的一种重要形式,电子签章广泛存在于电子身份认证系统应用中,其通过与电子文件信息建立起对应逻辑关联的方式,对电子文件的签署者进行身份辨识、保证文件的完整性、确保文件的合法性[1]。

电子签章在实现过程中采用报文摘要算法、非对称加密算法等方式。利用电子签章的方式进行电子病历及其他信息传递,使需要发布的电子信息文件与电子签章融合在一起,非 CA 系统授权人将无权进行文件操作,保证了信息系统的安全可靠,避免了电子签章丢失。

随着网络技术的日趋成熟,在医院信息网络的构建过程中,应该构建一个可信的电子病历认证中心存放所有信息授权人的相关电子证书,同时将信息系统所产生的所有资料进行保存、归档,便于事后取证及查询。

2　CA 认证系统实施过程中存在的安全漏洞

就医院电子信息的产生过程而言,电子病历信息主要是由医院各科室在患者就医过程中录入的医疗过程信息,然后通过医院局域网络传输到服务器中进行存储。在整个传输过程中,每个环节的实时动态性都要求很高。在信息传输过程中存在的安全漏洞主要包括以下几个方面[2]。

2.1 身份验证漏洞　CA 系统身份认证的最终目的是要解决是否有人利用他人的用户名及口令进行病历信息的修改与登

入,是否存在越过 CA 系统的身份验证程序进行病历信息的修改与登入等。当前,大部分医院的 CA 认证系统身份验证方法都较为简单,进入 CA 系统只需要简单的用户名及密码即可。加之用户名与密码在服务器中以明文记录,或者是只进行简单加密之后就存储起来,容易被其他人获得并修改。

2.2 信息网络传输过程中的安全问题 医院的 CA 认证系统运行在医院的局域网中,外网难以给医院局域网造成影响。正是这种现状导致整个局域网上 CA 认证服务终端节点与后台服务器之间的信息传输安全经常被忽视,不能保证医务人员在 CA 终端上进行相关信息操作的正确性。

2.3 数据存储安全漏洞 医院的电子病历信息一般是采用明文方式存在后台服务器中,而后台服务器对于相关人员(例如管理人员等)则是透明的。而对于数据库内容是否被人浏览或者是修改过,当前的 CA 认证系统还没有一个很好的解决方案。因此,这不能完全确保所登入及修改电子病历信息者完全是拥有合法身份的医疗人员所为。

2.4 电子病历信息的实时性漏洞 医院对电子病历信息的实时性要求较高,针对患者在就诊过程中的各个环节,医护人员不但要对各项诊疗信息进行记录,同时还应该对诊疗时间进行记载。而当前 CA 认证系统所记录的时间是系统时间,并不是国家授权时间,在对时间的查询及管理上存在一定障碍。

3 基于医院 CA 认证系统安全性的 CA 认证方案架构

3.1 医院信息系统 CA 认证方案特点 医院信息系统中使用 CA 认证系统所存储的信息以各种形式保存在数据库中,同时具有其自身的特点:医院各个子系统所产生的信息格式较多,包括文本、图片、影像等文件;关联性强,由于需要认证的信息数据都采用代码方式进行记录和保存,例如患者的处方单存放于处方明细表中,而这个表的信息只有与药品表、科室表、患者信息表等相关联之后才能形成一个完整的合法处方表;系统多,1 份完整的病历信息资料需要通过不同时段的不同医、护、医技等人员进行处理,而处理过程必然需要有对应的签名,系统因此会产生繁杂的信息。

3.2 医院 CA 系统认证功能基本范围 医院 CA 系统认证功能基本范围应该包括这样几个方面:医生签名,医生开具、分解、删除病历的所有记录,诸如患者的入院记录、病程记录、手术记录、出院小结等过程中产生的相关文档;护士签名、三测记录单、医嘱执行记录、护理记录以及护理医嘱记录等;医技人员签名,检查申请单,各种检验报告、影像报告等;药师签名,处方配发药记录等。

3.3 CA 认证系统的存储架构

3.3.1 混合式存储方案架构 在 CA 系统认证过程中,通过直接对医院已有的信息数据表进行修改,将对应的签名数据与被签名记录并存储到对应的数据表格当中。但是,在实施过程中,由于系统问题或其他因素,导致其需要直接打开对应的数据库对保存的数据进行直接操作,这将造成其与 CA 认证数据的不一致[3]。如上文所述,为了保证 CA 认证系统具有较强的实时性,通常需要进行大量签名,而签名之后的数据记录量将迅速增加。这时,医院网络系统负载的增加将会使系统运行缓慢,给非法入侵者提供了可乘之机。因此,为了避免混合式存储方案给医院局域网系统流量增加,降低系统运行效率,增加系统的维护难度等问题出现,一般不采用混合式存储方案进行 CA 系统的架构。

3.3.2 独立式存储方案架构 基于对混合式存储方案架构缺陷的认识,通过单独建立 CA 认证服务系统,将 CA 认证系统实施过程中产生的明文记录及数字签名数据保存在该独立服务器中[1]。其具体架构由服务接口、Web 服务器、签名数据库、签名验证审计等部分组成,医院电子病历系统调用和保存数字签名均通过服务实现,由独立的服务器处理。若为调用,则服务接口通过公钥和私钥分别取得当前使用者及签名数据库中的签名摘要,用签名验证审计来证明使用者身份;若为存储,则由服务接口判断是否需要时间戳,如果需要则通过外网访问 CA 中心获得时间戳,加盖时间戳签名再进行存储,否则存储的为普通数字签名。

在该架构体系中,由可信赖的 CA 中心给医院电子病历系统中各用户进行数字证书签发。由于在该病历系统中集成了 CA 中心所提供的 PKI 端口,实现了基于数字证书的身份验证,彻底代替了传统用户名加密码的身份认证方式[4]。同时,该认证系统还采用了基于数字证书的身份验证方式,通过对不同权限操作人员进行访问权限控制,使不同权限的操作人员只能够对其权限范围内的信息资源进行访问,保证了信息的过度扩散。另外,该身份认证系统通过调用 CA 中心里对应的电子签名信息及端口验证程序,能够实现基于数字证书及电子签章的信息管理体系,保证了信息的完整性、真实性及可靠性。最后,在数字签名的保存及时间戳的调用过程中,通过 1 台独立的服务器进行处理,避免了信息扩散。在数字签名及对应签名文档进行明文存储之后,使用 XML 文档将之保存到 XML 数据库中,而且通过构建签名数据与 CA 身份认证系统的图像关联来对电子信息中的图像进行关联处理,保证了信息的连锁安全性。

4 结 语

随着计算机网络技术的不断发展,信息技术在医院管理中的应用必然逐步加深。如何在利用信息管理技术优势的同时,避免由于信息系统的构建造成的信息泄露问题成为了当前信息系统构建的热门话题。基于此,医院应该重视 CA 身份认证系统的构建,同时应结合医院自身的具体特征选取合理的认证系统架构方案。

参考文献

[1] 肖辉,商建国,陈敏. 医院信息系统 CA 认证方案探讨[J]. 中国数字医学,2012,7(1):105-107.

[2] 廖淑华,许垂泽. CA 认证在电子病历信息安全的应用探索[J]. 医学信息,2005,18(11):1420-1424.

[3] 曾国宇,林阳,廖邦富,等. 数字认证在区域信息安全的应用探索[J]. 中国数字医学,2012,7(1):114-115.

[4] 孙瑜. 数字证书与电子病案的安全[J]. 信息安全与技术,2011,10(4):44-45.

(收稿日期:2013-05-21 修回日期:2013-07-12)