（三）具有符合《卫生系统电子认证服务规范》、《卫生系统数字证书格式规范》、《卫生系统数字证书介质技术规范》、《卫生系统数字证书应用集成规范》和《卫生系统数字证书服务管理平台接入规范》等的电子认证服务体系；

（四）符合法律、行政法规规定的其他条件。

第七条　卫生部信息化工作领导小组办公室负责选择卫生部及其直属单位的电子认证服务机构。各省级卫生行政部门信息化工作领导小组办公室负责选择本辖区的电子认证服务机构。

第八条　各省级卫生行政部门信息化工作领导小组办公室选定电子认证服务机构后，应当将服务机构名单及其相关材料向卫生部信息化工作领导小组办公室上报，并要求电子认证服务机构在开展服务前接入卫生部数字证书服务管理平台。

第九条　鼓励各地卫生系统数字证书应用单位优先选择已接入卫生部数字证书服务管理平台的电子认证服务机构提供服务。

第十条　卫生部信息化工作领导小组办公室与各省级卫生行政部门信息化工作领导小组办公室共同对各电子认证服务机构的服务质量及开展情况进行定期检查。

第十一条　卫生部信息化工作领导小组办公室通过数字证书服务管理平台收集、汇总电子认证服务机构面向卫生系统证书发放和服务质量反馈等信息，综合掌握全国卫生系统电子认证服务的整体应用情况。

第三章　电子认证服务机构的服务要求

第十二条　电子认证服务机构应当按照《卫生系统电子认证服务规范》的要求，建立全面、规范、安全、高效的运行服务体系，并至少提供以下服务：

（一）数字证书的颁发、更新、吊销、密码解锁、密钥恢复等服务；

（二）数字证书及黑名单的查询与下载服务；

（三）为数字证书用户提供应用支持服务；

（四）提供数字证书相关的培训服务。

第十三条　电子认证服务机构应当妥善保存数字证书业务申请材料，并承担保密责任，不得泄露或遗失，信息保存期至少为证书到期后 5 年。

第十四条　电子认证服务机构应当建立信息安全保障机制，针对相关资产、人员、物理环境和软件系统等制定安全策略及管理制度，采取有效的安全保障措施，并对安全策略的执行情况进行有效的监督检查，确保运行服务安全可靠，满足卫生信息系统业务连续性要求。

第四章　数字证书的应用管理

第十五条　凡涉及国家安全、社会稳定、公众利益等方面的各类重要卫生信息系统，应当按照国家法律法规、信息安全等级保护制度等要求，采用电子认证服务，解决身份认证、授权管理、责任认定等安全问题，主要包括：

（一）涉及公共卫生业务的信息系统；

（二）涉及医疗保健的医疗卫生信息系统；

（三）网上申报、年检、备案、资质认定等行政审批信息系统；

（四）各类网上招标采购信息系统；

（五）其他重要卫生信息系统。

第十六条 使用电子认证服务的各类卫生信息系统，应当遵循《卫生系统数字证书应用集成规范》进行建设，实现数字证书的各项安全功能。

第十七条 纳入卫生系统电子认证服务体系的电子认证服务机构，其颁发的数字证书应当能够在各类卫生信息系统中进行注册、授权及使用，确保实现互信互认、一证多用。

第十八条 数字证书使用单位应当加强证书管理，指导并要求证书持有人妥善保管数字证书介质。出现数字证书介质丢失或损坏等异常情况时，证书持有人应当立即联系电子认证服务机构进行妥善处理。

第十九条 数字证书原则上由信息系统建设单位统一采购配发并负责初次办理费用，其年服务费用由使用单位负责；对于向社会提供服务的信息系统，其费用由服务申请者支付。

第二十条 多个卫生信息系统覆盖相同用户群体时，由卫生部和各省级卫生行政部门信息化工作领导小组办公室协调各信息系统建设单位，分摊数字证书的初次办理费用。

第五章 附则

第二十一条 各省级卫生行政部门信息化工作领导小组应当按照本办法第六条要求，对本辖区已开展服务的电子认证服务机构进行评估。符合第六条各项条件的，方可接入卫生部数字证书服务管理平台并继续开展服务；不符合第六条规定条件的，应当责令其进行整改，如1年内仍达不到相关要求的，应当终止其服务。

第二十二条 已建成但尚未采用数字证书的重要卫生信息系统，应当尽快采用数字证书，实现身份认证、授权管理和责任认定；已经采用数字证书的重要卫生信息系统应当尽快按照本办法的有关要求进行系统改造，纳入卫生系统电子认证服务体系。

第二十三条 本办法由卫生部信息化工作领导小组办公室负责解释。

第二十四条 本办法自2010年1月1日起试行。

27.6 商用密码管理条例

（中华人民共和国国务院第273号令，1999年10月7日发布，自发布之日起施行）

第一章 总则

第一条 为了加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益，制定本条例。

第二条 本条例所称商用密码，是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。

第三条 商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理。

第四条 国家密码管理委员会及其办公室（以下简称国家密码管理机构）主管全国的商用密码管理工作。

省、自治区、直辖市负责密码管理的机构根据国家密码管理机构的委托，承担商用密

码的有关管理工作。

第二章　科研、生产管理

第五条　商用密码的科研任务由国家密码管理机构指定的单位承担。

商用密码指定科研单位必须具有相应的技术力量和设备，能够采用先进的编码理论和技术，编制的商用密码算法具有较高的保密强度和抗攻击能力。

第六条　商用密码的科研成果，由国家密码管理机构组织专家按照商用密码技术标准和技术规范审查、鉴定。

第七条　商用密码产品由国家密码管理机构指定的单位生产。未经指定，任何单位或者个人不得生产商用密码产品。

商用密码产品指定生产单位必须具有与生产商用密码产品相适应的技术力量以及确保商用密码产品质量的设备、生产工艺和质量保证体系。

第八条　商用密码产品指定生产单位生产的商用密码产品的品种和型号，必须经国家密码管理机构批准，并不得超过批准范围生产商用密码产品。

第九条　商用密码产品，必须经国家密码管理机构指定的产品质量检测机构检测合格。

第三章　销售管理

第十条　商用密码产品由国家密码管理机构许可的单位销售。未经许可，任何单位或者个人不得销售商用密码产品。

第十一条　销售商用密码产品，应当向国家密码管理机构提出申请，并应当具备下列条件：

（一）有熟悉商用密码产品知识和承担售后服务的人员；

（二）有完善的销售服务和安全管理规章制度；

（三）有独立的法人资格。

经审查合格的单位，由国家密码管理机构发给《商用密码产品销售许可证》。

第十二条　销售商用密码产品，必须如实登记直接使用商用密码产品的用户的名称（姓名）、地址（住址）、组织机构代码（居民身份证号码）以及每台商用密码产品的用途，并将登记情况报国家密码管理机构备案。

第十三条　进口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准。任何单位或者个人不得销售境外的密码产品。

第四章　使用管理

第十四条　任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。

第十五条　境外组织或者个人在中国境内使用密码产品或者含有密码技术的设备，必须报经国家密码管理机构批准；但是，外国驻华外交代表机构、领事机构除外。

第十六条　商用密码产品的用户不得转让其使用的商用密码产品。商用密码产品发生故障，必须由国家密码管理机构指定的单位维修。报废、销毁商用密码产品，应当向国家密码管理机构备案。

第五章 安全、保密管理

第十七条 商用密码产品的科研、生产，应当在符合安全、保密要求的环境中进行。销售、运输、保管商用密码产品，应当采取相应的安全措施。

从事商用密码产品的科研、生产和销售以及使用商用密码产品的单位和人员，必须对所接触和掌握的商用密码技术承担保密义务。

第十八条 宣传、公开展览商用密码产品，必须事先报国家密码管理机构批准。

第十九条 任何单位和个人不得非法攻击商用密码，不得利用商用密码危害国家的安全和利益、危害社会治安或者进行其他违法犯罪活动。

第六章 罚则

第二十条 有下列行为之一的，由国家密码管理机构根据不同情况分别会同工商行政管理、海关等部门没收密码产品，有违法所得的，没收违法所得；情节严重的，可以并处违法所得1至3倍的罚款：

（一）未经指定，擅自生产商用密码产品的，或者商用密码产品指定生产单位超过批准范围生产商用密码产品的；

（二）未经许可，擅自销售商用密码产品的；

（三）未经批准，擅自进口密码产品以及含有密码技术的设备、出口商用密码产品或者销售境外的密码产品的。

经许可销售商用密码产品的单位未按照规定销售商用密码产品的，由国家密码管理机构会同工商行政管理部门给予警告，责令改正。

第二十一条 有下列行为之一的，由国家密码管理机构根据不同情况分别会同公安、国家安全机关给予警告，责令立即改正：

（一）商用密码产品的科研、生产过程中违反安全、保密规定的；

（二）销售、运输、保管商用密码产品，未采取相应的安全措施的；

（三）未经批准，宣传、公开展览商用密码产品的；

（四）擅自转让商用密码产品或者不到国家密码管理机构指定的单位维修商用密码产品的。

使用自行研制的或者境外生产的密码产品，转让商用密码产品，或者不到国家密码管理机构指定的单位维修商用密码产品，情节严重的，由国家密码管理机构根据不同情况分别会同公安、国家安全机关没收其密码产品。

第二十二条 商用密码产品的科研、生产、销售单位有本条例第二十条、第二十一条第一款第（一）、（二）、（三）项所列行为，造成严重后果的，由国家密码管理机构撤销其指定科研、生产单位资格，吊销《商用密码产品销售许可证》。

第二十三条 泄露商用密码技术秘密、非法攻击商用密码或者利用商用密码从事危害国家的安全和利益的活动，情节严重，构成犯罪的，依法追究刑事责任。

有前款所列行为尚不构成犯罪的，由国家密码管理机构根据不同情况分别会同国家安全机关或者保密部门没收其使用的商用密码产品，对有危害国家安全行为的，由国家安全机关依法处以行政拘留；属于国家工作人员的，并依法给予行政处分。

第二十四条　境外组织或者个人未经批准，擅自使用密码产品或者含有密码技术的设备的，由国家密码管理机构会同公安机关给予警告，责令改正，可以并处没收密码产品或者含有密码技术的设备。

第二十五条　商用密码管理机构的工作人员滥用职权、玩忽职守、徇私舞弊，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第七章　附则

第二十六条　国家密码管理委员会可以依据本条例制定有关的管理规定。

第二十七条　本条例自发布之日起施行。

27.7　商用密码科研管理规定

（国家密码管理局公告第 4 号，2005 年 12 月 11 日公布，自 2006 年 1 月 1 日起施行）

第一条　为了加强商用密码科研管理，促进商用密码技术进步，根据《商用密码管理条例》，制定本规定。

第二条　商用密码体制、协议、算法及其技术规范的科研活动适用本规定，学术和理论研究除外。

第三条　国家密码管理局主管全国的商用密码科研管理工作。

第四条　商用密码科研由国家密码管理局指定的单位（以下称商用密码科研定点单位）承担。

第五条　国家密码管理局根据商用密码发展以及科研的需要，指定商用密码科研定点单位。

商用密码科研定点单位必须具备独立法人资格，具有从事密码科研相应的技术力量和设备，能够采用先进的编码理论和技术，编制具有较高保密强度和抗攻击能力的商用密码算法。

第六条　国家密码管理局指定商用密码科研定点单位原则上定期集中进行。

指定商用密码科研定点单位的程序如下：

（一）申请单位填写《商用密码科研定点单位申请表》，提交国家密码管理局；

（二）对申请单位提交的书面材料进行初审，提出初审意见；

（三）对通过初审的单位进行实地考察，必要时组织专家进行评估；

（四）作出指定决定并告知指定结果。

第七条　被指定为商用密码科研定点单位的，由国家密码管理局发给《商用密码科研定点单位证书》并予以公布。

《商用密码科研定点单位证书》有效期 6 年。

国家密码管理局对商用密码科研定点单位每年考核一次。考核不合格的，撤销其商用密码科研定点单位资质。

第八条　商用密码科研定点单位变更名称的，应当自变更之日起 30 日内，持变更证明文件到国家密码管理局更换《商用密码科研定点单位证书》。

商用密码科研定点单位变更住所、法定代表人的，应当自变更之日起 30 日内，持变更