国家卫生健康委统计信息中心

国卫统信函〔2023〕17号

关于印发《卫生健康行业医疗机构场景密码应用与安全性评估实施指南》《全民健康信息平台密码应用与安全性评估实施指南》的通知

各省、自治区、直辖市及新疆生产建设兵团卫生健康委统计信息中心，医疗机构及有关单位：

为贯彻落实《密码法》，促进卫生健康行业正确合规有效使用商用密码，指导、推进行业密码应用。由国家密码管理局、国家卫生健康委组织，国家卫生健康委统计信息中心牵头编制了《卫生健康行业医疗机构场景密码应用与安全性评估实施指南》《全民健康信息平台密码应用与安全性评估实施指南》，并通过了国家密码管理局评审，现印发你们，供各单位参照执行。

附件：1. 卫生健康行业医疗机构场景密码应用与安全性评估实施指南

2. 全民健康信息平台密码应用与安全性评估实施指南

国家卫生健康委统计信息中心

2023年12月29日

卫生健康行业医疗机构场景
密码应用与安全性评估实施指南

国家卫生健康委统计信息中心

2023 年 12 月

目 录

前 言

卫生健康医疗机构承担着人民生命健康安全的责任，作为民生重要领域，网络及数据安全问题不容忽视。医疗机构信息系统承载着大量医疗健康、患者隐私等敏感数据，一旦泄漏或者被窃取、篡改，可能涉及患者生命安全及社会稳定。本指南针对医疗机构场景“等保三级”及以上的核心业务信息系统的密码应用情况展开描述，围绕着门急诊、住院、检验检查、互联网诊疗四个典型业务场景，分析业务流程、安全风险及保护对象，给出了用户身份真实性和医患行为不可否认、重要数据传输安全、重要数据存储安全等方面的密码应用设计，并明确了密码应用安全性评估测评内容。

本指南适用于医疗机构开展核心业务信息系统密码应用和安全性评估实施工作，同时可为主管监管部门、第三方测评机构等组织开展医疗机构场景密码应用的安全监督、检查、评估等工作提供参考。

本指南由国家卫生健康委统计信息中心牵头，北京天坛医院、中国医科大附属第一医院、华中科技大学同济医学院附属同济医院、北京数字认证股份有限公司、中国科学院信息工程研究所等多家卫生健康行业单位和密码相关单位共同开展研究与编制。

术语和定义

下列术语和定义适用于本文件。

- 机密性 confidentiality

保证信息不被泄露给非授权实体的性质

- 数据完整性 data integrity

数据没有遭受以非授权方式所做的改变的性质

- 真实性 authenticity

一个实体是其所声称实体的这种特性，真实性适用于用户、进程、系统和信息之类的实体。

- 不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的特性。

- 加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

- 密钥 key

控制密码算法运算的关键信息或参数。

- 密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

- 身份鉴别 identity authentication

证实一个实体所声称身份的过程。

- 消息鉴别码 message authentication code

利用对称密码技术或密码杂凑技术，在秘密密钥参与下，由消息所导出的数据项。任何持有这一秘密密钥的实体，可利用消息鉴别码检查消息的完整性和始发者身份。

- 动态口令 one-time password

基于时间、事件等方式动态生成的一次性口令。

- 访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

缩略语

下列缩略语适用于本文件。

APP：应用程序（Application）

VPN：虚拟专用网络（Virtual Private Network）

PC：个人计算机 (personal computer)

CA：证书认证机构 （certificate authority）

SSL：安全套接层 secure sockets layer

IPSec：IP 层协议安全结构 (Internet Protocol Security)

SSH：安全外壳（Secure Shell）

HMAC：密钥相关的哈希运算消息认证码（Hash-based Message Authentication Code）

HIS：医院信息系统（Hospital Information System）

LIS：实验室信息管理系统（Laboratory Information Management System）

PACS：医学影像存档与通讯系统（(Picture archiving and communication systems）

EMR：计算机化的病案系统（Electronic Medical Record）

1 场景概述

1.1 背景

密码技术作为网络安全的基础性核心技术，是信息保护和网络信任体系建设的基础，是保障网络空间安全的关键技术。我国于 2020 年 1 月 1 日正式实施《中华人民共和国密码法》，其中第二十七条指出“法律、行政法规和国家有关规定要求使用密码进行保护的关键信息基础设施，其运营者应当使用密码进行保护，自行或者委托密码检测机构开展密码应用安全性评估”。国务院印发的《商用密码管理条例》（国务院令第 760 号）、公安部印发《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960 号），要求网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范，网络安全等级保护第三级（含第三级）以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

在卫生健康行业，《国家卫生计生委办公厅关于印发医院信息化建设应用技术指引（2017 年版）的通知》（国卫办规划函〔2017〕1232 号）、《卫生健康委 中医药局关于印发互联网诊疗管理办法（试行）等 3 个文件的通知》（国卫医发〔2018〕25 号）、《关于印发电子病历系统应用水平分级评价管理办法（试行）及评价标准（试行）的通知》（国卫办医函〔2018〕1079 号）等政策文件，均对业务信息系统的身份认证、电子签名等密码应用提出了明确要求；2022 年国家卫生健康委、国家中医药局、国家疾控局印发《关于印发医疗卫生机构网络安全管理办法的通知》（国卫规划发〔2022〕29 号），要求各医疗卫生机构应按照《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。同时，2021 年发布的《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）标准，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面提出了密码应用技术要求，从管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求。

国家对卫生健康行业网络安全高度重视，卫生健康行业内医疗机构承担着人民生命健康安全的责任，作为民生重要领域，网络及数据安全问题不容忽视。医疗机构信息系统承载着大量医疗健康、患者隐私等敏感数据，一旦泄漏或者被窃取、篡改，可能涉及患者生命安全及社会稳定。本指南聚焦于指导卫生健康行业中医疗机构场景核心业务信息系统开展密码应用与安全性评估实施工作，有利于提升卫生健康行业网络安全保障能力，提升安全自主可控水平，对保障和促进医院信息化建设发展、保障卫生健康事业和“健康中国”战略全面落实有积极意义。

1.2 典型场景介绍

本指南主要针对医疗机构场景符合等保三级的核心业务信息系统的密码应用情况展开描述，依据《医院信息化建设应用技术指引（2017 年版试行）》、《电子病历系统应用水平分级评价标准（试行）》、《互联网诊疗管理办法（试行）》等政策标准文件，选定医疗机构内门急诊、住院、检验检查、互联网诊疗为典型业务场景，这些业务面向医院医生、护士、技师等医院工作者及患者、患者家属等就医相关人员身份认证以及可靠电子签名的密码应用需求，同时还需对业务过程中产生的重要医疗数据进行安全保护。

门急诊业务主要面向的用户为门诊医护人员，包含门急诊处方和处置管理、门急诊检验检查申请单管理、门急诊检验检查报告管理、门急诊病历记录书写等业务场景。

住院业务主要面向的用户为病房医生、病房护士，对于病房医生包含病房医嘱处理、病房检验检查申请单管理、病房检验检查报告管理、病房病历记录书写等业务场景；对于病房护士包含病人管理与评估、医嘱执行、护理记录书写等业务场景。

检验检查业务主要面向的用户为检验检查医技护人员，检查技师包含检查申请与预约、检查记录管理、检查报告管理、检查图像管理等业务；检验技师包含标本处理管理、检验结果记录、报告生成等业务场景。

互联网诊疗业务主要面向的用户为已注册的医生，直接通过互联网提供部分常见病、慢性病复诊及患者移动终端登录认证等业务场景。

本指南针对的医疗机构核心业务系统为院内电子病历系统、互联网诊疗系统。其中，电子病历系统包含上述门急诊、住院、检验检查业务场景；互联网诊疗系统主要包含上述互联网诊疗业务场景。关键业务流程如下表 1 所示：

表 1 医疗机构业务流程梳理

序号	业务名称	业务流程描述
1	门急诊	(1) 患者挂号缴费； (2) 调出患者基本信息； (3) 问诊后，如需检验检查，开具检验检查申请单，患者缴费后，同步信息到检验检测系统； (4) 检验检测后返回检验检查报告； (5) 医生书写病历（个人基本信息、诊断信息、治疗方案信息）； (6) 推送知情同意书等文件给患者/家属终端，患者/家属签署知情同意书； (7) 开具医嘱及药物处方，病人缴费开药； (8) 病人离院后归档电子病历。
2	住院	(1) 患者到住院收费处办理入院登记，并缴纳预定金； (2) 调出患者就诊信息等基本信息； (3) 问诊后，如需检验检查，开具检验检查申请单，同步信息到检验检测系统； (4) 检验检测后返回检验检查报告； (5) 住院期间定期做检验检查并更新书写电子病历； (6) 推送知情同意书等文件给患者/家属终端，患者/家属签署知情同意书； (7) 开具医嘱及药物处方，病房护士执行医嘱并产生护理记录； (8) 病人离院后归档电子病历，如果有医疗纠纷，需要对

序号	业务名称	业务流程描述
		病历进行封存； (9) 如有需要可能会同步电子病历/部分电子病历到分级诊疗、转院、第三方检验检测等。
3	检验检查	**检验：** (1) 医生根据患者诊断情况开检验项目申请单，医生签字生效； (2) 患者缴费后，化验室根据护士或患者送到的检验样本调取患者基本信息及检验申请单进行化验； (3) 检验技师对检验申请单及标本进行处理，生成检测报告； (4) 检验结果有检验技师医师签字盖章生效，将检验报告传输到门诊医生工作站，医生可对检验结果及显示图形进行诊断。 **检查：** (1) 医生根据患者诊断情况开检查项目申请单，医生签字生效； (2) 患者到指定科室进行检查； (3) 生成检查报告后，检查医技医师在报告提交和审核时进行签名，把检查诊断电子图文报告发送到医生，医生根据诊断报告描述、结论、医师建议进行诊疗。
4	互联网诊疗	(1) 患者使用手机等移动终端登录互联网诊疗系统，就诊前患者需预先填写病情信息并上传相关检查资料； (2) 到预定的就诊时间，在线医生根据患者预先填好的病情资料，采用视频、文字、语音等进行线上问诊。如需检验检查，患者根据医生开具检验检查单，在线预约检查。 (3) 检查后，向医生推送检查结果，医生在线开具药品处方。

序号	业务名称	业务流程描述
		(4) 医生书写病历（个人基本信息、诊断信息、治疗方案信息），并归档。

2 密码应用需求

2.1 风险分析和安全需求

医疗机构场景核心业务信息系统主要涉及 4 个业务场景：门急诊、住院、检验检查、互联网诊疗。表 2 从业务流程角度分析信息系统的密码安全需求，并列出主要保护对象。

表 2 主要保护对象

序号	相关业务	保护对象	保护对象描述	安全需求
1	门急诊	门诊医护人员身份	(1) 医院内信息系统用户必须为授权用户，需要验证登录用户的身份真实性，禁止非授权访问。 (2) 建立、记录、修改、使用病历需要对操作者进行身份鉴别。（包括信息共享和归档）	☑ 真实性 □传输机密性 □存储机密性 □传输完整性 □存储完整性 □不可否认性
2		门诊医疗数据	(1) 患者个人隐私信息：身份证号、住址、电话、联系人； (2) 检验检测信息：检测结果 (3) 医嘱信息及诊断结果信息 (4) 费用信息 其中患者个人隐私信息需要机密性、完整性保护。 费用信息、检验检测结果、医嘱及诊断结果信息均为重要业务数据需要完整性保护。	□真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 □不可否认性

序号	相关业务	保护对象	保护对象描述	安全需求
3		门诊医疗行为	门诊医生对处方、医嘱、电子病历的全生命周期管理。创建、修改、归档等操作需要电子签名保障电子文件签署时的可追溯性（行为的不可否认性）； 患者在签署知情同意文书时需要进行签名。	□真实性 □传输机密性 □存储机密性 □传输完整性 □存储完整性 ☑ 不可否认性
4	住院	病房医护人员身份	(1) 院内业务信息系统用户必须为授权用户，需要验证登录用户的身份真实性，禁止非授权访问。 (2) 建立、记录、修改、使用病历需要对操作者进行身份鉴别。（包括信息共享和归档）	☑ 真实性 □传输机密性 □存储机密性 □传输完整性 □存储完整性 □不可否认性
5		住院医疗数据	(1) 患者个人隐私信息：身份证号、住址、电话、联系人； (2) 检验检测信息：检测结果 (3) 医嘱信息及诊断结果信息 (4) 费用信息 其中患者个人隐私信息需要机密性、完整性保护。 费用信息、检验检测结果、医嘱及诊断结果信息均为重要业务数据需要完整性保护。	☐真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 □不可否认性
6		住院医疗行为	病房医生对处方、医嘱、电子病历的全生命周期管理。创建、修改、归档等操作需要电子签名保障电子文件签署时的可追溯性（行为的不可否认性）； 病房护士对护理记录创建、修改、归档等操	□真实性 □传输机密性 ☐存储机密性 □传输完整性 □存储完整性

序号	相关业务	保护对象	保护对象描述	安全需求
			作需要电子签名保障电子文件签署时的可追溯性 患者在签署知情同意文书时需要进行签名。	☑ 不可否认性
7	检验检查	检验检查医技护人员身份	医院内检验检查信息系统用户必须为授权用户，需要验证登录用户的身份真实性，禁止非授权访问。	☑ 真实性 □传输机密性 ☐存储机密性 □传输完整性 □存储完整性 □不可否认性
8		检验检查数据	(1) 患者个人隐私信息：身份证号、住址、电话、联系人； (2) 检验检测信息：检测结果 (3) 医嘱信息及诊断结果信息 (4) 费用信息 其中患者个人隐私信息需要机密性、完整性保护。 费用信息、检验检测结果、医嘱及诊断结果信息均为重要业务数据需要完整性保护。	□真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 □不可否认性
9		检验检查行为	检验项目化验单或检查诊断报告提交和审核时需要医师技师的电子签名保障行为可追溯性（行为的不可否认性）。	□真实性 □传输机密性 ☐存储机密性 □传输完整性 □存储完整性 ☑ 不可否认性
10	互联网诊	在线医生身份	医院内互联网诊疗系统用户必须为授权用户，需要验证登录用户的身份真实性，禁止	☑ 真实性 □传输机密性

序号	相关业务	保护对象	保护对象描述	安全需求
	疗		非授权访问。	☐存储机密性 □传输完整性 □存储完整性 □不可否认性
11		互联网诊疗数据	(1) 患者个人隐私信息：身份证号、住址、电话、联系人； (2) 检验检测信息：检测结果 (3) 医嘱信息及诊断结果信息 (4) 费用信息 其中患者个人隐私信息需要机密性、完整性保护。 费用信息、检验检测结果、医嘱及诊断结果信息均为重要业务数据需要完整性保护。	□真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 □不可否认性
12		互联网诊疗行为	在线医生对处方、医嘱、电子病历的全生命周期管理。创建、修改、归档等操作需要电子签名保障电子文件签署时的可追溯性（行为的不可否认性）； 患者在签署知情同意文书时需要进行签名。	□真实性 □传输机密性 ☐存储机密性 □传输完整性 □存储完整性 ☑ 不可否认性

2.2 场景对密码应用的特殊要求

（1）医院线上运行数据具备实时信息、即时性读取及更新的特点，例如，医护人员通过检验检测系统获取患者基本信息、检查后书写医嘱、开药时医技人员需要获取医嘱、处方等信息同步场景，对运行中的业务连续性、稳定性、响应

速度有着高要求，通过服务器密码机、安全网关设备对数据做机密性、完整性保护时做性能冗余建设。

（2）由于医院内业务信息系统需要频繁调用患者个人信息，存在模糊查询、复杂查询等情况，部分敏感数据在业务信息系统应用过程中较难进行存储机密性保证，可将患者的身份证号、住址、电话、联系人等不涉及索引的数据字段进行加密保护。

（3）医院内存在各类知情同意文书需要患者签名的场景，不方便发放个人数字证书，可基于患者签名行为的由第三方 CA 机构签发的数字证书方式解决患者行为不可否认性需求。

（4）医院内业务信息系统医技护用户存在大量需要签名的场景，如：住院期间开医嘱、处方、病历书写等需要长期多次签名，需要对签名次数以及时间戳进行数量管理，严格对应实际的签名操作；同时会也面临业务系统数据库存储的原文、签名值会占据较多存储空间，需提前规划好数据存储方式。

（5）医院内业务信息系统需使用密码技术先对检验检查报告、电子病历等送签材料在签名前进行核实，保障送签材料内容的真实和完整。

（6）如医疗机构的 PC 机等设备更换为信创设备后，针对密码设备的信创能力也需进行要求。

3 密码应用实施指南

卫生健康行业的医疗机构场景信息系统依据《全国医院信息化建设标准与规范》指标体系进行建设，包含业务应用、信息平台、基础设施、安全防护、新兴技术五大块内容，本指南内容针对便民服务、医疗服务、医疗管理、医疗协同等业务应用部分的密码应用情况展开描述，主要聚焦于医疗服务中的门急诊、住院、检验检查、互联网诊疗核心业务场景，指导医疗机构建设以患者为核心基于电子病历的业务信息系统，同时满足《医院信息平台应用功能指引》、《医院信息化建设应用技术指引》和相关医院数据上报管理规范的要求，设计合规易用的密码应用手段，保障医院信息化建设过程中的密码应用合规性、正确性及有效性。全国医院信息化建设标准与规范指标体系如下图 3-1 所示：

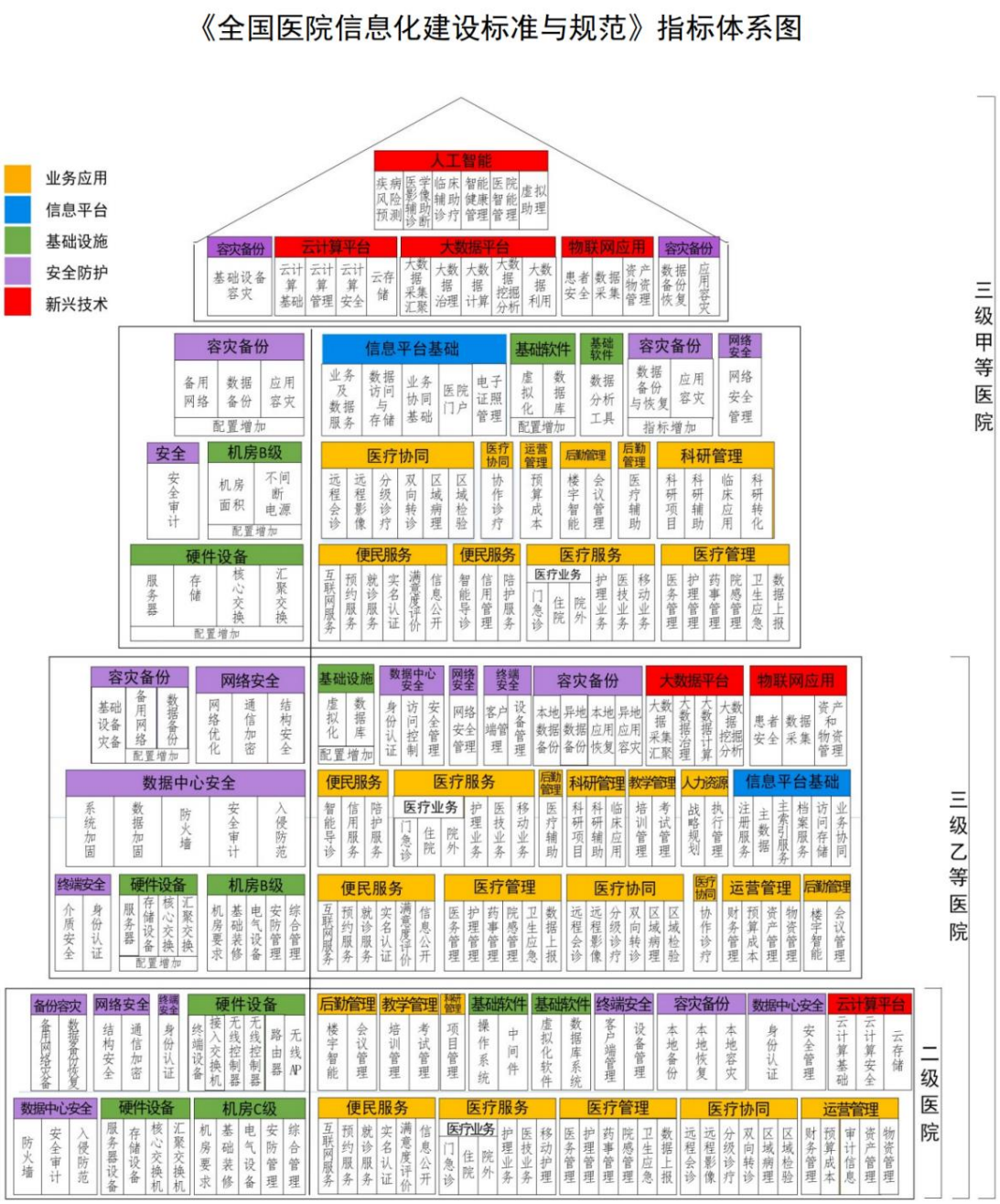

图 3-1 全国医院信息化建设标准与规范指标体系图

3.1 典型场景的密码应用设计

3.1.1 用户身份真实性的密码应用设计

在医疗机构场景中涉及到医院医生、护士、技师等医院工作者及患者、患者家属等就医相关人员的身份鉴别需求，其中患者及患者家属的身份认证存在涉及范围大、人员不固定的情况，可采用协同签名技术或其它手段保障患者及患者家属的身份真实性。医生、护士、技师等医务人员通过 PC 端以及移动终端登录医

院业务信息系统，不同的登录方式对用户身份鉴别的应用要求不一，对此本指南设计了如下两种方案保障用户身份真实性。

院内医务人员使用 PC 端登录时可通过部署符合国密标准 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0029《签名验签服务器技术规范》的签名验签服务器，为 PC 端用户配发基于国密算法且符合 GM/T 0027《智能密码钥匙技术规范》的智能密码钥匙，并配套第三方 CA 机构签发的数字证书，采用符合 GB/T 15843.3 的非对称密码算法的身份鉴别方式实现用户接入的可信身份鉴别。

在线医务人员在移动终端登录时可通过部署符合国密要求且具备商用密码产品认证证书的协同签名系统、GM/T 0028《密码模块安全技术要求》的密码服务管理平台，为移动智能终端用户提供协同签名服务，移动 App 集成符合 GM/T 0028《密码模块安全技术要求》的移动智能终端安全密码模块，通过调用协同签名系统的协同签名技术实现移动端用户的身份鉴别。

医务人员的身份鉴别采用数字证书方式的身份认证，根据数字证书载体的不同，如采用 USBkey 或移动终端等，其身份认证的方式有所区别，使用 USBkey 时需要医务人员将 USBkey 插入 PC 端；使用移动终端时，可通过协同签名技术用数字证书直接登录移动终端系统，也可通过扫描二位码等方式登录 PC 端系统，但业务信息系统的身份认证实现流程是类似的，具体实现流程如图 3-2 所示：

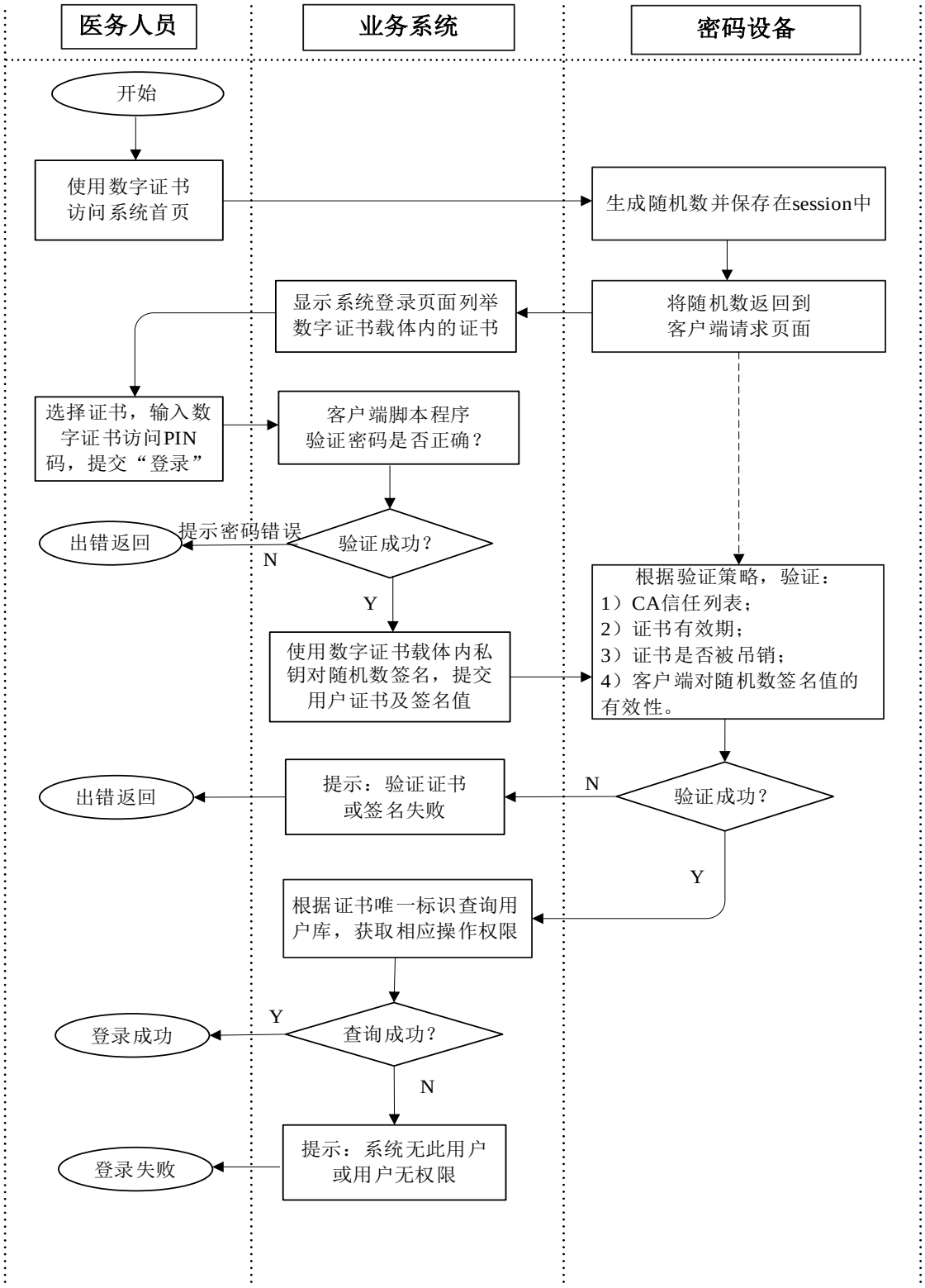

图 3-2 身份鉴别流程图

3.1.2 医患行为不可否认性的密码应用设计

经过对医疗机构业务场景分析，门诊、住院、检验检查、互联网诊疗业务场景中对不可否认性的需求包含医技护人员处方书写、医嘱书写、护理记录书写、

电子病历书写、检验检查诊断报告生成等关键业务操作的不可否认性，医护人员病历完成时间的不可否认性以及患者知情同意文书签署的不可否认性。

(1) 病历完成时间的不可否认性

根据病历书写基本规范要求，病历书写完成具有明确时间要求，在医疗应用数据作为法律责任认定时，可通过部署符合国密要求且具备商用密码产品认证证书的时间戳服务器，保证医疗应用数据时间的不可否认性。

(2) 医技护人员行为的不可否认性

门诊、住院、检验检查场景中医技护人员的电子签名，可调用符合国密要求且具备商用密码产品认证证书的密码产品的数字签名验签服务，配套使用符合 GM/T 0027《智能密码钥匙技术规范》的智能密码钥匙以及第三方 CA 认证机构颁发的数字证书，用于保障医护人员处方、医嘱、护理记录、电子病历书写以及检验检查诊断报告生成等关键业务行为的不可否认性。在互联网诊疗业务场景中，可通过部署符合国密要求且具备商用密码产品认证证书的协同签名系统，为移动智能终端用户提供协同签名服务，移动 App 集成符合 GM/T 0028《密码模块安全技术要求》的移动智能终端安全密码模块，通过调用协同签名系统的协同签名技术，基于 SM2 算法实现在线医生处方、医嘱、电子病历书写等行为的不可否认。

电子病历文档来自于不同的业务信息系统，因此当医务人员在医院各类信息系统中编写完电子病历后进行数字签名时，需要由生成该电子病历的信息系统在当前节点调用密码设备的数字签名服务、时间戳服务实现数字签名和加盖时间戳。

具体实现流程如图 3-3 所示：

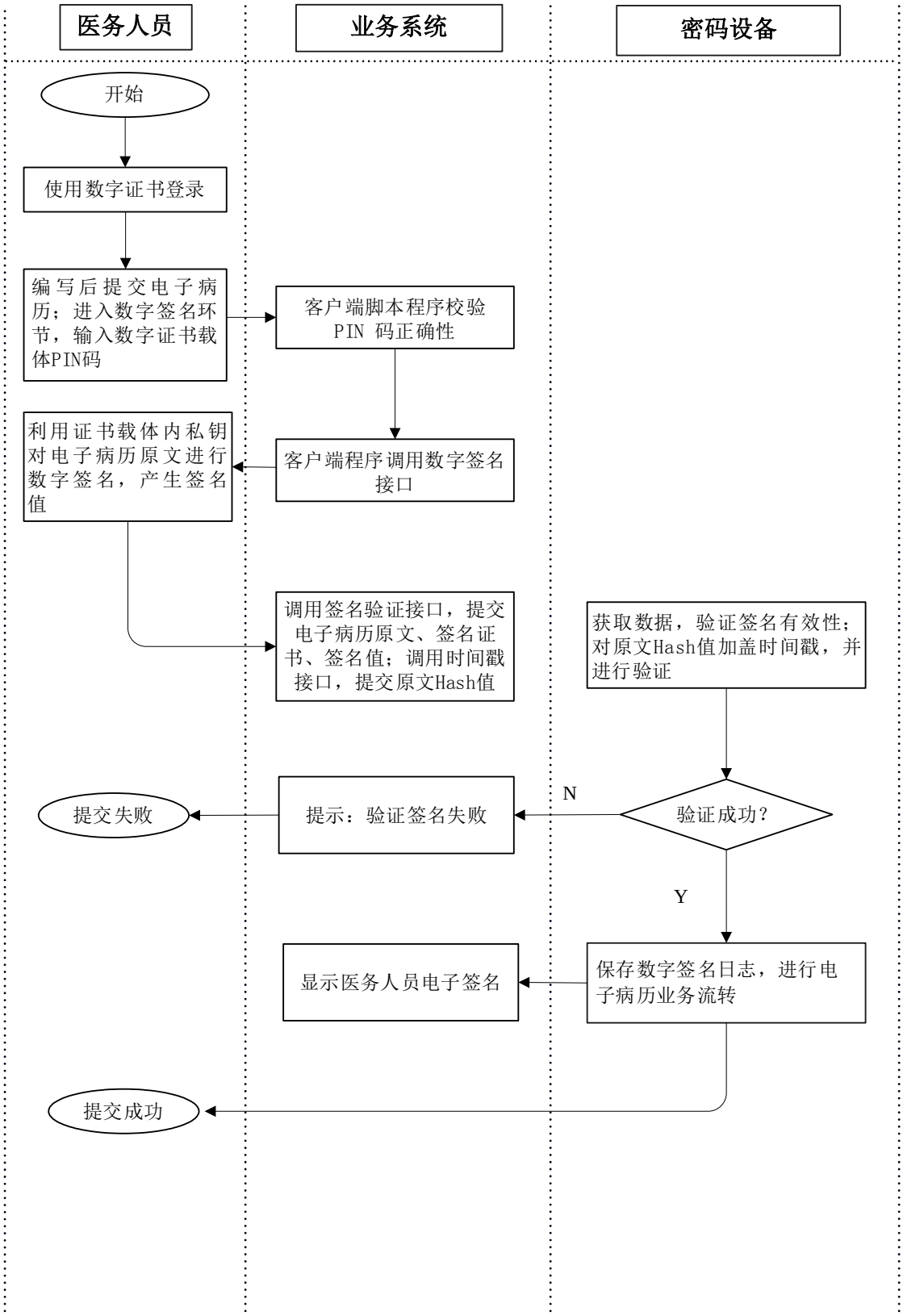

图 3-3 医技护人员电子签名流程图

(3) 患者知情同意文书签署的不可否认性

根据医疗机构患者签署知情同意文书的场景，不便于为患者发放智能密码钥匙，同时为提升患者电子签名实现效率，可通过为患者签署介质部署符合 GM/T 0028《密码模块安全技术要求》第二级要求的密码模块，配套在业务域部署的符合国密要求且具备商用密码产品认证证书的手写信息数字签名系统并基于患者签名行为的由第三方 CA 机构签发的数字证书，保障患者签署知情同意类文书行为的不可否认性。

患者对知情同意类文书进行知情确认时，由生成该知情同意类文书的信息系统在当前节点调用数字签名服务、时间戳服务实现数字签名、时间戳，成功后会在该知情同意类文书的相应位置显示签名人的电子签名。

具体实现流程如图 3-4 所示。

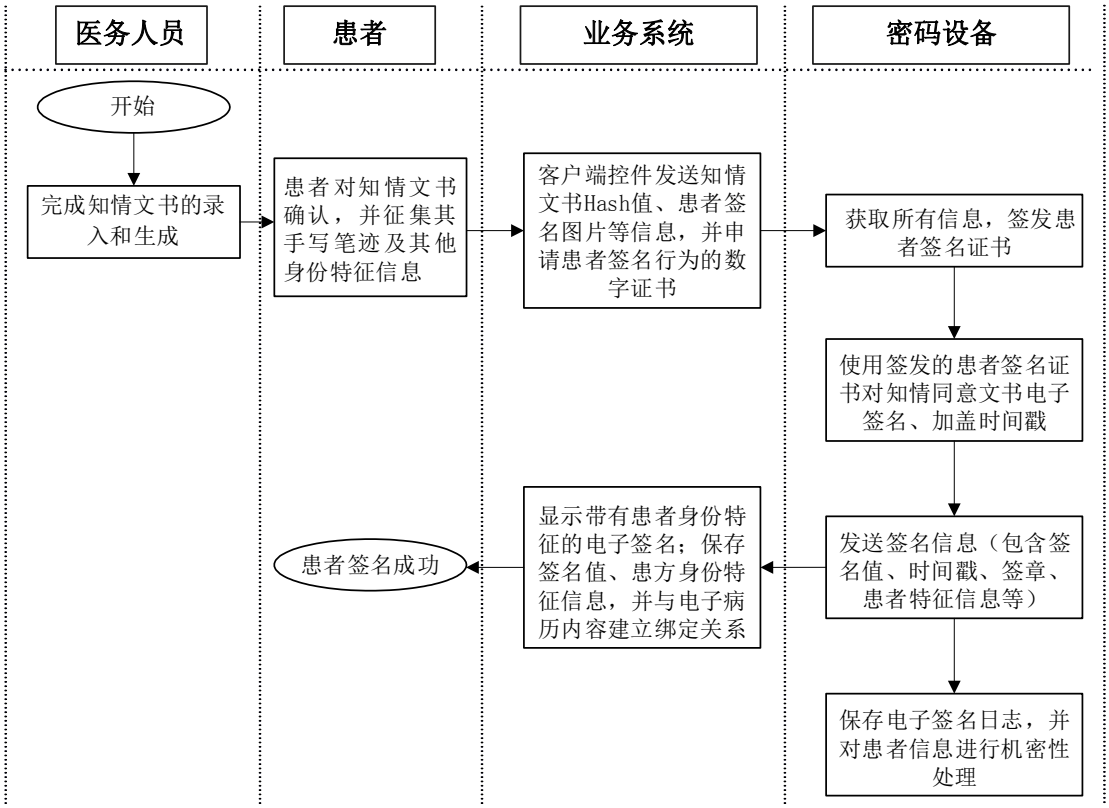

图 3-4 患者知情同意文书确认电子签名流程图

3.1.3 重要数据传输安全的密码应用设计

在医疗机构场景中门急诊、住院、检验检查、互联网诊疗均涉及到重要数据传输安全需求，包含患者个人隐私信息的传输机密性、传输完整性以及费用信息、检验检查报告等重要业务数据的传输完整性，同时也涉及与医保机构、区域平台之间医保报销、分级诊疗、区域检查、绩效考核等协同业务，其中包括费用支付数据、绩效信息数据、电子病历等重要业务数据的信息交换和互联互通，此类数据在传输过程中的安全保护至关重要，需使用密码技术保障重要数据机密性、完整性，可在网络和数据层面分别采用密码技术保障通信数据的传输安全。

在网络安全保护层面，可在医院机房部署符合 GM/T 0024《SSL VPN 技术规范》、GM/T 0025《SSL VPN 网关产品规范》、GM/T 0026《安全认证网关产品规范》的 SSL VPN 安全网关及安全认证网关，采用数字证书为应用系统提供身份鉴别、传输加密、访问控制和安全审计服务等功能服务，通过建立国密 SSL 加密通道，保障业务数据传输过程、互联网医疗等业务环节中，医疗健康数据在客户端与服务端之间的传输安全。网络层面的传输安全保障如下图 3-5 所示：

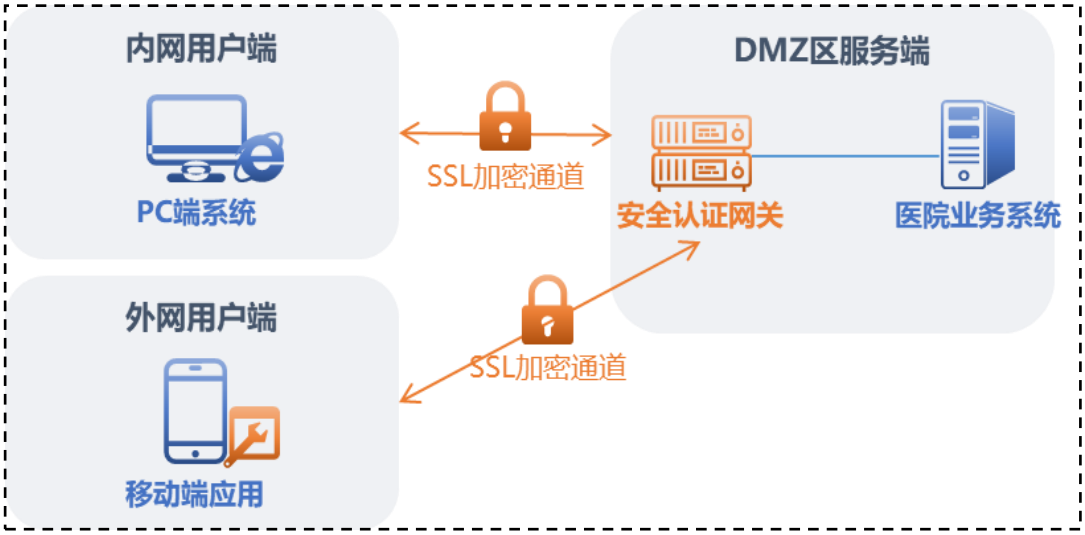

图 3-5 网络层面客户端-服务端传输安全示意图

在数据安全保护层面，传输数据时，业务系统调用符合 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0030《服务器密码机技术规范》的服务器密码机，基于 SM2、SM3、SM4 密码算法的数据签名验签、数据加解密技术对业务系统中需要传输的重要数据实现机密性、完整性保护，数据层面的传输安全保障，如下图 3-6 所示：

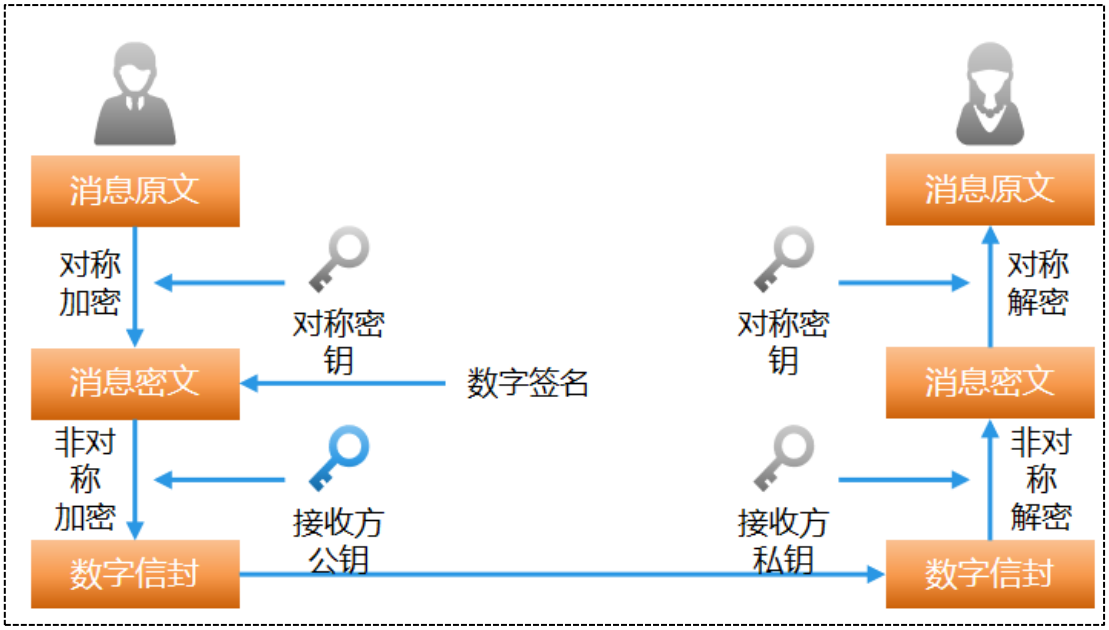

图 3-6 数据层面客户端-服务端传输安全示意图

3.1.4 重要数据存储安全的密码应用设计

在医疗机构场景中门急诊、住院、检验检查、互联网诊疗均涉及到重要数据存储安全需求，包含患者个人隐私信息的存储机密性、存储完整性以及费用信息、检验检查报告等重要业务数据的存储完整性。

(1) 重要数据存储完整性保护

可部署符合 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0030《服务器密码机技术规范》的服务器密码机，业务系统在对诊断信息、费用信息、检验检查报告等重要业务数据进行存储时，基于密码设备/服务提供的 HMAC-SM3 技术，实现重要数据的存储完整性保护。

(2) 重要数据存储机密性保护

可部署符合 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0030《服务器密码机技术规范》的服务器密码机，调用数据加解密服务，基于 SM4 的对称密码技术，对患者个人隐私信息(身份证号、住址、电话、联系人)等重要数据进行加密保护，确保数据库里的患者个人敏感信息内容不被非法泄露，实现重要数据的存储机密性保护。

业务系统重要数据的存储机密性、完整性调用加解密服务、完整性运算服务实现，如下图 3-7 所示：

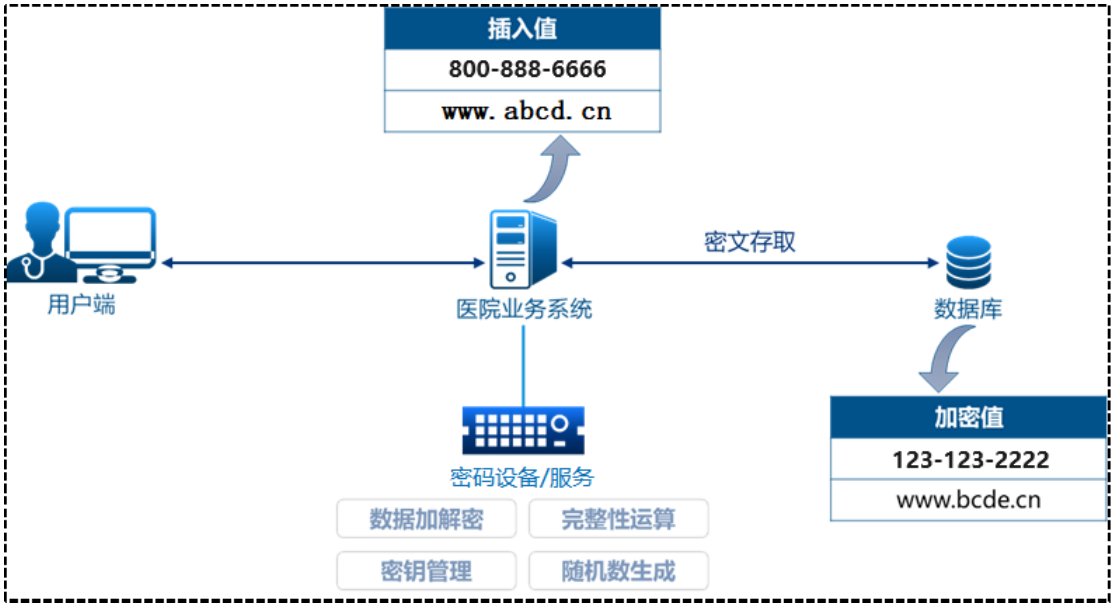

图 3-7 数据存储安全示意图

也可根据系统实际业务以及功能需求，选用具备商用密码产品认证证书的数据库加密系统、数据安全网关、磁盘阵列加密等合规的密码产品/服务实现数据加密存储。

3.1.5 密钥管理建设

密钥管理包括对密钥的生成、存储、分发、使用、更新、备份和恢复、归档、撤销等全生命周期管理。其中第三方 CA 机构签发的数字证书，用于实现系统用户登录时的身份鉴别及行为不可否认，此类密钥由第三方 CA 机构规范管理，并将相关管理制度补充到密钥管理规范中；对于业务信息系统涉及的密钥全生命周期管理如下表 3 所示：

表 3 密钥全生命周期管理

密钥名称	生成	存储	分发	使用	更新	备份和恢复	归档	销毁	用途说明
数据传输签名私钥	服务器密码机内部产生	服务器密码机内部存储	私钥不进行分发	在密码模块中进行签名运算	按照管理制度定期更新	不涉及	不涉及	密码设备内部进行销毁	数据传输完整性保护
数据传输验签公钥	服务器密码机内部产生	以公钥和证书形式存储	以证书形式分发	在密码模块中进行签名运算	按照管理制度定期更新	签名公钥不提供备份恢复机制	不涉及	密码设备内部进行销毁	数据传输完整性保护验证

密钥名称	生成	存储	分发	使用	更新	备份和恢复	归档	销毁	用途说明
数据传输加密密钥	服务器密码机内部产生	服务器密码机内部存储	分发至客户端	在密码模块中进行加解密运算	按照管理制度定期更新	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据传输机密性保护
临时会话密钥	服务器密码机内部产生	不涉及	不涉及	分别在客户端和服务端	会话恢复时更新	不涉及	不涉及	会话终止时销毁	数据传输安全通信
HMAC密钥	服务器密码机内部产生	服务器密码机内部存储	不涉及	在密码模块中进行验证签名运算	按照管理制度定期更新	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据存储完整性保护
数据存储加密密钥	服务器密码机内部产生	服务器密码机内部存储	不进行分发	在密码模块中进行加解密运算	按照管理制度定期更新	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据存储机密性保护

3.1.6 安全管理体系建设

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）的要求，从管理制度、人员管理、建设运行和应急处置四个层面制定了相应的制度文件、规章流程，对医院的密码应用安全管理体系进行完备的建设，保障系统规划、建设、后期运维和应急响应的安全性。依据《信息系统密码应用测评要求具体》（GM/T 0115-2021）确定每个安全层面的建设内容，如下表 4 所示：

表 4 安全管理体系建设内容

安全层面	建设内容	内容描述
管理制度	具备密码应用安全管理制度	具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。

安全层面	建设内容	内容描述
	密钥管理规则	根据密码应用方案建立相应密钥管理规则。
	建立操作规程	对管理人员或操作人员执行的日常管理操作建立操作规程。
	定期修订安全管理制度	定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。
	明确管理制度发布流程	明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。
	制度执行过程记录留存	具有密码应用操作规程的相关执行记录并妥善保存。
人员管理	了解并遵守密码相关法律法规和密码管理制度	相关人员了解并遵守密码相关法律法规、密码应用安全管理制度。
	建立密码应用岗位责任制度	建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限。
	建立上岗人员培训制度	建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能。
	定期进行安全岗位人员考核	定期对密码应用安全岗位人员进行考核。
	建立关键岗位人员保密制度和调离制度	建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。
建设运行	制定密码应用方案	依据密码相关标准和密码应用需求，制定密码应用方案。
	制定密钥安全管理策略	根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求。

安全层面	建设内容	内容描述
	制定实施方案	按照应用方案实施建设。
	投入运行前进行密码应用安全性评估	投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行。
	定期开展密码应用安全性评估及攻防对抗演习	在运行过程中，严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
应急处置	应急策略	制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置。
	事件处置	事件发生后，及时向信息系统主管部门进行报告。
	向有关主管部门上报处置情况	事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

3.2 密码产品/服务选择和部署

根据系统密码应用的需求和建设目标，通过对医疗机构信息系统和系统用户提供安全可信服务，其服务核心是实现“可信身份、可信行为、可信数据、可信通道、可信时间”等密码应用，保障系统网络身份和实体身份的真实对应，建设重要数据防篡改、重要数据防窃取等服务的重要支撑基础设施。

医疗机构核心业务信息系统主要面向的用户为院内医技护人员，通过 PC 端或者移动终端接入系统，密码应用部署可采用本地部署密码设备模式，也可根据系统密码设备、接口、密钥等统一管理及密码资源合理分配等需求采用密码服务管理平台统一建设部署模式，具体的密码产品选择和部署如下图 3-8 所示：

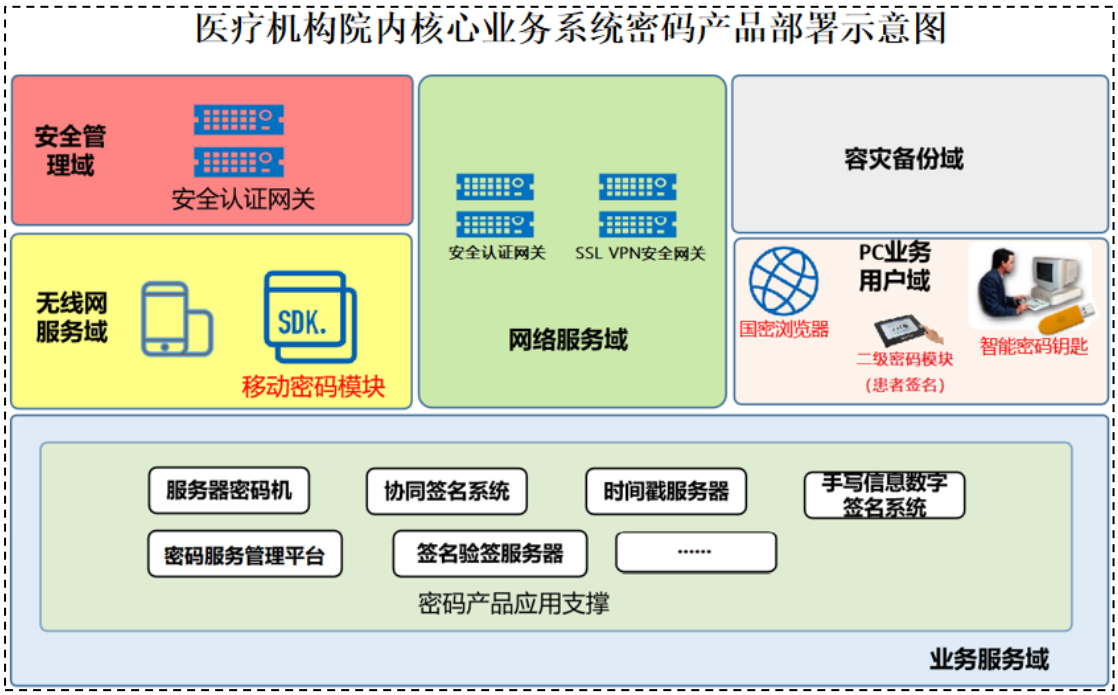

图 3-8 医疗机构院内核心业务系统密码产品部署示意图

医疗机构互联网核心业务系统主要面向的用户为互联网在线医生，通过移动终端接入系统，其中协同签名系统部署在 DMZ 区域，密码应用部署如下图 3-9 所示：

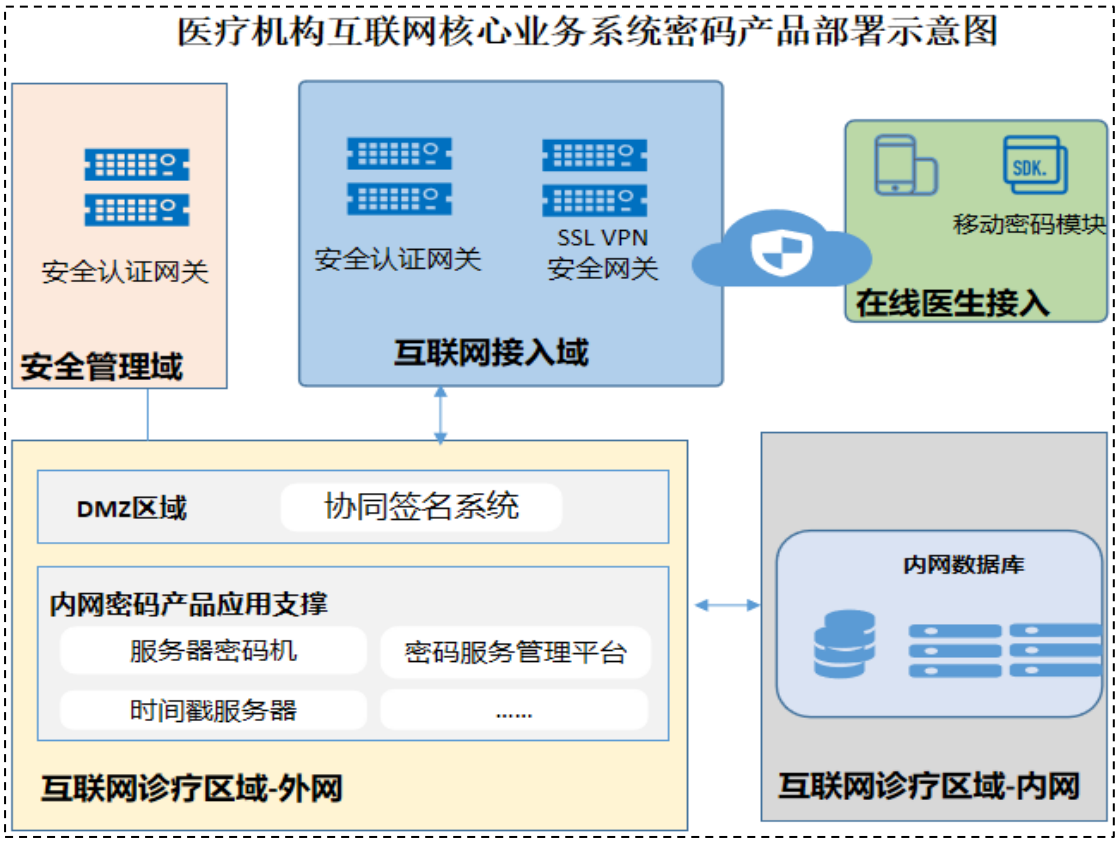

图 3-9 医疗机构互联网核心业务系统密码产品部署示意图

表 5 密码产品/服务

序号	密码产品/服务名称	在场景中提供的密码功能
1	密码服务管理平台	通过将若干密码设备、密码模块按照统一的聚合机制进行池化，搭建密码服务管理平台，引入微服务与虚拟化等技术，通过密码设备、密码安全服务接口进行有效统一管理、配置，密码服务拥有弹性扩展、平行扩容能力，提供丰富的密码服务支撑； 通过内建多层密钥管理模型，运用应用认证、计算隔离、密钥存储分离、访问授权、全流程审计等技术手段，有效阻断各种攻击路径，对密码应用涉及的各类密钥的全生命周期进行安全管理，符合医疗机构信息系统中密钥层次复杂、种类多、数量大等特点需求； 满足医疗机构核心业务信息系统各层面的用户身份真实性、数据机密性、数据完整性、不可否认性的密码应用需求。
2	安全认证网关	基于密码技术构建安全通道，保证网络通信层身份鉴别、通信数据的机密性和完整性保护以及网络边界访问控制信息完整性；保证设备计算层身份鉴别、远程管理通道安全。
3	SSL VPN 安全网关	基于 SSL/TLS 协议，在通信网络中构建安全通道，保证网络通信层身份鉴别、通信数据的机密性和完整性保护以及网络边界访问控制信息完整性。
4	服务器密码机	为设备和计算层提供日志完整性保护。 为应用和数据层访问控制信息提供完整性保护。 为应用和数据安全层基础医疗卫生信息等历史存量数据提供存储机密性和完整性保护。

序号	密码产品/服务名称	在场景中提供的密码功能
5	签名验签服务器	为应用和数据层提供基于PC端用户数字证书的身份鉴别服务。
6	时间戳服务器	为应用和数据层医疗应用数据提供时间不可否认性服务。
7	协同签名系统	为应用和数据层提供基于移动端用户数字证书的身份鉴别服务。
8	移动智能终端安全密码模块	部署于移动智能终端介质中,实现医院信息系统移动端用户身份鉴别。
9	手写信息数字签名系统（患者服务端）	基于患者签名行为的由第三方CA机构签发的数字证书，为患者知情同意文书提供不可否认性服务。
10	二级密码模块（患者终端）	处理患者手写笔迹、身份认证信息，实现医院信息系统患者知情同意文书提供不可否认性服务。
11	国密智能密码钥匙	用于安全认证网关登录堡垒机身份鉴别。 实现医院信息系统用户登录身份鉴别。

3.3 与 GB/T 39786 对照情况说明

根据 GB/T 39786 相关配套标准《商用密码应用安全性评估 FAQ》要求，GB/T 39786-2021 中的密码应用等级一般由网络安全等级保护的级别确定。信息系统根据 GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级。根据要求可知，在开展密码应用涉及测评相关活动前，应首先明确密码应用主体，范围及责任主体。

本指南针对医疗机构场景符合等保三级的核心业务系统，例如院内电子病历系统、互联网诊疗系统。范围为业务系统及其机房网络设备情况；责任主体为医院。与 GB/T 39786 对照情况说明如下表 6 所示：

表 6 与 GB/T 39786 对照情况说明

安全层面	密码技术应用点	采取的密码措施
物理和环境安全	身份鉴别	业务系统所在机房选择符合相关国家标准、行业标准的门禁管理系统，实现进入机房人员身份真实性鉴别。
	电子门禁记录数据存储完整性	业务系统所在机房选择符合相关国家标准、行业标准的门禁管理系统，实现电子门禁记录数据的完整性保护。
	视频监控记录数据存储完整性	业务系统所在机房采用符合相关国家标准、行业标准的视频监控管理系统，保证视频监控记录数据完整性。
网络和通信安全	身份鉴别	存在四类通路： (1) PC 业务客户端用户数据流经链路； (2) 移动业务客户端用户数据流经链路； (3) 运维用户数据流经链路； (4) 业务系统与其他系统通信通道（主要适用于本业务系统提供接口的情况）。 在网络服务域部署并使用具有商用密码产品认证证书的网关产品实现通信实体的身份真实性，同时实现数据在通信过程中的机密性、完整性。
	通信数据完整性	
	通信过程中重要数据的机密性	
	网络边界访问控制信息完整性	按照等保三级要求建设。同时可采用基于合规的密码设备对边界设备访问控制信息做完整性保护。
	安全接入认证	当前医院信息系统在设备等方面的安全，按照等保三级要求建设。医院自助机、移动设备在接入信息系统时，可使用具有商用密码产品认证证书的网关产品和客户端密码模块实现接入设备的真实性。
设备和计算安全	身份鉴别	为运维人员发放智能密码钥匙，在运维主机部署国密浏览器，在安全管理域部署安全认证网关代理，保证运维人员的身份真
	远程管理通	

安全层面	密码技术应用点	采取的密码措施
	道安全	实性与远程管理通道安全。
	系统资源访问控制信息完整性	密码产品：部署的密码产品均具有合格的商用密码产品认证证书。
		其他服务器：系统资源访问控制信息依赖操作系统实现，不做额外建设。
	重要信息资源安全标记完整性	不适用。
	日志记录完整性	密码产品具有合格的商用密码产品认证证书，且可以确定实际部署的产品与认证产品一致的情况下，密码产品可判定为符合。
		在业务服务域部署合规的服务器密码机，日志审计系统调用服务器密码机的密码服务，实现日志记录完整性保护。
	重要可执行程序完整性、重要可执行程序来源真实性	医院所有业务系统都是明确来源、安全性可控，部署的密码产品具有合格的商用密码产品认证证书。
应用和数据安全	身份鉴别	主要用户：医技护人员 PC 端依托合规的智能密码钥匙和密码设备采用基于 SM2 算法的签名技术实现登录用户的身份鉴别；移动端依托协同签名移动端模块及协同签名服务采用协同签名技术实现登录用户的身份鉴别。
	访问控制信息完整性	业务系统角色与权限，系统关键应用访问与控制信息存储于数据库中。业务系统调用数据完整性运算服务，基于 HMAC-SM3

安全层面	密码技术应用点	采取的密码措施
		保障访问控制信息完整性。
	重要信息资源安全标记完整性	不适用。
	重要数据传输机密性、完整性	重要数据在业务系统的应用层传输的场景下，服务端向客户端传输数据时，服务端调用符合 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0030《服务器密码机技术规范》的服务器密码机，基于 SM2、SM3、SM4 密码算法的数据签名验签、数据加解密技术对业务系统中需要传输的重要数据实现机密性、完整性保护；客户端向服务端传输数据时，调用客户端密码模块，基于 SM2、SM3、SM4 密码算法的数据签名验签、数据加解密技术对业务系统中需要传输的重要数据做安全保护，实现重要数据传输的机密性、完整性保护。
	重要数据存储机密性	部署符合 GM/T 0028《密码模块安全技术要求》的密码服务管理平台、GM/T 0030《服务器密码机技术规范》的服务器密码机，调用服务器密码机的数据加密功能，基于 SM4 的对称密码技术，对患者个人隐私信息(身份证号、住址、电话、联系人)等重要数据进行加密保护，确保数据库里的患者身份信息等敏感信息内容不被非法泄露，实现重要数据的存储机密性保护。
	重要数据存储完整性	业务系统调用数据完整性运算密码服务，保证业务系统中诊断信息、费用信息、检验检查报告等重要数据的存储完整性。
	不可否认性	通过调用符合国密要求且具备商用密码产品认证证书的密码产品的数字签名验签服务，配套保障第三方 CA 机构签发的数字证书，保障医技护人员医疗行为不可否认性。
		根据病历书写基本规范要求，病历书写完成具有明确时间要求，在医疗应用数据作为法律责任认定时，在业务服务域部署时间

安全层面	密码技术应用点	采取的密码措施
		戳服务器，保证医疗应用数据时间的不可否认性。
		在业务系统医疗用客户端部署患者电子签名客户端二级密码模块，在业务系统医疗应用服务端部署患者电子签名服务端，配套基于患者签名行为的由第三方 CA 机构签发的数字证书，保证患者知情同意一类文书的不可否认性。

3.4 注意事项

(1) 密码应用范围确认。在设计密码应用方案前，需要确认系统边界范围、密码保护范围。建议参照网络安全等级保护第三级定级范围规划密码应用设计范围，明确范围后，结合系统实际业务情况考虑安全性、可用性及性能。

(2) 为保障业务连续性，避免系统瘫痪，网关设备、服务器密码机等密码产品建议采用双机热备方式运行。

(3) 系统上云情况，若在院内私有云部署，可按照前文密码应用设计进行实施部署；若部署于公有云或使用云签名、云认证等密码技术，新建系统选择密码应用合规的云环境、云密码技术进行部署，已建信息系统的安全保护依托所在云平台的物理机房、网络通信、设备计算、应用数据的密码应用基础设施建设情况。

4 密码应用安全性评估实施指南

4.1 主要测评指标的选择和确定

4.1.1 测评范围

鉴于医疗机构涉及院内电子病历系统、互联网诊疗系统等不同系统架构的业务系统，涉及的用户较多，且院内电子病历系统由众多子系统组成，因此本指南给出的测评实施并非针对医疗机构的某个子系统，仅根据该场景下典型业务特点和密码应用设计方案，给出关键安全需求的测评实施指南，如网络和通信安全层面、应用和数据安全层面等关键安全需求的密码应用测评等，供相关方在开展密码应用安全性测评时参考。

4.1.2 测评指标

选择GB/T 39786-2021中的第三级安全要求作为本指南典型场景测评工作的基本指标。结合前文描述的场景业务情况，GB/T 39786-2021 第三级要求中的个别项可能并不适用，本指南典型场景的适用测评指标、不适用测评指标及其不适用原因如表 7 所示。

表 7 主要测评指标的选择和确定

类型	指标项			说明
主要适用指标	技术要求	物理和环境安全	身份鉴别	无
			电子门禁记录数据存储完整性	
			视频监控记录数据存储完整性	
		网络和通信安全	身份鉴别	
			通信数据完整性	
			通信过程中重要数据的机密性	
			网络边界访问控制信息的完整性	
			安全接入认证	
		设备和计算安全	身份鉴别	
			远程管理通道安全	
			系统资源访问控制信息完整性	
			日志记录完整性	
			重要可执行程序完整性、重要可执行程序来源真实性	
		应用和数据安全	身份鉴别	
			访问控制信息完整性	
			重要数据传输机密性	
			重要数据存储机密性	
			重要数据传输完整性	
			重要数据存储完整性	

类型	指标项			说明
			不可否认性	
	管理要求	管理制度	具备密码应用安全管理制度	
			密钥管理规则	
			建立操作规程	
			定期修订安全管理制度	
			明确管理制度发布流程	
			制度执行过程记录留存	
		人员管理	了解并遵守密码相关法律法规和密码管理制度	
			建立密码应用岗位责任制度	
			建立上岗人员培训制度	
			定期进行安全岗位人员考核	
			建立关键岗位人员保密制度和调离制度	
		建设运行	制定密码应用方案	
			制定密钥安全管理策略	
			制定实施方案	
			投入运行前进行密码应用安全性评估	
			定期开展密码应用安全性评估及攻防对抗演习	
		应急处置	应急策略	
			事件处置	
			向有关主管部门上报处置情况	
主要不适用指标	设备和计算安全		重要信息资源安全标记完整性	受测系统未对设备配置重要信息资源安全标记，故本指标不适用

类型	指标项		说明
	应用和数据安全	重要信息资源安全标记完整性	受测系统关键应用未设置重要信息资源安全标记，故本指标不适用

4.2 主要测评内容

4.2.1 物理和环境安全测评

(1) 测评对象

该层面的测评对象主要为医疗机构场景业务系统所在机房等重要区域及其电子门禁系统、视频监控系统。该层面确定的测评对象和采用的测评方式如下表8所示。

表 8 测评对象和测评方式

层面（类）	测评对象	测评方式
物理和环境安全	医疗机构场景业务系统所在部署机房	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☐ 配置检查 ☐ 工具测试

(2) 测评实施要点

测评实施时，测评人员应参照 GM/T 0115-2021《信息系统密码应用测评要求》和 GM/T 0116-2021《信息系统密码应用测评过程指南》对医疗机构场景业务系统所在机房等重要区域及其电子门禁系统、视频监控系统进行测评，核查重要区域进入人员身份鉴别机制、电子门禁记录数据和视频监控记录数据存储完整性保护机制等。如果被测业务系统部署在多个机房，则相应的机房均应列为测评对象。如果医疗机构场景业务系统所在机房由云服务提供商提供，则可以结合有关云平台、云上应用测评的相关指导性文件进行实施。

4.2.2 网络和通信安全测评

(1) 测评对象

根据本指南中典型场景承载的业务和密码应用设计，分析该层面涉及的测评对象。

医疗机构业务系统涉及不同种类角色的用户，包括医生、护士、技师等医务人员，不同角色的用户访问业务系统的渠道方式不完全一样，如 PC 端、移动终端等。该过程涉及的网络层传输保护主要为不同角色的用户访问业务系统的通信信道，主要包括：PC 端用户与业务系统之间的通信信道、移动终端用户与业务系统之间的通信信道等。鉴于患者用户涉及范围较大、人员不固定，访问渠道方式多样，网络层传输保护密码应用方案不统一，因此本指南测评实施部分仅考虑医生、护士、技师等医务人员通过 PC 端和移动终端访问其所属范围的业务系统的通信信道情况。此外，如果业务系统存在对外提供接口的情况，则被测业务系统与网络边界外的其他系统的通信信道也需要作为测评对象。

当远程管理通道跨越网络边界时，如在互联网访问 SSL VPN 接入内网后通过堡垒机对设备进行管理的情况，则网络和通信安全层面需要测评管理员在互联网访问 VPN 的过程。

综上所述，该层面可能涉及的测评对象和采用的测评方式如表 9 所示。

表 9 测评对象和测评方式

层面（类）	测评对象	测评方式
网络和通信安全	医生、护士、技师等医务人员通过 PC 端访问其所属范围的业务系统的通信信道	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试
	医生、护士、技师等医务人员通过移动终端用户访问其所属范围的业务系统的通信信道	
	业务系统与其他系统的通信信道（如涉及）	
	远程管理员访问 VPN 的通信信道（如涉及）	

(2) 测评实施要点

测评实施时，测评人员应重点关注通信实体身份鉴别、通信数据完整性、通信过程重要数据的机密性、网络边界访问控制信息的完整性以及设备接入认证等，

可参照 GM/T 0115-2021 中 6.2 章节描述的内容实施测评，测评关键检查点如下图 4-1 所示。

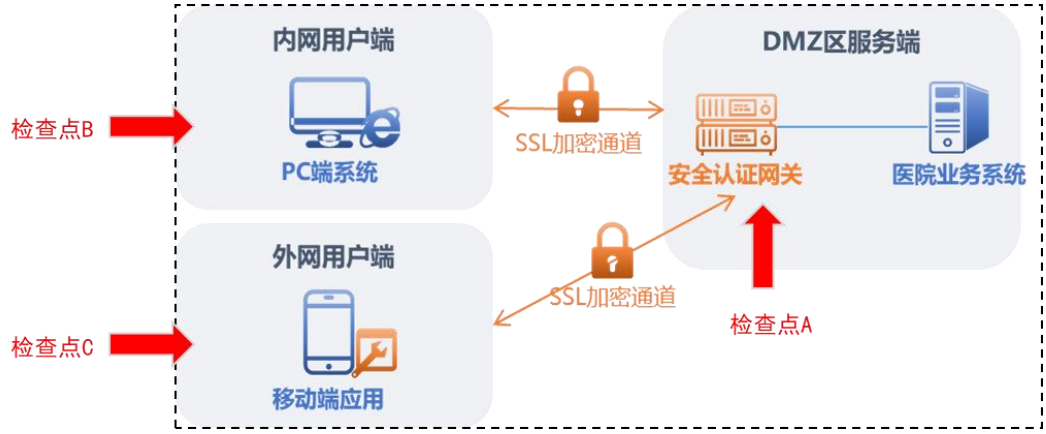

图 4-1 测评实施检查点

测评实施要点包括：

1) 核查用于密钥管理和密码计算的密码产品是否符合法律法规的相关要求，需依法接受检测认证的，核查是否经商用密码认证机构认证合格；了解密码产品的型号和版本等配置信息，核查密码产品是否符合密码模块标准中相应安全等级及以上安全要求，并核查密码产品的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件。

2) 在检查点使用协议分析工具，抓取内网用户 PC 端与安全认证网关、外网移动用户端与安全认证网关之间的通信数据，分析是否采用密码技术对通信实体进行身份鉴别，是否采用密码技术保证通信过程中数据的完整性、通信过程中重要数据的机密性。

3) 通过文档审查、配置检查等方式验证是否使用密码技术保护网络边界访问控制信息的完整性，是否使用密码技术对有设备接入认证需求的设备进行接入认证等。

4.2.3 设备和计算安全测评

(1) 测评对象

该层面可能涉及的测评对象和采用的测评方式如下表 10 所示。

表 10 测评对象和测评方式

层面（类）	测评对象	测评方式
设备和计算安全	通用服务器（如应用服务器、数据库服务器）、数据库管理系统、安全认证网关、密码服务管理平台、服务器密码机、签名验签服务器、协同签名系统、时间戳服务器、移动智能终端安全密码模块、堡垒机等	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试

(2) 测评实施要点

测评指标包括登录设备时采用的身份鉴别方式、远程管理通道安全、系统资源访问控制信息完整性、日志记录完整性、重要可执行程序完整性与来源真实性。鉴于该层面与系统业务关联性不强，因此测评时可按照 GM/T 0115-2021 中 6.3 章节描述的测评方法实施测评。

4.2.4 应用和数据安全测评

(1) 测评对象

医疗机构核心业务系统为院内电子病历系统、互联网诊疗系统，实际测评时根据测评范围确定具体测评对象。业务系统应用涉及的用户包括医生、护士、技师等医务人员；涉及的重要数据包括患者个人隐私信息相关数据，费用支付信息、检验检查报告、电子病历等业务数据；涉及的关键行为包括医技护人员处方书写、医嘱书写、护理记录书写、电子病历书写、检验检查诊断报告生成等业务行为。其中，关于患者个人用户身份鉴别的测评本指南暂不考虑。

该层面涉及的测评对象和采用的测评方式如表 11 所示。

表 11 测评对象和测评方式

层面（类）	测评对象	测评方式
应用和数据安全	医疗机构场景业务系统应用	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试

(2) 测评实施要点

测评指标包括用户身份鉴别、访问控制信息完整性、重要数据传输机密性和完整性、重要数据存储机密性和完整性、不可否认性。

测评实施要点包括：

1）业务系统用户身份的真实性鉴别机制

首先，采用访谈安全管理人员、查看系统设计文档等方式，了解业务系统应用用户的身份鉴别机制及鉴别过程中涉及密钥的生命周期管理。然后，采用审查代码片段、配置检查和查看日志等方式，对之前获取证据进行确认。

根据系统密码应用设计，业务系统采用如下两种方案保障用户身份的真实性：

a) PC 端用户：通过为用户配发具有商用密码产品认证证书的智能密码钥匙，使用第三方 CA 机构签发的数字证书，基于 SM2 算法实现对用户的身份鉴别。

b) 移动终端用户：在移动终端集成具备商用密码产品认证证书的移动智能终端安全密码模块，通过调用协同签名系统的协同签名服务，基于 SM2 算法实现移动终端用户的身份鉴别。

针对两种不同的鉴别机制，采用不同的测评方法。

如果采用 a)方式中描述的使用智能密码钥匙实现身份鉴别，可以通过抓取用户 PC 端与业务系统服务端的通信数据包，分析是否包含服务端挑战值的签名字段；查看业务系统的签名验签服务器日志，查看是否对挑战的签名字段进行了验签操作；查看用户智能密码钥匙的签名数字证书是否符合要求。

如果采用 b)方式中描述的协同签名机制，则可以查看协同签名系统日志和业务系统配置界面，确认是否执行协同签名操作；抓取移动终端与业务系统服务端的通信数据包，分析是否包含签名字段；查看协同签名系统的日志，查看是否进行了验签操作。

2）访问控制信息完整性

业务应用涉及的访问控制信息可以通过查看数据库、代码实现片段、服务器密码机调用日志等方式检查是否对访问控制信息进行完整性保护。

3）重要数据传输保护机制

重要数据中基准站观测数据、实时差分改正数据需要进行传输。在测评实施

过程中，首先，通过访谈方式了解数据在传输过程中是否使用密码技术进行机密性和完整性保护以及涉及密钥的生命周期管理；然后，通过审查代码片段、查看服务器密码机调用日志、计算签名值或 HMAC 长度是否与声称采用密码算法输出长度一致等方式，确认采用的密码技术，密钥生成、存储和传输保护机制等。

4）重要数据存储保护机制

业务系统应用涉及的重要数据主要包括患者个人隐私信息，以及门急诊、住院、检验检查、互联网诊疗等业务中涉及的费用支付、电子病历等基础医疗卫生信息等。对医疗应用数据、医疗支付数据等重要数据进行存储时，基于密码设备/服务提供的 HMAC-SM3 技术，实现重要数据的存储完整性保护；通过调用密码设备/服务，基于 SM4 对称加密技术，对患者个人隐私信息（电话、住址、身份证、联系人等）等重要数据进行加密保护，确保数据库里的用户身份信息等敏感信息内容不被非法泄露，实现重要数据的存储机密性保护。

在测评实施过程中，首先，通过访谈方式了解数据在存储时是否采用密码技术进行机密性和完整性保护以及涉及密钥的生命周期管理。然后，通过查看服务器密码机的算法配置、审查代码片段、查看服务器密码机调用日志、查看数据库、工具验证测试等方式，确认采用的密码算法、密码技术等是否合规、正确、有效。

4.2.5 安全管理

(1) 测评对象

安全管理包括管理制度、人员管理、建设运行和应急处置四个指标体系。测评对象如表 12 所示。

表 12 测评对象和测评方式

层面（类）	测评对象	测评方式
安全管理	系统相关人员、管理体系（如安全管理制度类文档、操作规程类文档、记录表单类文档、系统相关人员等）、密码应用方案、密钥管理制度及策略类文档、密码实施方案、密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告和整改文档等	☑ 访谈 ☑ 文档审查

(2) 测评实施要点

测评实施主要通过访谈和文档审查，检查管理制度是否全面、规范、合理；访谈系统相关人员，确认人员是否了解并遵守密码相关法律法规、是否正确使用密码相关产品。具体可按照 GM/T 0115-2021 中 6.5 至 6.8 章节描述的测评方法实施测评。

4.2.6 密钥管理

除对密码应用技术要求四个层面和安全管理方面进行测评外，还需要对该场景下的密钥管理安全性进行测评。对于医疗机构业务系统场景，需重点关注门急诊、住院、检验检查、互联网诊疗等涉及的用户/通信实体身份真实性密钥、重要数据传输完整性保护密钥、重要数据存储机密性保护密钥、重要数据存储完整性保护密钥等密钥的全生命周期的安全，包括核实密钥管理使用的密码产品、密码服务是否满足要求，核查密钥管理安全性实现技术是否正确有效等。在核实证书有效性时，应注意核实证书管理的各个环节。

4.3 主要测评结果

结合本指南 4.1、4.2 章节确定的测评指标和测评内容，根据 GM/T 0115-2021 结果判定规则，得出各个测评对象和测评单元的测评结果。进一步从单元间、层面间进行测评和综合安全分析，得出整体测评结果。

由于部分测评对象测评结果的得出需要结合系统具体实现，且测评结果判定依据比较明确，此处不再进行具体描述。本节重点对其中部分测评对象测评结果的判定方法进行分析。

在网络和通信安全层面，如用户端与业务系统之间的通信传输，通过部署具有商用密码产品认证证书的 SSL VPN 安全网关及安全认证网关，使用国密 SSL 套件为用户端和业务系统之间建立安全通道，使用国密 SM2、SM3、SM4 算法，配套由第三方 CA 机构签发的数字证书，实现用户端到业务系统之间的通信实体的身份鉴别以及通信数据的机密性和完整性保护；以上网络通信信道均采用合规的密码产品和密码技术进行通信实体的身份鉴别，保障通信过程中数据的完整性和重要数据的机密性，均符合要求。

在应用和数据安全层面，（1）身份鉴别：通过智能密码钥匙或者协同签名系统，基于 SM2 算法，保证业务系统 PC 端或移动终端用户身份的真实性；（2）重要数据存储的机密性和完整性：通过部署具有商用密码产品认证证书的密码服务管理平台、服务器密码机，使用密码设备/服务实现的基于 SM4 算法的对称加解密功能和基于 SM3 算法的消息鉴别码功能对存储的重要数据进行机密性和完整性保护；（3）不可否认性：通过部署具有商用密码产品认证证书的密码服务管理平台、签名验签服务器或协同签名系统，基于 SM2 数字签名的方式保证业务系统医技护人员处方书写、医嘱书写、护理记录书写、电子病历书写、检验检查诊断报告生成等业务行为的不可否认性；另外，通过部署具有商用密码产品认证证书的时间戳服务器，保证电子病历签署等完成时间的不可否认性。以上均采用合规的密码算法、密码技术、密码产品和密码服务保障应用用户身份和业务重要数据来源的真实性，重要数据存储的机密性和完整性以及用户关键行为的不可否认性，均符合要求。

在整体测评阶段，应依照 GM/T 0115-2021 的整体测评要求，考虑是否存在单元间和层面间的弥补情况，如本指南场景中应用和数据安全层面的重要数据传输的机密性和完整性保护通过网络层的传输保护进行弥补。

在风险分析和评价阶段，应依照 GM/T 0115-2021 的风险分析和评价中的要求执行。另外，可根据安全威胁严重程度、安全威胁发生频率和关联资产价值等方面进行具体分析和评价工作。

4.4 注意事项

在测评过程中需要注意以下事项：

(1) 测评前需明确测评范围和责任主体，且需要重点关注测评对象的选取问题。在实施具体测评时，需根据被测系统的网络安全等级保护定级范围确定被测系统的网络边界和测评范围及具体的测评对象。

(2) 医疗机构业务场景涉及的数据种类繁杂，在实施具体测评时，需与被测方进一步明确重要业务数据的安全需求，如涉及到机密性传输和存储保护的数据范围、涉及到完整性传输和存储保护的数据范围等。

(3) 系统可能采用不同的密码技术实现数据的传输和存储保护，如可能通过

调用智能密码钥匙、软件密码模块、服务器密码机、密码服务管理平台等采用数字签名或 HMAC 等算法进行机密性或完整性保护，应注意在测评实施过程中，应根据不同实现机制采用不同的测评方式。

(4) 对于通过互联网或者其他跨网络使用 VPN 进行运维管理的情况，此时远程管理终端与 VPN 之间的通信信道也应作为网络和通信安全层面的测评对象进行测评。

(5) 系统在实现过程中，可能会采用多种缓解措施降低未使用密码技术带来的安全风险，此时应根据具体场景和实际情况分析缓解措施如何降低风险，判断缓解措施是否有效等。

全民健康信息平台

密码应用与安全性评估实施指南

国家卫生健康委统计信息中心

2023 年 12 月

目 录

前　言

全民健康信息平台作为医疗健康领域重要的民生健康保障，承载着大量的居民个人电子健康档案、电子病历等敏感数据，一旦泄漏或者被窃取、篡改，可能涉及患者生命安全及社会稳定的风险，全民健康信息平台的网络安全问题不容忽视。本指南针对全民健康信息平台惠民服务、业务协同、业务监管及平台基础建设四个典型业务场景，分析业务流程、安全风险及保护对象，给出了用户身份真实性和重要数据来源真实性、关键行为不可否认、通信数据传输安全、基础医疗卫生信息存储安全等四个方面的密码应用设计，并给出了密码应用安全性评估测评内容。

本指南适用于各级卫生健康信息部门开展全民健康信息平台密码应用和安全性评估实施工作，同时可为主管监管部门、第三方测评机构等部门开展全民健康信息平台密码应用的安全监督、检查、评估等工作提供参考。

本指南由国家卫生健康委统计信息中心牵头，北京市卫生健康大数据与政策研究中心、广东省卫健委、广东省卫健委政务服务中心、江苏省南京市卫生信息中心、北京数字认证股份有限公司、广州竞远安全技术股份有限公司、数字广东网络建设有限公司、中国科学院信息工程研究所等多家卫生健康单位和密码相关单位共同开展研究与编制。

术语和定义

下列术语和定义适用于本文件。

- 机密性 confidentiality

保证信息不被泄露给非授权实体的性质

- 数据完整性 data integrity

数据没有遭受以非授权方式所做的改变的性质

- 真实性 authenticity

一个实体是其所声称实体的这种特性，真实性适用于用户、进程、系统和信息之类的实体。

- 不可否认性 non-repudiation

证明一个已经发生的操作行为无法否认的特性。

- 加密 encipherment；encryption

对数据进行密码变换以产生密文的过程。

- 密钥 key

控制密码算法运算的关键信息或参数。

- 密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

- 身份鉴别 identity authentication

证实一个实体所声称身份的过程。

- 消息鉴别码 message authentication code

利用对称密码技术或密码杂凑技术，在秘密密钥参与下，由消息所导出的数据项。任何持有这一秘密密钥的实体，可利用消息鉴别码检查消息的完整性和始发者身份。

- 动态口令 one-time password

基于时间、事件等方式动态生成的一次性口令。

- 访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

缩略语

下列缩略语适用于本文件。

平台：全民健康信息平台

APP：应用程序（Application）

VPN：虚拟专用网络（Virtual Private Network）

PC：个人计算机 (Personal Computer)

ID：身份标识（Identity）

SOA：面向服务的架构(Service-Oriented Architecture)

CA：证书认证机构 （Certificate Authority）

SSL：安全套接层 (Secure Sockets Layer)

IPSec：IP 层协议安全结构 (Internet Protocol Security)

SSH：安全外壳（Secure Shell）

MAC：消息鉴别码 (Message Authentication Code)

HMAC：密钥相关的哈希运算消息认证码（Hash-based Message Authentication Code）

1 场景概述

1.1 背景

建设形成统一权威、互联互通的全民健康信息平台是推进数字中国、健康中国战略的重要信息化保障，是深化“互联网+医疗健康”和医疗健康大数据发展的主要支撑。国家卫生健康委于 2015 年启动国家及省统筹区域全民健康信息平台互联互通工作，并制定了全民健康信息平台互联互通技术方案。2022 年 11 月 7 日，国家卫生健康委、国家中医药局、国家疾控局联合印发的《“十四五”全民健康信息化规划》中指出，到 2025 年，初步建设形成统一权威、互联互通的全民健康信息平台支撑保障体系，基本实现公立医疗卫生机构与全民健康信息平台联通全覆盖。目前，国家级全民健康信息平台已实现与 31 个省（直辖市）和新疆生产建设兵团全民健康信息平台的互联互通。

全民健康信息平台作为医疗健康领域重要的民生健康保障，承载着大量的居民个人电子健康档案、电子病历等敏感数据，一旦泄漏或者被窃取、篡改，可能涉及患者生命安全及社会稳定的风险，全民健康信息平台的网络安全问题不容忽视。本指南以《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》以及《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号）、国务院印发《商用密码管理条例》（国务院令第 760 号）、公安部印发《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960 号）、《关于印发医疗卫生机构网络安全管理办法的通知》（国卫规划发〔2022〕29 号）、《关于印发“十四五”全民健康信息化规划的通知》《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）等法律法规和标准规范中对密码应用的要求为依据，根据全民健康信息平台应用功能指引及建设技术指南，聚焦于医疗健康行业中全民健康信息平台业务场景，促进开展密码应用与安全性评估的实施。

本指南面向对象为国家及省统筹区域全民健康信息平台，网络安全等级保护定级为第三级的系统。

1.2 典型场景介绍

全民健康信息平台作为保障全民健康的信息化工程，目前已覆盖国家及省统筹区域全民健康信息平台互联互通，建立了全员人口、健康档案、电子病历、卫生健康资源等基础数据库，建立了公共服务、医疗服务、医疗保障、药物管理、计划生育、综合管理等业务库，主要业务场景功能介绍如下：

表 1 业务场景功能描述

序号	业务名称	业务场景功能描述
惠民服务		
1	**预约挂号**	为居民提供预约专家号、普通号服务，可以通过健康网站、手机APP等多种方式实现。 **具体功能包括但不限于：**统一号源池管理、医疗机构号源管理、患者身份认证、预约规则管理，预约、挂号流程、医疗机构和专科专家介绍。
2	**智能导诊**	针对患者提供就医导诊的互联网服务，主要是提供给患者安全、可靠、权威的就医指导意见，保障居民合理、有序、安全的就医。 **具体功能包括但不限于：**导诊知识库、症状评估、就诊机构推荐、就诊科室推荐等。
3	**处方流转服务**	为居民提供凭借实体医疗机构或互联网医院开具的电子处方，到药店购药的服务。 **具体功能包括但不限于：**药品目录管理、药品供应商/药店管理、流转方式管理、处方查询、电子处方发药记录等。
4	**统一结算支付服务**	基于居民健康卡整合居民就诊支付渠道，提供覆盖主流在线支付机构（基本/商业医疗保险、银行、第三方支付平台）的统一结算支付服务。 **具体功能包括但不限于：**用户管理、个人用户实名制认证管理、接入机构资质管理、综合分析、线下扫码支付、在线支付、商保理赔、对账服务等。
5	**检验检查报告查询**	居民可以通过区域全民健康信息平台提供的门户网站、手机APP等多种途径，查询近日在区域内医院进行的检验检查报告。

序号	业务名称	业务场景功能描述
		具体功能包括但不限于：报告提醒、报告查询、报告定制与推送等。
6	**互联网+医疗服务**	为居民提供线上医疗服务，通过远程监测和在线咨询服务，让医护人员及时了解患者状况，为患者提供便捷的医疗健康服务。 **具体功能包括但不限于：**在线咨询、在线复诊、护理咨询、在线护理监测、护理指导、健康管理计划、居家护理、用药咨询、处方重整、膳食资讯、随访服务等。
7	**医疗健康资源地图**	为居民提供区域卫生健康服务资源分布地图查询服务。 **具体功能包括但不限于：**服务资源管理、机构基本信息、机构服务信息、机构交通导航等。
8	**家庭医生签约服务**	为居民提供“互联网+家庭医生签约服务”。 **具体功能包括但不限于：**家庭医生团队信息查询、家庭医生签约服务申请与签订、个人及家庭就诊记录查询、家庭医生上门服务记录查询、居民健康咨询、健康常识及惠民活动信息查询。
9	**中医药健康促进**	为居民提供“互联网+中医药健康服务”。 **具体功能包括但不限于：**中医药健康知识宣教、中医疾病预防保健指南、中医疾病预防知识、中医公共卫生常识等。
10	**健康档案查询**	居民通过互联网、自助服务等多种途径，依据居民健康卡等进行身份实名安全认证与有效授权，实现对居民电子健康档案的查询。 **具体功能包括但不限于：**电子健康档案首页、个人就诊记录、检验检查结果、公共卫生服务记录、签约协议、授权查询等。
11	**慢病管理**	为高血压、Ⅱ型糖尿病等慢性病患者提供慢病信息查询、推送服务。 **具体功能包括但不限于：**慢病档案管理、慢病监护、健康数据监测、在线咨询、远程随访、健康体检信息、健康状况信息、健康宣教和日常护理知识等。
12	**接种免疫服务**	为居民提供跨定点机构的在线免疫接种查询、预约服务，为居民提供免疫接种服务提醒和相关知识。 **具体功能包括但不限于：**免疫接种服务提醒、接种记录查询、跨区免

序号	业务名称	业务场景功能描述
		疫接种服务、接种知识定制与推送、接种档案记录。
13	**医养服务**	依托家庭医生签约机制，对社区内医疗护理服务与养老服务资源进行整合，实现区域内各类有需求的老年群体适宜的医疗卫生服务全覆盖。 **具体功能包括但不限于：**养护需求申请、服务计划推送、服务评价、全科医生与养老机构签约、需求评估、服务资源调配、服务计划制定、服务前提醒、服务档案记录、服务质控，服务机构排名等。
14	**用药服务**	面向居民和社区医生提供合理用药与安全用药知识查询服务。针对艾滋病、结核病、高血压、糖尿病、精神疾病等需要长期服药的疾病，面向妇女、儿童、老年人等特定人群提供规范用药提醒服务。 **具体功能包括但不限于：**药品信息查询、规范用药提醒等。
15	**健康教育**	为居民提供基于“互联网+”的健康知识查询、健康教育服务。 **具体功能包括但不限于：**健康评估、信息推送、健康教育资讯服务、健康教育评价。
16	**健康体检服务**	为居民提供从业人员体检、适龄幼儿入园体检相关的机构在线查询、预约服务。 **具体功能包括但不限于：**服务指南、体检机构选择、在线预约、体检项目选择、预约提醒、报告查询等。
17	**生育服务和指导**	为育龄人群提供个性化在线生育技术关怀、指导与服务。 **具体功能包括但不限于：**服务资源查询、在线咨询、服务指导、避孕药具网上配送、生育服务线上登记、出生医学证明在线申领等。
18	**心理健康服务**	为居民提供“互联网+心理健康服务”。 **具体功能包括但不限于：**服务资源查询、知识库、心理科普、心理测评、心理咨询服务等。
业务协同		
19	**院前急救**	打通急救车和医疗机构之间的数据互通共享通道。

序号	业务名称	业务场景功能描述
	业务协同	**具体功能包括但不限于：**患者健康档案、既往病史、过敏记录提取、传输、共享，医疗机构急诊等候时间、手术床位可用状态、血液可用状态查询共享，急救车患者信息采集和传输、生命体征实时监测信息共享、车辆定位等。
20	**分级诊疗协同**	推动机构间和医生间的信息共享和服务协同，为医院间分级诊疗提供信息化支撑。 **具体功能包括但不限于：**分级诊疗签约服务、资源排班、预约规则管理、资源授权、挂号预约、检验检查预约、住院预约、康复预约、处方共享调阅、转诊患者病历共享、医医互动和带教等。
21	**远程会诊协同**	开展远程会诊业务和远程联合门诊协同服务。 **具体功能包括但不限于：**会诊预约、音视频会诊、异步会诊、会诊管理、会诊评价等。
22	**检查检验结果共享协同**	开展区域范围内检查检验结果共享互认。 **具体功能包括但不限于：**检查检验结果互认管理、检查检验结果共享调阅、数据分析等。
23	**区域检查检验服务协同**	开展医疗机构间检验、影像、心电、病理等医疗协同服务。 **具体功能包括但不限于：**医疗机构注册、医务人员注册、标本物流运送、报告智能审核、检查/病理诊断、检查检验报告、检查检验会诊、辅助诊断、服务评价等。
24	**血液安全管理业务协同**	开展血液安全风险监测。 **具体功能包括但不限于：**采血信息采集、血液使用追溯、血库资源调配、血库库存预警、血液安全预警、输血不良反应管理、单采血浆站原料血浆采集、检测、存储、供应等。
25	**中医馆服务协同**	为基层医疗卫生服务机构中医馆提供中医、中西医结合信息化服务。 **具体功能包括但不限于：**中医电子病历、辅助诊断、远程诊疗与教育、中医养生保健治未病、中医辨证论治智能辅助诊疗等。
26	**慢病业务**	为基层医疗卫生服务机构开展慢性病个案处置、随访、干预、评估等

序号	业务名称	业务场景功能描述
	协同	业务提供数据协同支撑。 **具体功能包括但不限于：**慢病报卡、慢病随访填报、辖区新增病例情况查询、全科医生任务推送和全科医生服务计划管理等。
27	**健康促进与教育业务协同**	对健康促进与教育业务在各级健康教育专业机构、基层医疗卫生机构、医院、专业公共卫生机构之间协同联动提供协同支撑。 **具体功能包括但不限于：**健康危险因素和健康素养水平监测、健康科普资源库、个性化健康教育和健康干预、健康教育效果评价等。
28	**妇幼健康业务协同**	推动妇幼健康业务在区域内不同医疗机构之间的协同联动。 **具体功能包括但不限于：**妇女保健信息采集、儿童保健信息采集、产妇分娩信息和出生医学证明信息采集、生育技术服务信息采集、出生缺陷防治信息采集、孕产妇健康服务信息整合、保健服务提示等。
29	**家庭签约与履约协同**	对医生在诊疗或为居民提供其他服务过程中开展履约服务协同提供支撑。 **具体功能包括但不限于：**家庭医生签约、签约服务包管理、履约计划、服务履约、健康随访等。
30	**食品安全防控协同**	对公共卫生部门联合食药监、市场监管部门开展食品在生产、流通和消费领域的安全预防、相关因素分析、突发食源性疾病事件与溯源、食物样本采集与送检、检验检测结果发布等业务提供信息共享和协同防控。 **具体功能包括但不限于：**食品安全风险监测结果分析、食源性疾病溯源、食品样本送检、食品检验检测结果分析等。
31	**疾病控制监测协同**	对医疗卫生机构开展免疫接种、传染病报告、结核病防治、艾滋病综合防治、血吸虫病患者管理、职业病报告、职业性健康监护、伤害监测报告、中毒报告、行为危险因素监测等业务提供信息共享与数据协同支撑。 **具体功能包括但不限于：**疾病诊断与建档协同、疾病分级分组管理与临床路径协同、医院门诊与随访管理协同、医疗体检与随访管理协同、

序号	业务名称	业务场景功能描述
		医疗质量与疾病监管质控协同等。
32	**突发公共卫生事件应急指挥协同**	为突发公共卫生事件应急指挥提供信息和技术支撑。 **具体功能包括但不限于：**应急值班信息、突发急性传染病和突发公共卫生事件监测信息、舆情信息收集、分析与研判；突发公共卫生事件预警信息发布；联防联控工作机制和卫生应急指挥部等会议保障；卫生应急队伍、专家、储备、预案、知识、案例等应急资源的管理；应急能力评估和工作评价等。
33	**药品供应保障监测协同**	对基本药物运行监管和药品供应保障监测提供协同支撑。 **具体功能包括但不限于：**基本药物运行监管、药品使用监测、医保目录药品耗材使用监测、集中采购药品耗材使用监测、处方流转监管、短缺药品预警与协调监测等。
34	**医保业务协同**	通过与医保机构的信息交换和共享，为患者提供异地转诊、异地就医结算服务。包括本地医院出院证明等，为异地医保费用支付提供结算依据。 **具体功能包括但不限于：**本地医院转诊证明、本地医院出院证明、跨区域结算基金流转预警功能信息接口。
业务监管		
35	**医院运营情况监管**	对各级医疗机构的运营情况进行监测与分析。 **具体功能包括但不限于：**资产运营、工作负荷、工作效率、患者负担、医院运行能耗等。
36	**医疗质量情况监管**	开展医院质量监测，对合理用药、诊疗质量、服务规范和患者安全进行监测、警示与追踪评价。 **具体功能包括但不限于：**合理用药监测、医疗服务执行与提示、医院感染情况监测、不良事件监测、临床知识库接口、质量管理指标统计分析等。
37	**互联网医疗服务**	对互联网诊疗、“互联网+护理”、“互联网+药事”等服务进行统一监管。

序号	业务名称	业务场景功能描述
	监管	**具体功能包括但不限于：**机构备案管理、医护备案管理、诊疗服务监管、处方服务监管、医疗费用监管、在线服务评价、异常预警监测等。
38	**检验检查互认业务监管**	对互认的检验检查项目、医疗机构、检查检验报告进行统一监管。 **具体功能包括但不限于：**互认项目管理、互认报告质控、互认标准管理、临床互认监控、互认统计分析等。
39	**远程医疗业务监管**	对各远程医疗服务中心、分中心以及合作医院的远程医疗业务进行统一的监管。 **具体功能包括但不限于：**远程医疗服务中心备案、远程医疗服务分中心备案、合作医院备案、远程医疗专家信息备案、远程医疗服务项目备案、会诊记录个案、远程教育课程信息、远程费用结算信息监管、远程医疗服务质量监管、会诊业务综合统计分析等。
40	**公立医院绩效考核**	对公立医院绩效考核情况进行统一监管。 **具体功能包括但不限于：**考核指标管理、能力提升相关指标监测、创新增效相关指标监测、医疗质量监管、运营效率、持续发展、满意度评价等。
41	**预防接种业务监测**	对预防接种工作开展情况进行监测。 **具体功能包括但不限于：**受种者基本信息和疫苗接种信息登记情况、儿童建卡证情况、国家免疫规划疫苗应种人数和实种人数统计和报告情况、第二类疫苗接种统计和报告情况、群体性接种应种接种人数和实种接种人数统计和报告情况、疫苗出入库和损耗报告统计报告情况、国家免疫规划针对传染病监测报告情况、疑似预防接种异常反应监测报告情况等。
42	**中医药服务项目监管**	对中医药服务项目执行情况进行统一监管。 **具体功能包括但不限于：**中医医疗机构管理、中医药服务项目管理、中医药服务项目查询、中医药服务项目执行数据管理、中医药服务项目质量控制管理、中医药教育数据统计分析及挖掘等。
43	**重点人群健**	对妇幼、老年人等重点人群健康服务情况进行监测。

序号	业务名称	业务场景功能描述
	康服务监测	**具体功能包括但不限于：**重点人群风险管理、重点人群风险地图、妇幼健康服务监测、老年人医养服务监测等。
44	**国家基本公共卫生服务项目监管**	对国家基本公共卫生服务项目开展情况进行统一监管。 **具体功能包括但不限于：**居民电子健康档案建档率、基层医疗卫生服务机构提供的0-6岁以下儿童、孕产妇、65岁及以上老年人、高血压患者、Ⅱ型糖尿病患者、严重精神障碍患者、结核病患者的健康管理，了解健康教育、预防接种服务、传染病和突发公共卫生事件报告和处理、卫生监督协管、中医药健康管理的服务数量等。
45	**基层医疗卫生机构绩效考核监管**	对基层医疗卫生机构相关业务进行统一监管。 **具体功能包括但不限于：**考核指标管理、医疗服务质量数量、患者满意度、任务完成情况、城乡居民健康状况等。
46	**医改进展监测**	对医改实施情况进行监测。 **具体功能包括但不限于：**指标的定义与维护、监测数据收集、指标汇总分析、指标展现等。
47	**卫生服务资源监管**	对卫生服务资源进行统一监管。 **具体功能包括但不限于：**卫生人员统计分析、医疗设施和设备统计分析、事业经费投入统计分析等。
48	**基建装备监管**	对医疗卫生机构业务用房建设和医疗设备等相关工作进行监管。 **具体功能包括但不限于：**业务用房监管、大型医用设备基本情况及相关使用人员监管等。
49	**综合业务监管**	对卫生政策执行、卫生健康人才队伍建设、卫生健康经济管理等开展实时监测。 **具体功能包括但不限于：**卫生健康政策综合分析、卫生健康人力资源综合监管、卫生健康经济综合监管等。
50	**食品安全风险监测**	对食品安全进行统一监测。 **具体功能包括但不限于：**特殊医学用途配方食品监管、食品安全风险监测计划、食品化学污染物及有害因素监测、食品微生物风险监测、

序号	业务名称	业务场景功能描述
		食源性疾病监测、食品安全风险监测质量管理、食品安全风险监测数据汇总分析及预警管理、食品安全风险监测报告管理等。
51	**人口生育支持信息监测**	对人口信息监测关键指标进行对比分析和预警预测。 **具体功能包括但不限于：**人口信息监测、人口自身变动统计分析、人口结构统计分析、人口与发展统计分析、家庭单元信息统计、人口迁移流动评估、育龄妇女生育行为评估、出生人口变动预测、人口生育支持政策辅助决策等。
52	**电子健康码应用监测**	对区域内的电子健康码应用范围、业务广度与深度进行监测。 **具体功能包括但不限于：**分区域、分年度健康码应用实现情况统计与分析，机构码受理环境建设统计与分析，用码情况统计与分析，综合分析与辅助决策，电子健康码应用目录维护管理等。
平台基础建设		
53	**平台主索引**	以居民身份证号码、护照等身份标识作为平台基础服务的主索引，依托电子健康码跨域主索引管理为居民（患者）提供个人身份认证、个人注册基本信息核实服务。 **具体功能包括但不限于：**主索引服务，交叉索引服务，居民个人数据自动匹配关联等。
54	**注册服务**	提供对居民个人、医疗卫生人员、医疗卫生机构、医疗卫生术语等基础共享信息的注册。 **具体功能包括但不限于：**个人注册、医疗卫生人员注册、医疗卫生机构注册、医疗卫生术语注册等。
55	**数据采集与交换**	以集约化建设模式实现平台批量数据采集和个案数据交换，强化数据采集与交换中的数据标准化管理。 **具体功能包括但不限于：**数据采集、数据整合、数据标准映射与转换、文档交换等。
56	**数据质量管理**	提供全生命周期的数据质量管理。 **具体功能包括但不限于：**数据质量管理、数据质量检核执行、数据质

序号	业务名称	业务场景功能描述
		量评价、日常质量监测等。
57	**主数据管理**	提供省统筹区域平台基础数据库、医疗卫生数据、标准规范数据等的规范化管理。 **具体功能包括但不限于：**主数据管理、参考数据管理、文档注册、事件注册、索引服务等。
58	**数据提取分析**	对数据进行提取和深入挖掘分析。 **具体功能包括但不限于：**数据应用开发、数据可视化分析、数据标签管理等。
59	**数据资源中心**	提供省统筹区域平台的数据库存储、跨地域的数据存储/访问服务。 **具体功能包括但不限于：**基础资源库、主题库、专题库、文档库等。
60	**数据资源目录**	基于元数据、信息资源分类、标识符编码和全文检索技术实现信息资源的统一管理。 **具体功能包括但不限于：**元数据管理、文档共享管理、资源目录管理等。
61	**数据资源共享**	通过统一整合梳理信息资源编目，形成资源目录，结合审批流程，对外提供多种资源共享。 **具体功能包括但不限于：**数据规范上报、数据资源共享、资源订阅管理、共享访问控制、API接口池、目录服务、数据存证与审计监管等。
62	**数据分类分级**	通过自动化识别数据格式和业务含义，对数据进行梳理分析、分类分级，为开展数据资产管理、数据安全治理、数据安全防护等提供基础。 **具体功能包括但不限于：**配置管理、业务类型解析、数据分类分级等。
63	**基础设施服务**	为省统筹区域平台提供基础设施相关服务。 **具体功能包括但不限于：**计算资源服务、存储资源服务、网络资源服务等。
64	**平台支撑服务**	为平台上层业务应用提供基础技术支撑及保障。 **具体功能包括但不限于：**数据库服务、大数据平台服务、容器服务、中间件服务、云管理服务等。

序号	业务名称	业务场景功能描述
65	**平台管理**	为全民健康信息平台提供基础管理。 **具体功能包括但不限于：**用户管理、角色管理、权限管理、配置管理、日志管理、监控管理等。
66	**信息安全**	提供身份认证、用户管理和权限控制、审计追踪、通讯 安全、节点认证等手段保证信息安全和隐私保护。 **具体功能包括但不限于：**用户访问管理、不可抵赖性、数据安全传递、数据安全路由、隐私保护、审计追踪、节点与机构认证、平台安全加固等。

全民健康信息平台主要面向医生、护士等医院相关工作者和孕妇、患者、患者家属等就医居民以及参加城乡居民医疗保险等个人，面向卫生健康行政管理部门、基层医疗卫生机构、医院、公共卫生、健康教育等机构开展惠民服务、业务协同、业务监管及平台基础建设等业务应用，实现国家及省统筹区域全民健康信息平台的互联互通。结合以上业务场景功能描述，梳理归纳惠民服务、业务协同、业务监管及平台基础建设四个业务应用的主要功能介绍如下：

（1） 惠民服务

惠民服务主要面向居民个人、医疗卫生人员、医疗卫生机构提供注册、预约挂号、就诊、信息查询等相关业务功能。

1） 居民个人

居民个人用户通过使用健康网站、手机APP等方式登录全民健康信息平台，实现预约挂号、医院科室医生检索、就医体验与评价、远程与医生交流、查询检验检查报告、预约家庭医生及签约、惠民活动查询、医保转诊、就诊支付、电子档案查询、生育登记办理、疾病信息查询、药品信息查询、养护需求申请等业务。

2） 医疗卫生人员

医疗卫生人员用户通过健康网站、手机APP等方式登录全民健康信息平台，面向患者提供就医指导、病人随访、膳食指南、面向跨院医生沟通交流等业务。

3） 医疗卫生机构

全民健康信息平台上注册的医疗卫生机构、预防保健机构等相关机构通过业务专网或 VPN 虚拟专线登录门户网站、手机 APP 实现健康评估、各种疾病的信息推送、信息分级公开、线下药具配送、贫困人口信息采集、信用管理、“治未病”各类健康干预服务数据采集、数据分析与决策等操作管理。

（2） 业务协同

国家全民健康信息平台依托国家电子政务外网、VPN 专网与省级全民健康信息平台实现网络联通，完成数据采集，实现全国各省级平台患者基本信息、就诊信息、电子病历数据，健康档案信息在国家层面的整合集成等业务协同。

省统筹区域全民健康信息平台依托国家电子政务外网或业务专网或 VPN 虚拟专线实现网络全联通；医疗机构和直属单位依托业务专网或 VPN 虚拟专线接入区域全民健康信息平台，实现与全民健康信息平台之间、不同医疗机构之间、国家药管平台之间等的疾病监测业务协同、疾病管理业务协同、突发公共卫生事件应急指挥协同、妇幼健康业务协同、血液安全管理业务协同、院前急救业务协同、分级诊疗协同、出生人口监测业务协同、跨境重大疫情防控协同、药品（疫苗）监管协同、食品安全防控协同等协同业务。

（3） 业务监管

全民健康信息平台依托国家电子政务外网、业务专网、VPN 虚拟专线与不同医疗机构之间进行业务监管，包括但不限于医改进展监测、综合业务监管、卫生服务资源监管、医务人员执业行为监管、传染性疾病管理业务监管、慢病管理业务监管、精神疾病业务监管、预防接种业务监管、妇女保健业务监管、儿童保健业务监管、国家基本公共卫生服务项目监管、食品安全监测业务监管、医院运营情况监管、预约挂号业务监管、检验检查互认业务监管、远程医疗业务监管、卫生监督业务监测、居民健康卡应用监督。

全民健康信息平台依托国家电子政务外网、业务专网、VPN 虚拟专线实现对互联网医疗服务监管平台的监督与管理，重点监管互联网医院医务人员、处方、诊疗行为、患者隐私保护和信息安全等内容。

（4） 平台基础建设

1） 医疗机构层面

医疗机构通过国家电子政务外网、业务专网、VPN 虚拟专线使用 PC 端登录系统，实现向区域全民健康信息平台数据上报。

2） 运营人员层面

全民健康信息平台运营人员（包括平台管理者和平台接入机构的管理者）通过国家电子政务外网、业务专网、VPN 虚拟专线使用 PC 端登录系统，完成医疗卫生术语的注册、维护，全民健康档案服务等管理。

表 2 典型场景业务流程梳理

序号	业务名称	业务流程描述
1	惠民服务	（1） 注册 1） 居民个人注册 居民个人通过 PC 端、移动终端、自助机等多渠道终端→访问全民健康信息平台→提交个人信息数据→根据通过实名制验证的用户信息生成电子健康卡 ID，完成用户注册并建立个人档案。 2） 医疗卫生人员、医疗卫生机构用户注册 医疗卫生人员、医疗卫生机构运营人员通过 PC 端→访问全民健康信息平台→获取医疗卫生人员管理系统、医疗卫生机构管理系统中个人及机构的信息数据→全民健康信息平台返回用户信息进行核验→核验成功，完成用户注册。 （2） 居民个人用户应用 居民个人通过 PC 端、移动终端、自助终端，使用电子健康卡、社保卡及身份证→登录全民健康信息平台→进行预约挂号、医院科室医生检索、就医体验与评价、远程与医生交流、查询检验检查报告、预约家庭医生及签约、医保转诊、就诊支付、惠民活动查询、电子档案查询、生育登记办理、疾病信息查询、药品信息查询、养护需求申请等业务应用→相关数据同步进行存档。 （3） 医疗卫生人员用户应用 医疗卫生人员用户通过 PC 端、移动终端→登录全民健康信息平台→调出居民个人等就诊信息、基本信息、历史病历等进行问诊、就

序号	业务名称	业务流程描述
		医指导等业务。 问诊后，如需检验检查，医疗卫生人员用户开具电子处方及电子医嘱→推送给患者→相关电子处方、电子医嘱等存档至电子病历档案库。 （4） 医疗卫生机构用户应用 医疗卫生机构用户通过 PC 端、移动终端→登录全民健康信息平台→实现健康评估、各种疾病的信息推送、信息分级公开、线下药具配送、贫困人口信息采集、信用管理、“治未病”各类健康干预服务数据采集、数据分析与决策等操作管理。
2	业务协同	（1） 国家与省统筹区域全民健康信息平台之间业务协同 国家级全民健康信息平台通过国家电子政务外网、VPN 虚拟专线，实现数据采集、整合集成等业务协同。 省统筹区域全民健康信息平台，通过国家电子政务外网，上传至国家级全民健康信息平台，实现数据汇聚。 （2） 区域全民健康信息平台之间业务协同 省内区域全民健康信息平台之间通过国家电子政务外网或业务专网或 VPN 虚拟专线，实现省级、市级、县级电子病历共享、业务协同等业务。 （3） 医疗机构和直属单位等与全民健康信息平台之间业务协同 医疗机构和直属单位通过业务专网或 VPN 虚拟专线，实现与全民健康信息平台之间、不同医疗机构之间、国家药管平台之间等的疾病监测业务协同、疾病管理业务协同、突发公共卫生事件应急指挥协同、妇幼健康业务协同等协同业务。
3	业务监管	通过国家电子政务外网、业务专网、VPN 虚拟专线，实现与不同医疗机构之间、互联网医疗服务监管平台的业务监管工作，包括医改进展监测、综合业务监管、卫生服务资源监管、医务人员执业行为监管、医疗行为监管、患者隐私保护和信息安全等业务监督。

序号	业务名称	业务流程描述
4	平台基础建设	（1） 平台运营人员注册 平台运营人员通过PC端→访问全民健康信息平台→提交个人信息数据→全民健康信息平台进行核查→核查成功，完成用户注册。 （2） 医疗机构层面 医疗机构管理者通过国家电子政务外网、业务专网、VPN 虚拟专线→登录全民健康信息平台→实现向区域全民健康信息平台数据上报。 （3） 运营人员层面 全民健康信息平台运营人员（包括平台管理者和医疗机构管理者）通过国家电子政务外网、业务专网、VPN 虚拟专线→登录全民健康信息平台，完成医疗卫生术语的注册、维护，全民健康档案服务等管理。

2 密码应用需求

2.1 风险分析和安全需求

根据以上全民健康信息平台中典型的业务场景分析，可能存在的安全风险和对应的密码应用需求情况如下：

在惠民服务中，包含居民个人、医疗卫生人员、医疗卫生机构用户的注册，居民个人预约挂号、就诊支付等业务，医疗卫生人员就诊指导，医疗卫生机构健康评估、数据采集等业务，此部分涉及居民个人、医疗卫生人员、医疗卫生机构等用户的身份真实性，居民个人及医疗卫生人员行为的不可否性，以及惠民服务中重要业务数据的传输和存储保护需求。

在业务协同中，包含国家及省统筹区域全民健康信息平台之间，全民健康信息平台与医疗机构和直属单位之间的业务协同，此部分涉及共享数据实体身份的真实性和通信数据的传输安全需求。

在业务监管及平台基础建设中，包含全民健康信息平台对不同医疗机构之间的业务监管工作，及平台的医疗卫生术语维护，全民健康档案服务管理等运营工作，此部分涉及重要数据的存储安全需求。

依据业务场景特点，针对各类业务场景梳理主要保护对象如下：

表 3 主要保护对象

序号	相关业务	保护对象	保护对象描述	安全需求
1	惠民服务	用户	全民健康信息平台登录的用户，包括居民个人、医疗卫生人员、运营人员、医疗卫生机构。	☑ 真实性 ☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☐ 不可否认性

序号	相关业务	保护对象	保护对象描述	安全需求
2		用户身份信息	（1） 居民个人用户身份：包括居民姓名、性别、出生年月日、证件号、联系方式、住址信息等； （2） 医疗卫生人员身份包括姓名、性别、出生年月日，证件号、联系方式、住址信息、所在医疗机构名称、科室、职位等； （3） 运营人员身份包括姓名、性别、出生年月日、证件号、联系方式、住址信息、所在医疗机构名称、科室、职位等； （4） 医疗卫生机构身份包括名称、地址、联系方式、组织机构信息等。	☐ 真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 ☐ 不可否认性
3		用户行为	医疗卫生人员、居民个人用户电子病历签署、预约家庭医生及签约、就诊支付等行为的不可否认性、完成时间的不可否认性。	☐ 真实性 ☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☑ 不可否认性
4		其他业务交互数据	费用支付信息； 绩效信息数据； 电子病历等文档数据。	☑ 真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 ☐不可否认性
5	平台基础建	用户	全民健康信息平台登录的用户，包	☑ 真实性

序号	相关业务	保护对象	保护对象描述	安全需求
	设		括居民个人、医疗卫生人员、运营人员、医疗卫生机构。	☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☐ 不可否认性
6		用户身份信息	（1） 居民个人用户身份：包括居民姓名、性别、出生年月日、证件号、联系方式、住址信息等； （2） 医疗卫生人员身份包括姓名、性别、出生年月日，证件号、联系方式、住址信息、所在医疗机构名称、科室、职位等； （3） 运营人员身份包括姓名、性别、出生年月日、证件号、联系方式、住址信息、所在医疗机构名称、科室、职位等； （4） 医疗卫生机构身份包括名称、地址、联系方式、组织机构信息等。	☐ 真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 ☐不可否认性
7		用户行为	医疗卫生人员、居民个人用户电子病历签署、预约家庭医生及签约、就诊支付等行为的不可否认性、完成时间的不可否认性。	☐ 真实性 ☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☑ 不可否认性
8		其他业务交互数据	费用支付信息； 绩效信息数据；	☑ 真实性 ☑ 传输机密性

序号	相关业务	保护对象	保护对象描述	安全需求
			电子病历等文档数据。	☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 ☐ 不可否认性
9	业务协同	共享数据实体	包括国家及省统筹区域全民健康信息平台实体。	☑ 真实性 ☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☐ 不可否认性
10		协同数据	费用支付信息； 绩效信息数据； 电子病历等文档数据。	☑ 真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性 ☑ 存储完整性 ☐ 不可否认性
11	业务监管	共享数据实体	包括国家及省统筹区域全民健康信息平台实体。	☑ 真实性 ☐ 传输机密性 ☐ 存储机密性 ☐ 传输完整性 ☐ 存储完整性 ☐ 不可否认性
12		协同数据	费用支付信息； 绩效信息数据； 电子病历等文档数据。	☑ 真实性 ☑ 传输机密性 ☑ 存储机密性 ☑ 传输完整性

序号	相关业务	保护对象	保护对象描述	安全需求
				☑ 存储完整性 □不可否认性

2.2 业务场景对密码应用的特殊要求

（1） 全民健康信息平台使用对象主要为居民个人、医疗卫生人员、运营人员等用户群体，为确保业务使用的连续性、稳定性，在密码应用设计中，需要充分考虑密码技术在平台应用过程中的响应速度及并发能力，保障平台的服务能力不受影响。

（2） 全民健康信息平台涉及居民个人用户使用场景，在居民个人用户使用电子健康卡、社保卡及身份证方式实现登录平台进行问诊、查询、费用支付等一系列操作时，宜采用身份鉴别、访问控制等技术手段，保障用户网络身份及数据的安全。

3 密码应用实施指南

3.1 典型场景业务的密码应用设计

全民健康信息平台在统一的网络基础设施支撑下，以标准规范体系和安全保障体系为保障，部署统一的全民健康保障数据库，构造统一的目录服务和数据交换体系，搭建统一的应用支撑平台，为公共卫生、医疗服务、医疗保障、药品供应保障、计划生育、综合管理等各类业务提供支撑。

全民健康信息平台总体架构如下图所示：

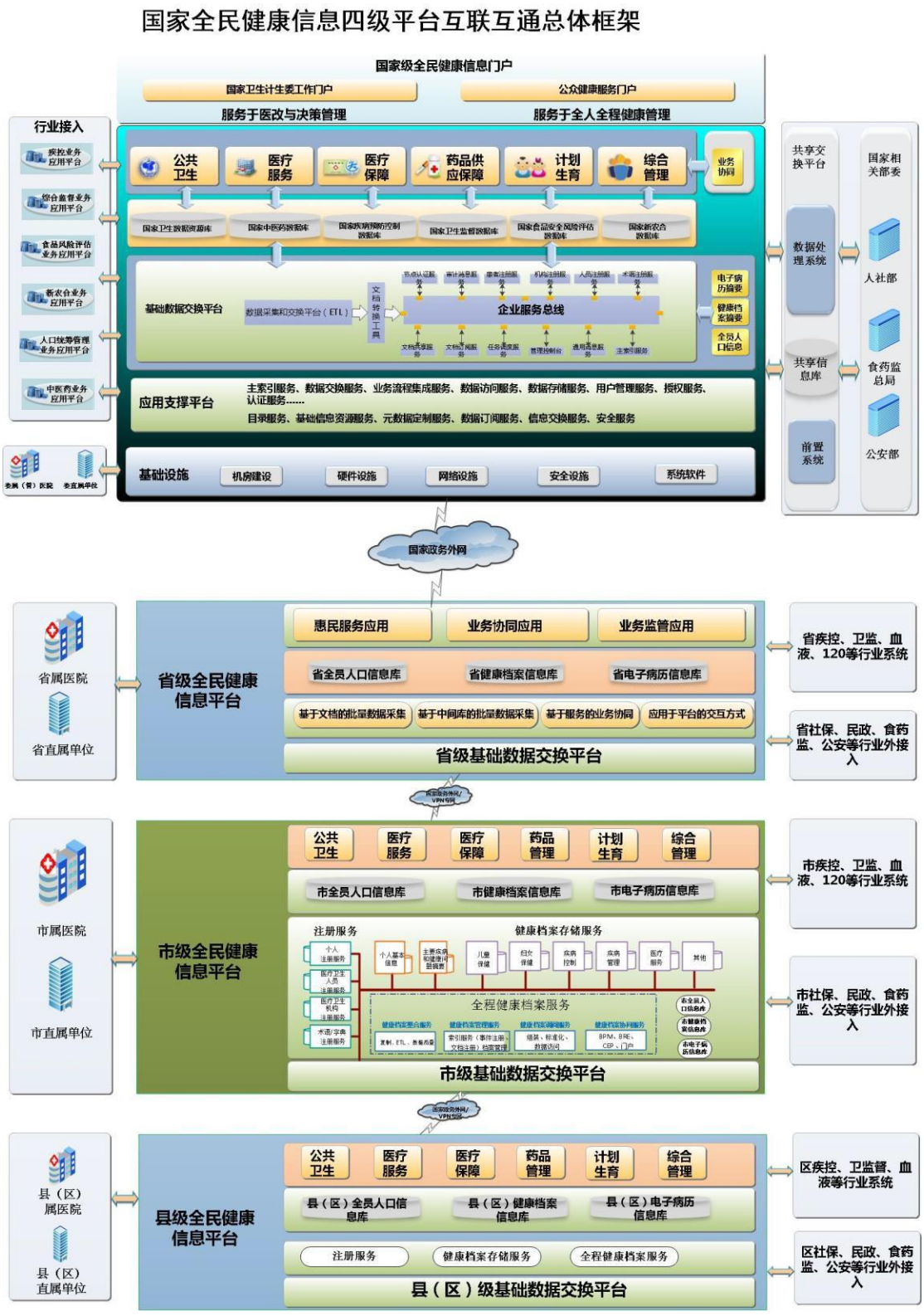

图 3-1 全民健康信息平台总体架构图

结合全民健康信息平台业务特点，本指南重点以用户身份和重要数据来源真实性、用户行为的不可否认性、重要数据传输安全和重要数据存储安全四个方面进行密码应用设计。

3.1.1 全民健康信息平台用户身份真实性和重要数据来源真实性的密码应用设计

（1）用户身份真实性密码应用设计

全民健康信息平台主要涉及居民个人、医疗卫生人员、医疗卫生机构、平台运营人员、平台运维等人员以及平台的身份鉴别需求，其中居民个人的身份认证由于涉及范围大、人员不固定，可采用协同签名技术或其它手段保障居民个人的身份真实性。医疗卫生人员、医疗卫生机构、平台运营人员、平台运维人员等平台工作者以及平台之间登录交互时通过 PC 端以及移动终端两种方式，对此本指南设计了如下两种方案保障用户身份的真实性。

医疗卫生人员、医疗卫生机构、平台运营等人员及平台注册时，提交平台机构或机构人员等相关信息，平台核查后提交第三方电子认证服务机构（简称“第三方 CA 机构”）并核查，通过后签发含有用户数字证书的智能密码钥匙。

图 3-2 身份鉴别示意图

1) PC 端用户身份鉴别

通过在全民健康信息平台机房内部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，为 PC 端用户医疗卫生人员、医疗卫生机构管理者、平台运营人员、平台运维人员、全民健康信息平台配发基于国密算法且符合 GM/T 0027-2014《智能密码钥匙技术规范》的智能密码钥匙，并配合第三方 CA 机构签发的数字证书，采用符合 GB/T 15843.3 的非对称密码算法的身份鉴别方式，基于 SM2 算法的挑战-响应机制实现用户接入的可信身份鉴别。

2) 移动终端用户身份鉴别

通过在全民健康信息平台机房部署符合 GM/T 0028-2014《密码模块安全技术要求》且具备商用密码产品认证证书的协同签名系统、密码服务管理平台为移动智能终端用户居民个人、医疗卫生人员、平台运营人员、平台运维人员等提供协同签名服务，移动 App 集成具备商用密码产品认证证书的移动智能终端安全密码模块，通过调用协同签名系统的协同签名服务，基于 SM2 算法的挑战-响应机制实现移动终端用户的身份鉴别。

（2） 重要数据来源真实性密码应用设计

全民健康信息平台涉及与医保机构、平台之间疾病监控、管理、应急指挥、卫生监督等业务协同，其中包括费用支付数据、绩效信息数据、电子病历等重要业务数据的信息交换和共享，此类数据的来源真实性至关重要，需使用密码技术保障重要数据来源的真实性。

通过在全民健康信息平台机房内部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，利用数字签名、验签技术，使用 SM2 国密算法，保证全民健康信息平台中费用支付、绩效信息、电子病历等重要业务协同数据的来源真实性。

3.1.2 用户关键行为的不可否认性的密码应用设计

全民健康信息平台不可否认性包含医疗卫生人员、居民个人用户电子病历签署、预约家庭医生及签约、就诊支付等行为的不可否认性、电子病历完成时间的不可否认性。

通过在全民健康信息平台机房内部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器或符合 GM/T 0028-2014《密码模块安全技术要求》的协同签名系统、密码服务管理平台，通过签名与验证签名的方式，基于国密 SM2、SM3 算法保证全民健康信息平台医疗卫生人员、居民个人用户电子病历签署、家庭医生签约等行为的不可否认性。另外，可信时间戳签署，通过部署符合 GM/T 0033-2014《时间戳接口规范》的时间戳服务器，保证电子病历签署等完成时间的不可否认性。

3.1.3 通信数据传输安全的密码应用设计

在国家及省统筹区域全民健康信息平台之间业务协同、业务监管、平台基础建设等场景，在平台与其他系统之间，例如医保系统之间电子保单传输等场景，用户依托国家电子政务外网、业务专网、VPN 虚拟专线访问平台场景中，均涉及到重要医疗数据传输安全需求，需采用密码技术保障通信数据的传输安全。

（1） “用户端－平台”之间通信数据传输安全

通过在国家及省统筹区域全民健康信息平台机房内部署符合 GM/T 0024-2014《SSL VPN 技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0028-2014《密码模块安全技术要求》的安全认证网关，通过合规的国密 SSL 算法套件及利用国密 SM2、SM4 算法，为用户端和平台之间建立安全通道，配套由第三方 CA 机构签发的数字证书，实现用户端到平台之间的通信信道通信实体的身份鉴别，通信数据的完整性和机密性保护。

（2） “平台－平台”、“平台与其他系统”之间通信数据传输安全

通过在国家及省统筹区域全民健康信息平台、其他系统机房内部署符合 GM/T 0024-2014《SSL VPN 技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0028-2014《密码模块安全技术要求》的安全认证网关，基于 SSL 协议建立 SSL 隧道，保障业务协同、业务监管等业务环节中，平台到平台之间的通信信道通信实体的身份鉴别，通信数据完整性和机密性保护。

3.1.4 基础医疗卫生信息存储安全的密码应用设计

全民健康信息平台惠民服务、业务协同、业务监管、平台基础建设业务中用户身份信息、费用支付信息、绩效信息数据、电子病历文档等基础医疗卫生信息数据涉及到存储安全需求，采用密码技术保障用户身份信息（身份证号、住址、电话、联系人等）重要数据的存储安全。因费用支付信息、绩效信息数据、电子病历文档等基础医疗卫生信息涉及大量非结构化数据，可采用数据字段加密保护手段进行重要数据的存储安全。

（1） 重要数据存储完整性保护

通过部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，全民健康信息平台在对医疗应用数据、医疗支付数据等重要数据进行存储时，基于服务

器密码机、密码服务管理平台提供的 HMAC-SM3 技术，实现重要数据的存储完整性保护。

（2） 重要数据存储机密性保护

通过部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台、软件密码模块，调用服务器密码机、密码服务管理平台、软件密码模块的数据加密功能，基于 SM4 算法的对称密码技术，对平台用户身份信息（身份证号、住址、电话、联系人等）、电子病历等重要数据进行加密保护，确保数据库里的用户身份信息等敏感信息内容不被非法泄露，实现重要数据的存储机密性保护。

3.1.5 密钥管理

密钥管理包括对密钥的生成、存储、分发、使用、更新、备份和恢复、归档、撤销等全生命周期管理。其中第三方 CA 机构签发的数字证书，用于实现平台用户登录时的身份鉴别及行为不可否认，此类密钥由第三方 CA 机构规范管理，并将相关管理制度补充到密钥管理规范中；对于平台涉及的密钥，例如电子病历、费用支付信息、绩效信息等数据存储、传输、签名私钥等密钥，由全民健康信息平台自建自管，并在密钥管理规范中体现相关管理制度。当数据量较大时，建议采用密钥管理系统实现密钥的生成、存储、分发、使用、更新、备份和恢复、归档、撤销等全生命周期管理。平台涉及的密钥全生命周期管理如下表所示：

表 4 密钥全生命周期管理

密钥名称	生成	存储	分发	使用	更新	备份和恢复	归档	销毁	用途说明
数据传输签名私钥	服务器密码机内部产生	服务器密码机内部存储	私钥不进行分发	在密码模块中进行签名运算	数据库字段定期更新密钥	不涉及	不涉及	密码设备内部进行销毁	数据传输完整性保护
数据传输验签公钥	服务器密码机内部产生	以公钥和证书形式存储	以证书形式分发	在密码模块中进行签名运算	数据库字段定期更新密钥	签名公钥不提供备份恢复机制	不涉及	密码设备内部进行销毁	数据传输完整性保护

密钥名称	生成	存储	分发	使用	更新	备份和恢复	归档	销毁	用途说明
数据传输加密密钥	服务器密码机内部产生	服务器密码机内部存储	分发至客户端	在密码模块中进行加解密运算	数据库字段定期更新密钥	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据传输机密性保护
HMAC密钥	服务器密码机内部产生	服务器密码机内部存储	不涉及	在密码模块中进行验证签名运算	数据库字段定期更新密钥	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据存储完整性保护
数据存储加密密钥	服务器密码机内部产生	服务器密码机内部存储	不进行分发	在密码模块中进行加解密运算	数据库字段定期更新密钥	利用密码设备产品自身的密钥备份、恢复机制实现	不涉及	密码设备内部进行销毁	数据存储机密性保护

3.1.6 安全管理体系建设

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）的要求，从管理制度、人员管理、建设运行和应急处置四个层面制定了相应的制度文件、规章流程，对平台的密码应用安全管理体系进行完备的建设，保障系统规划、建设、后期运维和应急响应的安全性。依据《信息系统密码应用测评要求具体》（GM/T 0115-2021）确定每个安全层面的建设内容，如下表 5 所示：

表 5 安全管理体系建设内容

安全层面	建设内容	内容描述
管理制度	具备密码应用安全管理制度	具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度
	密钥管理规则	根据密码应用方案建立相应密钥管理规则
	建立操作规程	对管理人员或操作人员执行的日常管理操作建立操作规程

安全层面	建设内容	内容描述
	定期修订安全管理制度	定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订
	明确管理制度发布流程	明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制
	制度执行过程记录留存	具有密码应用操作规程的相关执行记录并妥善保存
人员管理	了解并遵守密码相关法律法规和密码管理制度	相关人员了解并遵守密码相关法律法规、密码应用安全管理制度
	建立密码应用岗位责任制度	建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限
	建立上岗人员培训制度	建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能
	定期进行安全岗位人员考核	定期对密码应用安全岗位人员进行考核
	建立关键岗位人员保密制度和调离制度	建立关键人员保密制度和调离制度，签订保密合同，承担保密义务
建设运行	制定密码应用方案	依据密码相关标准和密码应用需求，制定密码应用方案
	制定密钥安全管理策略	根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求
	制定实施方案	按照应用方案实施建设
	投入运行前进行密码应用安全性评估	投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行

安全层面	建设内容	内容描述
	定期开展密码应用安全性评估及攻防对抗演习	在运行过程中，严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改
应急处置	应急策略	制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置
	事件处置	事件发生后，及时向信息系统主管部门进行报告
	向有关主管部门上报处置情况	事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况

3.2 密码产品/服务选择和部署

全民健康信息平台选用的密码产品、算法、技术及服务应符合国家法律法规及密码相关国家标准、行业标准的相关要求。全民健康信息平台主要面向居民个人、医疗卫生人员、医疗卫生机构、平台运营人员、平台运维等人员，通过 PC 端或者移动终端接入系统，密码应用部署如下图 3-3 所示：

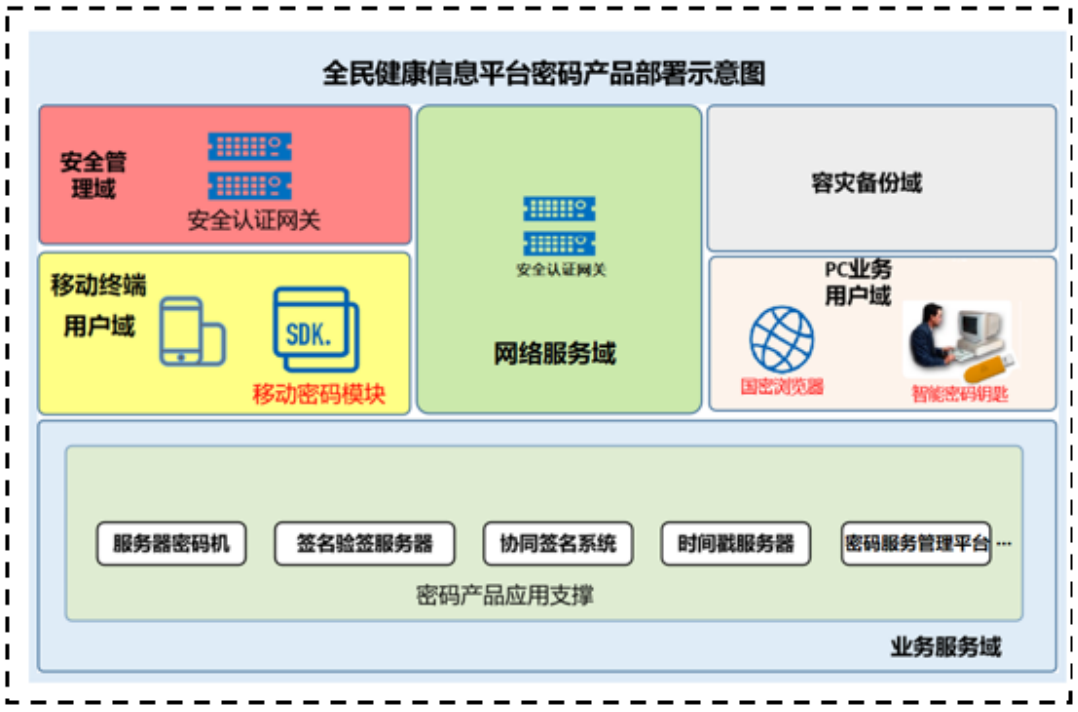

图 3-3 全民健康信息平台密码产品部署示意图

平台中主要的密码产品/服务选择如下所示：

表 6 密码产品/服务

序号	密码产品/服务名称	在场景中提供的密码功能
1	密码服务管理平台	通过将若干密码设备、密码模块按照统一的聚合机制进行池化，搭建密码服务管理平台，引入微服务与虚拟化等技术，通过密码设备、密码安全服务接口进行有效统一管理、配置，密码服务拥有弹性扩展、平行扩容能力，提供丰富的密码服务支撑； 密码服务管理平台具备服务、业务、日志等全链路监控、中间件监控、服务器监控等的智能化能力，实时监控实时报错，便于运营管理； 通过内建多层密钥管理模型，运用应用认证、计算隔离、密钥存储分离、访问授权、全流程审计等技术手段，有效阻断各种攻击路径，对密码应用涉及的各类密钥的全生命周期进行安全管理，符合全民健康信息平台中密钥层次复杂、种类多、数量大等特点需求； 满足全民健康信息平台各层面的用户身份真实性、数据机密性、数据完整性、不可否认性的密码应用需求。
2	安全认证网关	基于密码技术构建安全通道，保证网络通信安全层各级平台之间、平台与医疗机构之间等通信实体的身份鉴别、通信数据的机密性和完整性保护以及网络边界访问控制信息完整性。
3	服务器密码机	为设备和计算安全层提供日志完整性保护。 为应用和数据安全层访问控制信息提供完整性保护。 为应用和数据安全层基础医疗卫生信息等历史存量数据提供存储机密性和完整性保护。
4	签名验签服务器	为应用和数据安全层 PC 端用户提供基于数字证书的身份

序号	密码产品/服务名称	在场景中提供的密码功能
		鉴别服务。 为应用和数据安全层 PC 端用户提供关键行为不可否认性服务。
5	协同签名系统	为应用和数据安全层移动终端用户提供基于数字证书的身份鉴别服务。 为应用和数据安全层移动终端用户提供关键行为不可否认性服务。
6	时间戳服务器	为应用和数据安全层 PC 端用户、移动终端用户关键行为、医疗应用数据提供时间不可否认性服务。
7	智能密码钥匙	用于安全认证网关登录堡垒机身份鉴别。 为应用和数据安全层全民健康信息平台 PC 端用户提供身份鉴别服务。
8	移动智能终端安全密码模块	为应用和数据安全层全面健康信息平台移动终端用户提供身份鉴别服务。
9	国密浏览器	配合安全认证网关实现设备和计算安全层身份鉴别、通信数据完整性与机密性。

3.3 与 GB/T 39786 对照情况说明

对照 GB/T 39786-2021，分析给出全民健康信息平台业务场景密码应用技术层面的密码应用措施见表 7。

表 7 与 GB/T 39786 对照情况说明

安全层面	采取的密码措施
物理和环境安全	全民健康信息平台机房通过使用遵循 GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》的电子门禁系统，电子门禁系统使用 SM4 等算法进行密钥分散，实现门禁卡的一卡一密，并基于 SM4 等算法鉴别人员身份。 全民健康信息平台机房通过选择合适的密码产品（如智能密码钥

安全层面	采取的密码措施
	匙、服务器密码机等），采用 MAC 或数字签名等技术对电子门禁系统进出记录进行完整性保护。 全民健康信息平台机房通过采用专用设备（如服务器密码机、加密存储设备、视频加密系统等），采用 MAC 或数字签名等技术对视频监控系统音像记录进行完整性保护。
网络和通信安全	**（1） “用户端－平台”之间通信数据传输安全** 通过在国家及省统筹区域全民健康信息平台机房内部署符合 GM/T 0024-2014《SSL VPN 技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0028-2014《密码模块安全技术要求》的安全认证网关，通过合规的国密 SSL 算法套件及利用国密 SM2、SM4 算法，为用户端和平台之间建立安全通道，配套由第三方 CA 机构签发的数字证书，实现用户端到平台之间的通信信道通信实体的身份鉴别，通信数据的来源真实性、完整性和机密性保护。 **（2） “平台－平台”之间通信数据传输安全** 通过在国家及省统筹区域全民健康信息平台机房内部署符合 GM/T 0024-2014《SSL VPN 技术规范》、GM/T 0026-2014《安全认证网关产品规范》、GM/T 0028-2014《密码模块安全技术要求》的安全认证网关，基于 IPSec 协议建立 IPSec 隧道，保障业务协同、业务监管等业务环节中，平台到平台之间的通信信道通信实体的身份鉴别，通信数据的来源真实性、完整性和机密性保护。 依赖国密产品安全认证网关自身能力，实现通信信道网络边界访问控制信息完整性。
设备和计算安全	本地机房内的各类通用服务器、安全设备、数据库服务器等设备，均通过堡垒机进行集中运维。运维人员通过安全认证网关登录堡垒机，为全民健康信息平台的运维管理人员发放智能密码钥匙并由第三方 CA 机构签发个人数字证书，使用安全认证网关+堡垒机的方式、基于 SM2 算法的挑战-响应机制实现对运维管理员的身份鉴别。

安全层面	采取的密码措施
	运维人员通过国密浏览器登录安全认证网关，运维路径为：运维人员->安全认证网关->堡垒机->被管理设备，客户端到堡垒机使用安全认证网关构建的国密 SSL 安全通道,保障客户端至堡垒机通信链路的安全；堡垒机到被运维设备采用 SSH2.0 协议构建远程管理安全通道。 通过部署的服务器密码机、密码服务管理平台，对业务日志及审计日志利用 HMAC-SM3 技术进行密码运算，保护日志记录完整性。 堡垒机通过调用服务器密码机、密码服务管理平台的签名服务，利用国密 SM2 算法进行密码运算，实现堡垒机自身的系统访问控制信息完整性。
应用和数据安全	**(1)身份鉴别** 1) PC 端用户身份鉴别 通过在全民健康信息平台机房内部署符合 GM/T 0029-2014 的签名验签服务器、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，为 PC 端用户医疗卫生人员、医疗卫生机构管理者、平台运营人员、平台运维人员配发基于国密算法且符合 GM/T 0027-2014 的智能密码钥匙，并配合第三方 CA 机构签发的数字证书，采用符合 GB/T 15843.3 的非对称密码算法的身份鉴别方式，基于 SM2 算法的挑战-响应机制实现用户接入的可信身份鉴别。 2) 移动智能终端用户身份鉴别 通过在全民健康信息平台机房部署符合 GM/T 0028-2014《密码模块安全技术要求》且具备商用密码产品认证证书的协同签名系统、密码服务管理平台为移动智能终端用户居民个人、医疗卫生人员、平台运营人员、平台运维人员等提供协同签名服务，移动 App 集成具备商用密码产品认证证书的移动智能终端安全密码模块，通过调用协同签名系统的协同签名服务，基于 SM2 算法的挑战-响应机制实现移动端的身份鉴别。

安全层面	采取的密码措施
	(2)访问控制信息完整性 通过调用服务器密码机、密码服务管理平台的 HMAC-SM3 技术保证业务应用系统访问控制策略、数据库表访问控制信息等重要数据的完整性。 **(3)重要数据传输机密性、完整性** 重要数据在平台的应用层传输的场景下，服务端向客户端传输数据时，服务端调用符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，基于 SM2、SM3、SM4 密码算法的数据签名验签、数据加解密技术对平台中需要传输的重要数据实现机密性、完整性保护;客户端向服务端传输数据时,调用客户端密码模块,基于 SM2、SM3、SM4 密码算法的数据签名验签、数据加解密技术对平台中需要传输的重要数据做安全保护，实现重要数据传输的机密性、完整性保护。 **(4)重要数据存储完整性保护** 通过部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台，全民健康信息平台在对医疗应用数据、医疗支付数据等重要数据进行存储时，基于服务器密码机、密码服务管理平台提供的 HMAC-SM3 技术，实现重要数据的存储完整性保护。 **(5)重要数据存储机密性保护** 通过部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机、符合 GM/T 0028-2014《密码模块安全技术要求》的密码服务管理平台、软件密码模块，调用服务器密码机、密码服务管理平台、软件密码模块的数据加密功能，基于 SM4 算法的对称密码技术，对平台用户身份信息（身份证号、住址、电话、联系人等）、电子病历等重要数据进行加密保护，确保数据库里的用户身份信息等敏

安全层面	采取的密码措施
	感信息内容不被非法泄露，实现重要数据的存储机密性保护。 **(6)不可否认性** 通过在全民健康信息平台机房内部署符合 GM/T 0029-2014《签名验签服务器技术规范》的签名验签服务器或符合 GM/T 0028-2014《密码模块安全技术要求》的协同签名系统、密码服务管理平台，通过签名与验证签名的方式，基于国密 SM2、SM3 算法保证全民健康信息平台医疗卫生人员、居民个人用户电子病历签署、家庭医生签约等行为的不可否认性。另外，可信时间戳签署，通过部署符合 GM/T 0033-2014《时间戳接口规范》的时间戳服务器，保证电子病历签署等完成时间的不可否认性。

3.4 注意事项

（1） 基于全民健康信息平台涉及国家及省统筹区域全民健康信息平台之间的互通共享，平台之间存在一定差异性，建议由国家级全民健康信息平台进行统筹密码应用建设规划，省、市、县匹配建设。原则上，国家级、省级全民健康信息平台根据自身特点需要部署密码设备，市、县全民健康信息平台的密码设备部署由省级全民健康信息平台进行统筹建设规划。

（2） 本指南给出的密码应用方案设计具有通用性，具体设计和实施需结合全民健康信息平台及其各子系统的实际情况开展工作。其中需特别注意基础医疗卫生数据的机密性和完整性保护措施，例如居民个人身份证号、电话号、电子病历等内容的机密性和完整性保护，需结合平台实际，在不影响使用的情况下进行密码设计及实施。

（3） 全民健康信息平台包括健康信息平台、区域影像、区域检验、区域心电、基层医疗卫生、基层公共卫生、云平台等众多子系统，其中机房存在自建和云端托管情况。若是自建情况，建议本地进行密码设备部署；若是托管情况，包括云平台密码应用建设，如能进行密码设备部署，应进行密码应用建设，如不能进行密码设备本地部署，则依赖托管厂商或者云服务厂商进行密码应用建设。

（4） 全民健康信息平台涉及大量的居民个人电子健康档案、电子病历等

敏感数据，数据加密保护宜采用冗余部署模式，从而保障平台运行的稳定性、可靠性；同时，平台涉及大数据技术架构，可采用虚拟化密码技术提供高可用、高性能的密码服务能力，支持密码算力弹性伸缩、灵活分配，满足平台大数据密码应用需求。

（5） 各级全民健康信息平台存在与行业接入系统、所属医院、相关直属单位等之间的互联互通，此情况下通信信道的传输安全密码应用设计，依赖全民健康信息平台进行密码应用建设。

（6） 鉴于密钥的作用是保护数据，因此建议密钥保存的时间与数据的保存时间一致。例如电子病历的保存时间是 30 年，则涉及电子病历相关的密钥保存时间同样为 30 年。

4 密码应用安全性评估实施指南

4.1 主要测评指标的选择和确定

4.1.1. 测评范围

鉴于全民健康信息平台涉及国家、省、市、县等不同层级，涉及的用户、接入机构、行业系统、直属单位等较多，且平台由众多子系统组成，因此本指南给出的测评实施并非针对整个全民健康信息平台或者该平台中的某个子系统，仅根据该平台的典型业务特点和通用密码应用设计方案，给出关键安全需求的测评实施指南，供相关方在开展密码应用安全性测评时参考。

4.1.2. 测评指标

选择GB/T 39786-2021中的第三级安全要求作为本指南典型场景测评工作的基本指标。结合前文描述的全民健康信息平台业务情况，GB/T 39786-2021 第三级要求中的个别项并不适用，本指南典型场景的适用测评指标、不适用测评指标及其不适用原因如表 8 所示。

表 8 主要测评指标的选择和确定

类型	指标项			说明
主要适用指标	技术要求	物理和环境安全	身份鉴别	无
			电子门禁记录数据存储完整性	
			视频监控记录数据存储完整性	
		网络和通信安全	身份鉴别	
			通信数据完整性	
			通信过程中重要数据的机密性	
			网络边界访问控制信息的完整性	
		设备和计算安全	身份鉴别	
			远程管理通道安全	
			系统资源访问控制信息完整性	

类型	指标项			说明
			日志记录完整性	
			重要可执行程序完整性、重要可执行程序来源真实性	
		应用和数据安全	身份鉴别	
			访问控制信息完整性	
			重要数据传输机密性	
			重要数据存储机密性	
			重要数据传输完整性	
			重要数据存储完整性	
			不可否认性	
	管理要求	管理制度	具备密码应用安全管理制度	
			密钥管理规则	
			建立操作规程	
			定期修订安全管理制度	
			明确管理制度发布流程	
			制度执行过程记录留存	
		人员管理	了解并遵守密码相关法律法规和密码管理制度	
			建立密码应用岗位责任制度	
			建立上岗人员培训制度	
			定期进行安全岗位人员考核	
			建立关键岗位人员保密制度和调离制度	
		建设运行	制定密码应用方案	
			制定密钥安全管理策略	
			制定实施方案	
			投入运行前进行密码应用安全	

类型	指标项			说明
			性评估	
			定期开展密码应用安全性评估及攻防对抗演习	
		应急处置	应急策略	
			事件处置	
			向有关主管部门上报处置情况	
主要不适用指标	网络和通信安全		安全接入认证	受测场景为等级保护第三级系统，根据 GB/T 39786-2021 对等级保护第三级信息系统的密码应用技术要求，本项应用要求为“可”，且该场景对接入系统的设备无安全接入认证需求，故本指标不适用
	设备和计算安全		重要信息资源安全标记完整性	受测系统未对设备配置重要信息资源安全标记，故本指标不适用
	应用和数据安全		重要信息资源安全标记完整性	受测系统关键业务应用未设置重要信息资源安全标记，故本指标不适用

4.2 主要测评内容

4.2.1. 物理和环境安全测评

(1) 测评对象

该层面的测评对象主要为全民健康信息平台系统所在机房等重要区域及其

电子门禁系统、视频监控系统。该层面确定的测评对象和采用的测评方式如下表9所示。

表 9 测评对象和测评方式

层面（类）	测评对象	测评方式
物理和环境安全	全民健康信息平台系统所在部署机房	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☐ 配置检查 ☐ 工具测试

(2) 测评实施

测评实施时，测评人员应参照 GM/T 0115-2021《信息系统密码应用测评要求》和 GM/T 0116-2021《信息系统密码应用测评过程指南》对全民健康信息平台系统所在机房等重要区域及其电子门禁系统、视频监控系统进行测评。如果被测业务系统部署在多个机房，则相应的机房均应列为测评对象。如果区域平台场景业务系统所在机房由云服务提供商提供，则可以结合有关云平台、云上应用测评的相关指导性文件进行实施。

4.2.2. 网络和通信安全测评

(1) 测评对象

根据本指南中典型场景承载的业务和密码应用设计，分析该层面涉及的测评对象，具体如下：

1） 居民个人、医疗卫生人员、医疗卫生机构人员、运营人员等访问全民健康信息平台

全民健康信息平台涉及不同类别的用户，包括居民个人、医疗卫生人员、医疗卫生机构人员、平台运营人员等，不同类别的用户访问平台的渠道方式不完全一样，如 PC 端、移动终端、自助终端等。该过程涉及的网络层传输保护主要为不同类别的用户访问全民健康信息平台的通信信道，主要包括：PC 端用户与全

民健康信息平台之间的通信信道、移动终端用户与全民健康信息平台之间的通信信道、自助终端用户与全民健康信息平台之间的通信信道。

2） 国家及省统筹区域全民健康信息平台之间业务协同与数据交换共享

如图 3-1 所示，该过程主要涉及国家全民健康信息平台与省级全民健康信息平台实现网络联通；省级、市级、县级全民健康信息平台之间实现网络全联通；医疗机构和直属单位、行业系统等接入各级全民健康信息平台。其中，省级全民健康信息平台分别与省属医疗机构、省直属单位、行业系统、行业外系统之间的通信信道，市级全民健康信息平台分别与市属医疗机构、市直属单位、行业系统、行业外系统之间的通信信道，县级全民健康信息平台分别与县属医疗机构、县直属单位、行业系统、行业外系统之间的通信信道不在本指南考虑范围内，实际测评时，根据系统实际情况决定是否纳入测评对象。

综上所述，该层面可能涉及的测评对象和采用的测评方式如 10 所示。

表 10 测评对象和测评方式

层面 （类）	测评对象	测评方式
网络和通信安全	居民个人、医疗卫生人员、医疗卫生机构人员、运营人员等用户终端访问其所属层级的全民健康信息平台的通信信道	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试
	国家全民健康信息平台与省级全民健康信息平台之间的通信信道	
	省级全民健康信息平台与市级全民健康信息平台之间的通信信道	
	市级全民健康信息平台与县级全民健康信息平台之间的通信信道	
	国家全民健康信息平台分别与行业接入系统、委属医院、委直属单位、共享交换平台等之间的通信信道	

	远程管理通信信道（当远程管理通道跨网时）	

(2) 测评实施要点

测评实施时，测评人员应重点关注网络通信实体身份鉴别、通信数据完整性、通信过程重要数据的机密性、网络边界访问控制信息的完整性等保护需求，可参照 GM/T 0115-2021 中 6.2 章节描述的内容实施测评，测评关键检查点示例如下图所示。

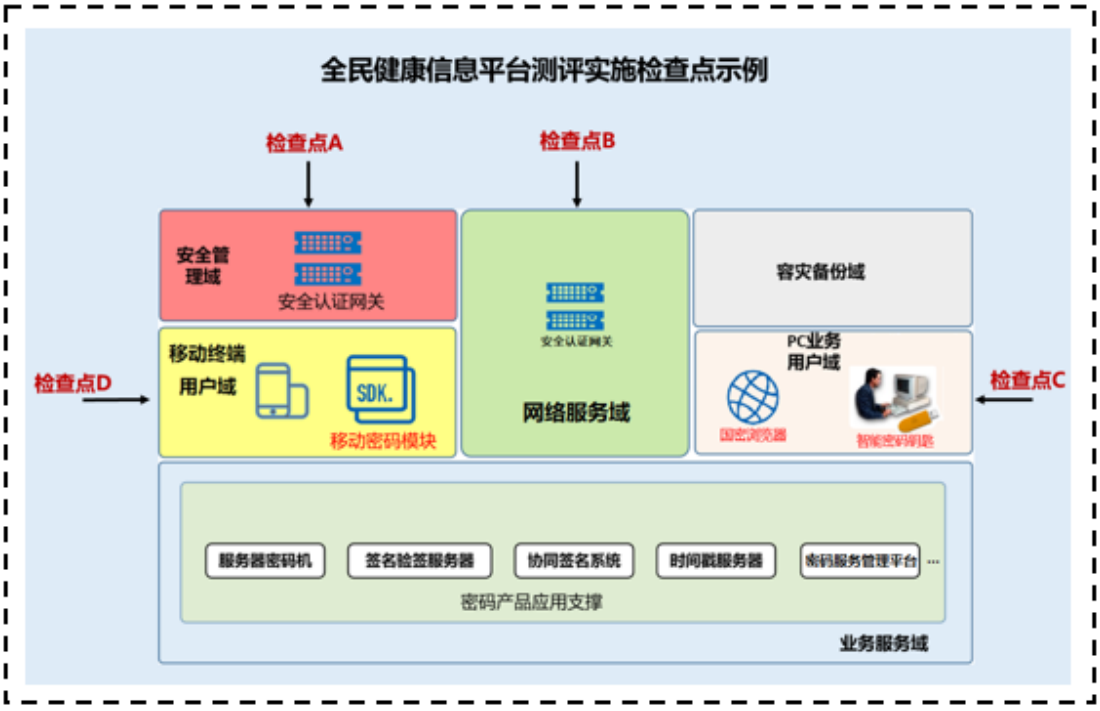

图 4-1 测评实施检查点示例

测评实施要点包括：

1) 核查用于密钥管理和密码计算的密码产品是否符合法律法规的相关要求，需依法接受检测认证的，核查是否经商用密码认证机构认证合格；了解密码产品的型号和版本等配置信息，核查密码产品是否符合密码模块标准中相应安全等级及以上安全要求，并核查密码产品的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件。

2） 检查点 A、B：当被测系统采用网关进行远程管理时，需在网关处使用协议分析工具，抓取远程管理终端与网关之间的通信数据，分析是否采用密码技术保证远程管理通信信道的安全性；当被测系统在网络接入区部署使用 SSL VPN、IPSec VPN 或安全认证网关等 VPN 产品时，在网络接入区的网关处接入协议分析工具，抓取网络接入区与网络边界外通信实体的通信数据，分析是否采用密码技术对通信实体进行身份鉴别、是否采用密码技术保证通信过程中数据的机密性和完整性等。

3） 检查点 C、D：在国家级及省统筹区域全民健康信息平台用户端（如 PC 端、移动端、自助终端等）或服务端使用协议分析工具，分别抓取各级平台用户与各级全民健康信息平台之间的通信数据，分析是否采用密码技术对通信实体进行身份鉴别、是否采用密码技术保证通信过程中数据的机密性和完整性等。

4） 各级全民健康信息平台之间的网络通信检查点：在国家级及省统筹区域全民健康信息平台网络边界处的安全设备（如 VPN 网关等）上使用协议分析工具，分别抓取国家级平台与省级平台、省级平台与市级平台、市级平台与县级平台之间的通信数据，分析是否采用密码技术对通信实体进行身份鉴别、是否采用密码技术保证通信过程中数据的机密性和完整性等。

5） 通过文档审查、配置检查等方式验证是否使用密码技术保护网络边界访问控制信息的完整性等。

4.2.3. 设备和计算安全测评

(1) 测评对象

该层面可能涉及的测评对象和采用的测评方式如下表 11 所示。

表 11 测评对象和测评方式

层面（类）	测评对象	测评方式

设备和计算安全	通用服务器（如应用服务器、数据库服务器）、数据库管理系统、安全认证网关、服务器密码机、签名验签服务器、协同签名系统、密码服务管理平台、时间戳服务器、移动智能终端安全密码模块、堡垒机等	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试

(2) 测评实施

测评指标包括登录设备时采用的身份鉴别方式、远程管理通道安全、系统资源访问控制信息完整性、日志记录完整性、重要可执行程序完整性与来源真实性。鉴于该层面与系统业务关联性不强，因此测评时可按照 GM/T 0115-2021 中 6.3 章节描述的测评方法实施测评。

4.2.4. 应用和数据安全测评

(1) 测评对象

全民健康信息平台包括国家级及省统筹区域信息平台，实际测评时根据被测系统范围确定具体测评对象。例如，如果被测系统为国家级全民健康信息平台，则该层面的测评对象为国家级全民健康信息平台应用；如果被测系统为省级全民健康信息平台，则该层面的测评对象为省级全民健康信息平台应用；如果被测系统为市级全民健康信息平台，则该层面的测评对象为市级全民健康信息平台应用；如果被测系统为县级全民健康信息平台，则该层面的测评对象为市级全民健康信息平台应用。

各级全民健康信息平台应用涉及的用户主要包括居民个人、医疗卫生人员、医疗卫生机构、平台运营人员、平台运维等人员；涉及的重要数据包括应用用户身份信息相关数据，费用支付信息、绩效信息、电子病历等业务交互和协同数据；涉及的关键行为包括医疗卫生人员、居民个人用户电子病历签署、预约家庭医生及签约、就诊支付等。

该层面涉及的测评对象和采用的测评方式如 12 所示。

表 12 测评对象和测评方式

层面（类）	测评对象	测评方式
应用和数据安全	全民健康信息平台应用（各级）	☑ 访谈 ☑ 文档审查 ☑ 实地查看 ☑ 配置检查 ☑ 工具测试

(2) 测评实施要点

测评指标包括用户身份鉴别、访问控制信息完整性、重要数据传输机密性和完整性、重要数据存储机密性和完整性、不可否认性。

测评实施要点包括：

1） 全民健康信息平台用户身份真实性和重要数据来源真实性鉴别机制

首先，采用访谈安全管理人员、查看系统设计文档等方式，了解全民健康信息平台应用用户的身份鉴别和重要数据来源真实性鉴别机制及鉴别过程中涉及密钥的生命周期管理。然后，采用审查代码片段、配置检查和查看日志等方式，对之前获取证据进行确认。

根据系统密码应用设计，平台主要采用如下两种方案保障用户身份的真实性：

a) PC 端用户：通过为用户配发具有商用密码产品认证证书的智能密码钥匙，使用第三方 CA 机构签发的数字证书，基于 SM2 算法的挑战-响应机制实现对用户的身份鉴别。

b) 移动终端用户：在移动终端集成具备商用密码产品认证证书的移动智能终端安全密码模块，通过调用协同签名系统、密码服务管理平台的协同签名服务，基于 SM2 算法的挑战-响应机制实现移动终端用户的身份鉴别。

针对两种不同的鉴别机制，采用不同的具体测评方法。

如果采用 a)方式中描述的使用智能密码钥匙实现身份鉴别，可以通过抓取用户 PC 端与全民健康信息平台服务端的通信数据包，分析是否包含服务端挑战值的签名字段；查看全民健康信息平台的签名验签服务器、密码服务管理平台日志，

查看是否对挑战的签名字段进行了验签操作；查看用户智能密码钥匙的签名数字证书是否符合要求。

如果采用 b)方式中描述的协同签名机制，则可以查看协同签名系统、密码服务管理平台日志和平台配置界面，确认是否执行协同签名操作；抓取移动终端与全民健康信息平台服务端的通信数据包，分析是否包含签名字段；查看协同签名系统、密码服务管理平台的日志，查看是否进行了验签操作。

在重要数据来源真实性测评实施方面，通过抓取传输的费用支付、绩效信息、电子病历等重要业务数据，分析是否采用基于 SM2 算法的数字签名机制进行签名后传输，以及接收方是否进行验签；查看相应签名验签服务器、密码服务管理平台的调用日志，确认是否执行签名验签操作。

2） 访问控制信息完整性

业务应用涉及的访问控制信息可以通过查看数据库、代码实现片段、服务器密码机、密码服务管理平台调用日志等方式检查是否对访问控制信息进行完整性保护。

3） 重要数据传输保护机制

费用支付信息、绩效信息、电子病历等业务交互和协同数据具有传输保护需求。首先，通过访谈方式了解数据在传输过程中是否使用密码技术进行机密性和完整性保护以及涉及密钥的生命周期管理。然后，通过审查代码片段、查看服务器密码机、签名验签服务器、密码服务管理平台等调用日志、计算签名值或 HMAC 长度是否与声称采用密码算法输出长度一致等方式，确认采用的密码技术，以及密钥生成和传输保护机制等。

4） 重要数据存储保护机制

全民健康信息平台应用涉及的重要数据主要包括用户身份信息，以及惠民服务、业务协同、业务监管、平台基础建设业务中涉及的费用支付、电子病历等基础医疗卫生信息等。对医疗应用数据、医疗支付数据等重要数据进行存储时，基于密码设备/服务提供的 HMAC-SM3 技术，实现重要数据的存储完整性保护；通过调用密码设备/服务，基于 SM4 对称加密技术，对平台用户身份信息（姓名、身份证等）、电子病历等重要数据进行加密保护，确保数据库里的用户身份信息

等敏感信息内容不被非法泄露，实现重要数据的存储机密性保护。

在测评实施过程中，首先，通过访谈方式了解数据在存储时是否采用密码技术进行机密性和完整性保护以及涉及密钥的生命周期管理。然后，通过查看服务器密码机、密码服务管理平台的算法配置、审查代码片段、查看服务器密码机、密码服务管理平台调用日志、查看数据库、工具验证测试等方式，确认采用的密码技术，以及密钥生成和存储保护机制等。

4.2.5. 安全管理

(1) 测评对象

安全管理包括管理制度、人员管理、建设运行和应急处置四个指标体系。测评对象如 13 所示。

表 13 测评对象和测评方式

层面 （类）	测评对象	测评方式
安全管理	系统相关人员、管理体系（如安全管理制度类文档、操作规程类文档、记录表单类文档、系统相关人员等）、密码应用方案、密钥管理制度及策略类文档、密码实施方案、密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告和整改文档等	☑ 访谈 ☑ 文档审查

(2) 测评实施要点

测评实施主要通过访谈和文档审查，检查管理制度是否全面、规范、合理；访谈系统相关人员，确认人员是否了解并遵守密码相关法律法规、是否正确使用密码相关产品。具体可按照 GM/T 0115-2021 中 6.5 至 6.8 章节描述的测评方法实施测评。

4.2.6. 密钥管理

除对密码应用技术要求四个层面和安全管理方面进行测评外，还需要对不同

业务场景下的密钥管理安全性进行测评。对于全民健康信息平台系统业务场景，需重点关注惠民服务、业务协同、业务监管、平台基础建设等业务涉及的用户/通信实体身份真实性密钥、重要数据传输完整性保护密钥、重要数据存储机密性保护密钥、重要数据存储完整性保护密钥等密钥的全生命周期的安全，包括核实密钥管理使用的密码产品、密码服务是否满足要求，核查密钥管理安全性实现技术是否正确有效等。在核实证书有效性时，应注意核实证书管理的各个环节。

4.3 主要测评结果

结合本指南 4.1、4.2 章节确定的测评指标和测评内容，根据 GM/T 0115-2021 结果判定规则，得出各个测评对象和测评单元的测评结果。进一步从单元间、层面间进行测评和综合安全分析，得出整体测评结果。

由于部分测评对象测评结果的得出需要结合系统具体实现，且测评结果判定依据比较明确，此处不再进行具体描述。本节重点对其中部分测评对象测评结果的判定方法进行分析。

在网络和通信安全层面，（1）例如，平台用户端-平台服务端之间的通信传输安全，通过部署具有商用密码产品认证证书的安全认证网关，使用国密 SSL 套件为用户端和平台之间建立安全通道，使用国密 SM2、SM3、SM4 算法，配套由第三方 CA 机构签发的数字证书，实现用户端到平台之间的通信实体的身份鉴别以及通信数据的机密性和完整性保护；（2）各级全民健康信息平台之间的通信传输，通过在各级平台机房内部署具有商用密码产品认证证书的安全认证网关/IPSec VPN 网关，基于国密 SSL/IPSec 协议建立安全传输通道，保障业务协同、业务监管等业务环节中平台到平台之间的通信实体的身份鉴别以及通信数据的完整性和机密性保护。以上网络通信信道均采用合规的密码产品和密码技术进行通信实体的身份鉴别，保障通信过程中数据的完整性和重要数据的机密性，均符合要求。

在应用和数据安全层面，（1）用户身份真实性：通过智能密码钥匙、协同签名系统、密码服务管理平台，基于 SM2 算法的挑战-响应机制，保证平台 PC 端或移动终端等用户身份的真实性；（2）重要数据来源的真实性：通过调用签名验签服务器、密码服务管理平台，基于 SM2 算法的数字签名机制保证重要数据来

源的真实性；（3）重要数据存储的机密性和完整性：通过部署具有商用密码产品认证证书的服务器密码机、密码服务管理平台、软件密码模块，使用服务器密码机、密码服务管理平台、软件密码模块实现的基于 SM4 算法的对称加解密功能和基于 SM3 算法的消息鉴别码功能对存储的重要数据进行机密性和完整性保护；（4）不可否认性：通过部署具有商用密码产品认证证书的签名验签服务器、协同签名系统、密码服务管理平台，基于 SM2 数字签名的方式保证全民健康信息平台医疗卫生人员、居民个人用户电子病历签署、家庭医生签约等行为的不可否认性；另外，通过部署具有商用密码产品认证证书的时间戳服务器，保证电子病历签署等完成时间的不可否认性。以上均采用合规的密码算法、密码技术、密码产品和密码服务保障应用用户身份和业务重要数据来源的真实性，重要数据存储的机密性和完整性以及用户关键行为的不可否认性，均符合要求。

在整体测评阶段，应依照 GM/T 0115-2021 的整体测评要求，考虑是否存在单元间和层面间的弥补情况，如本指南场景中应用和数据安全层面的重要数据传输的机密性和完整性保护是否能够通过网络和安全层面的传输保护进行弥补。

在风险分析和评价阶段，应依照 GM/T 0115-2021 的风险分析和评价中的要求执行。另外，可根据安全威胁严重程度、安全威胁发生频率和关联资产价值等方面进行具体分析和评价工作。

4.4 注意事项

在测评过程中需要注意以下事项：

（1） 本指南给出的全民健康信息平台业务场景并非一个独立的网络安全等级保护定级备案系统，而是涉及到国家、省、市、县等不同层级的信息平台，在实施具体测评时，需根据被测系统的网络安全等级保护定级范围确定被测系统的网络边界和测评范围，进而明确具体的测评对象。此外，在测评实施时，还需结合被测系统的实际情况进一步确定被测系统的不适用指标，如安全接入认证等。

（2） 该业务场景涉及的数据种类繁杂，在实施具体测评时，需与被测方进一步明确重要业务数据的安全需求，如涉及到机密性传输和存储保护的数据范围、涉及到完整性传输和存储保护的数据范围等。

（3） 系统可能采用不同的密码技术实现数据的传输和存储保护，如可能通

过调用智能密码钥匙、软件密码模块、服务器密码机、密码服务管理平台等采用数字签名或 HMAC 等算法进行机密性或完整性保护，需注意在测评实施过程中，应根据不同实现机制采用不同的测评方式。

（4） 对于通过互联网或者其他跨网络使用 VPN 进行运维管理的情况，此时远程管理终端与 VPN 之间的通信信道也应作为网络和通信安全层面的测评对象进行测评。

（5） 系统在实现过程中，可能会采用多种缓解措施降低未使用密码技术带来的安全风险，此时应根据具体场景和实际情况分析缓解措施如何降低风险，判断缓解措施是否有效等。