数字认证·共建可信任的数字世界

构建安全可信的医院网络空间

沈 雷

目 录

CONTENTS

一、医疗网络空间面临的安全风险与需求

二、国家法律规范高度重视医院安全可信问题

三、构建医院安全可信网络空间的框架思路

医院信息化建设进入新时代

✓ 无纸化

✓ 协同化

✓ 互联网+

✓ 大数据

数字认证 | 共建可信任的数字世界

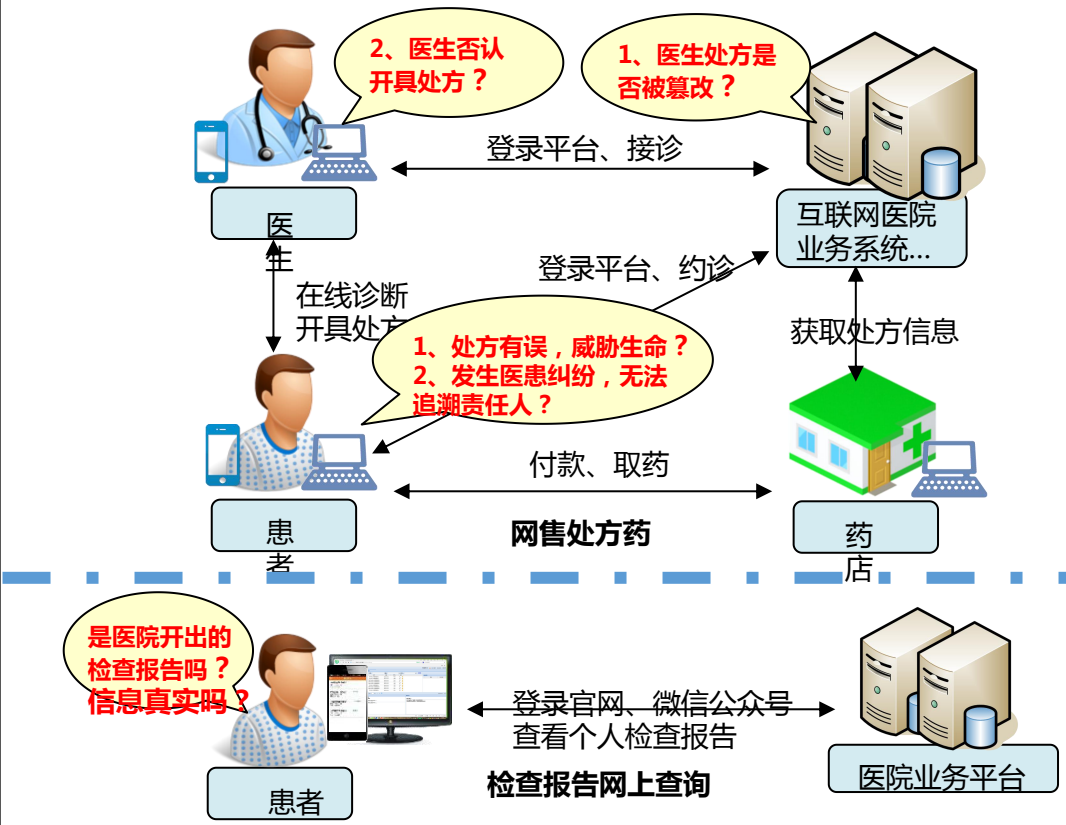
数字化、无纸化不可避免面临合法可信问题

- ✓ 节省病案管理以及纸张耗材成本
- ✓ 减轻医生工作量，提高检查效率
- ✓ 规范检查诊断秩序
- ✓ 优化就医流程

- 电子病历是否真实、可信？
- 电子病历责任归属是否明确？
- 一旦发生医疗纠纷，电子病历是否具备法律效力？

HNSF
Health Network Security Forum 2017
医疗网络安全论坛

“互联网+医疗”蓬勃发展，安全风险凸显



医生、机构真实性问题

医生执业身份？医疗机构资格？

患者身份？

数据安全问题

数据完整可信？

隐私得到保护？

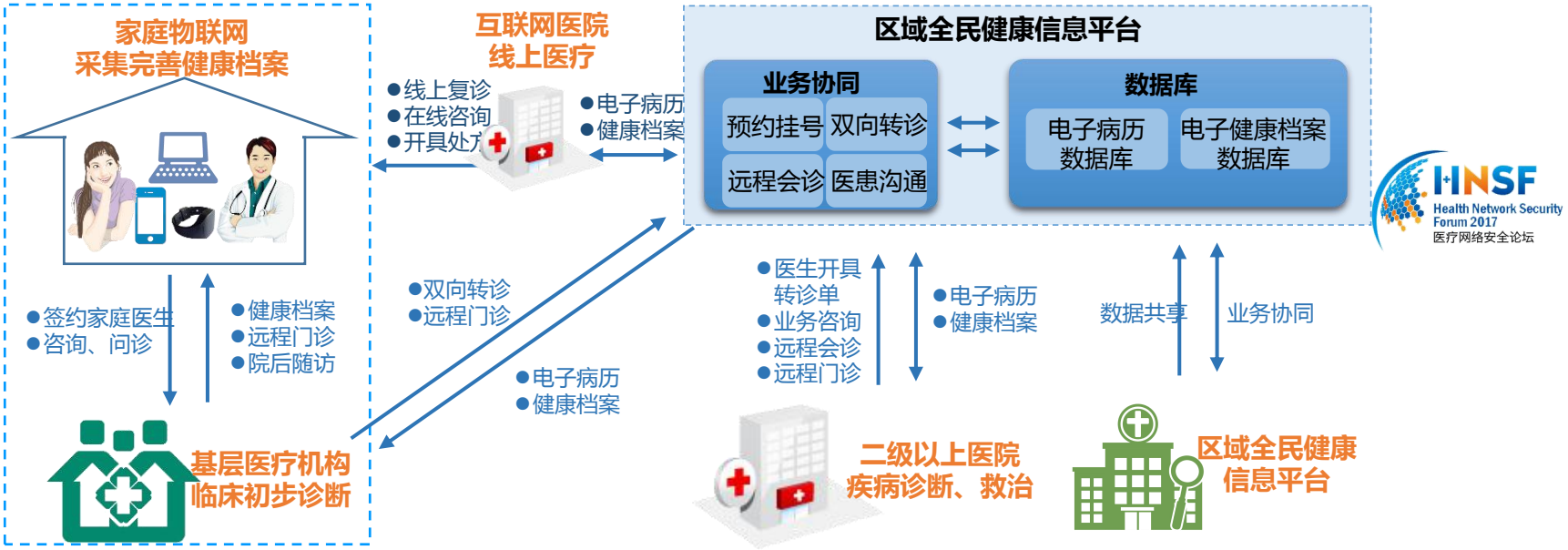
医疗质量安全问题

医疗行为全程可追溯？

HNSF Health Network Security Forum 2017 医疗网络安全论坛

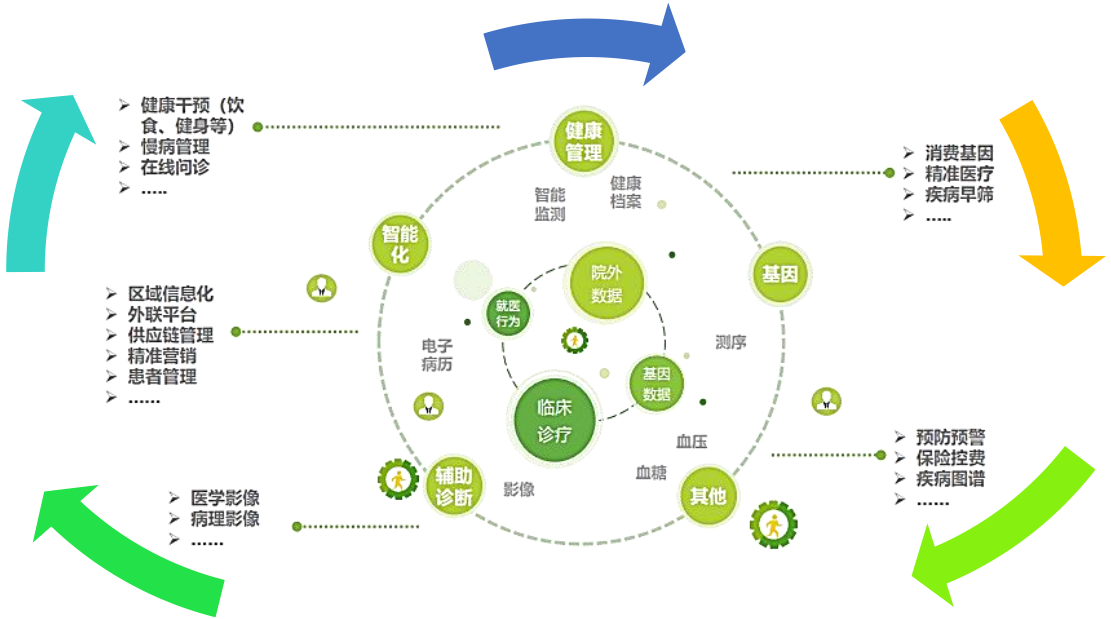
医疗健康业务协同快速发展，安全威胁加剧

分级诊疗、医药流通、医疗供应链、综合管理……



数据传输共享安全？接入的设备/系统安全可信？协同行为责任可追溯？

医疗健康大数据利用面临安全挑战



流动的健康医疗大数据

产生

共享

存储

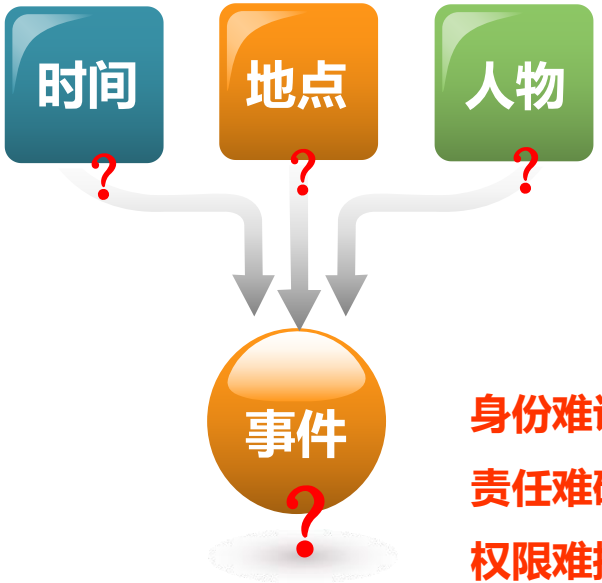
利用

冒用！

泄露！

篡改！

空间安全运行的基本要素面临挑战



身份难识别

责任难确定

权限难控制

隐私难保护

医疗网络空间的安全可信需求

参与各方数字身份可信可管

保证医生、患者、机构、系统、接入设备等各方**数字身份可信，**医生、机构的**执业与资格身份可信，**医生**“人证合一”**，各方**权限可控**。

可信身份管理
访问权限管理

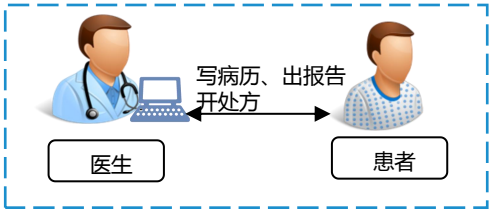
数据全生命周期安全可信

在医疗数据产生、传输、存储、挖掘、应用、运营等全生命周期环节中，保证**数据真实、完整、可信、机密、隐私不被泄露**。

全生命周期数据安全可信

服务和管理行为可追溯

在医生写病历、开处方等医疗服务行为过程中，一旦出现问题，保证**医生行为可追溯**。



诊疗行为责任可溯

用户访问行为可管、可控、可追溯
医疗健康数据自始至终可信、安全

密码技术是保障网络空间安全的基础性核心技术

HNSF Health Network Security Forum 2017 医疗网络安全论坛

目 录
CONTENTS

一、医疗网络空间面临的安全风险与需求

二、国家法律规范高度重视医院安全可信问题

三、构建医院安全可信网络空间的框架思路

国家出台政策推进国产密码应用

2015年两办4号文：

到2020年 ——在政务信息系统、基础信息网络、重要信息系统、重要工业控制系统实现国产密码全面应用；

——国产基础软件全面支持国产密码，国内使用的国外基础软件产品支持国产密码有突破进展；

——依法形成商用密码应用监管体系，对密码使用行为进行规范。

到2030年 ——国产密码在国内各行业得到全面应用；

——建成安全、规范、可靠、易用的密码服务体系；

——形成完善的商用密码应用监管体系。

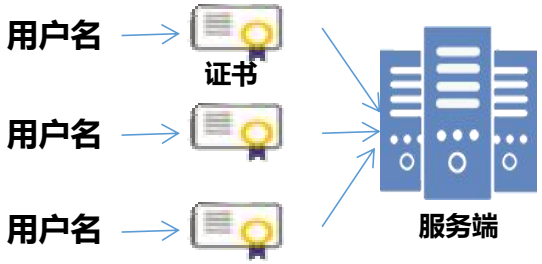
HNSF
Health Network Security Forum 2017
医疗网络安全论坛

2018年两办36号文：

加强全民健康保障信息化密码应用，构建卫生健康领域密码支撑体系。

构建卫生健康领域密码支撑体系。在医疗服务、医疗保障、医疗管理等卫生健康应用，以及全民健康信息化平台、医疗卫生电子证照、居民电子健康档案、电子病历、居民健康卡、医疗保障信息系统、分级诊疗信息系统、基础资源信息数据库等信息化系统中实现商用密码全面应用。

什么是合法合规的电子签名



将证书放在服务端或PC端统一管理不符合电子签名法要求

1.不被国家认可，会在各种评审时遭专家质疑，影响医院评审；

2.有风险的证书应用行为，会被相关机构叫停整改；

3.不合规的签名行为，医患纠纷时医院会败诉。

电子签名同时符合下列条件的，视为可靠的电子签名：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；”

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现

——《电子签名法》第十三条

可靠的电子签名与手写签名或者盖章具有同等的法律效力。

——《电子签名法》第十四条

用户名+口令无法实现电子签名

- **口令不是密码**。口令对应的英文单词是Password、PIN等，密码对应的英文是cryptography。密码是密码算法、密钥管理和密码协议的总和，通过密码算法、密钥管理和密码协议，共同实现明密变换或者安全认证。
- 用户名口令只能作为一种安全性很低的登录认证方式，无法实现电子签名，更无法实现符合《电子签名法》规定的“可靠电子签名”。

HNSF
Health Network Security Forum 2017
医疗网络安全论坛

合法可信是病历无纸化的关键

《关于印发医疗质量安全核心制度要点的通知》（国卫医发〔2018〕8号）

- 病历管理制度：“鼓励推行病历无纸化”
- 信息安全管理制度：“医疗机构应当确保实现本机构患者诊疗信息管理全流程的安全性、真实性、连续性、完整性、稳定性、时效性、溯源性。”

行业陆续推出数字签名应用规范指导医疗机构数字签名合规应用

《电子病历应用管理规范（试行）》

第十条 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的法律效力。

《医学电子文档数字签名技术规范》（行标，预计今年6月份正式发布）

《电子病历数字签名应用规范》（行标，预计今年6月份正式发布）

《医院电子病历数字签名实施指南》（已出版）

电子病历应用水平分级评价对安全可信的要求

- 所有公立医院都要参加电子病历评级，电子病历评级纳入三级医院的考核指标
- “智慧服务”与电子病历评级二者有机衔接，只有电子病历应用达到4级，才能与智慧服务相匹配

（1）可记录和存储就诊患者医疗机构内外的医疗及健康信息 （2）可记录和存储全国专病的注册登记信息及电子病历数据，数据内容具备代表性，可支持权威知识库的研发	8
无电子身份认证	0
专用的医疗信息处理系统有身份认证	1
（1）各个系统均有身份认证功能 （2）临床应用的电子病历系统（住院医师站、门诊医师站、护士站）可用相同用户与密码进行身份认证	2
重点电子病历相关系统（门诊、病房、检查与检验系统）对同一用户可用相同用户与密码进行身份认证	3
医疗相关的所有系统对同一用户可采用相同的用户与密码进行身份认证	4

（1）重点电子病历相关记录（门诊、病房、检查、检验科室产生的医疗记录）有统一的身份认证功能 （2）重点电子病历相关记录（门诊、病房、检查、检验科室产生的医疗记录）的最终医疗档案至少有一类可实现可靠电子签名功能	5
（1）所有医疗记录处理系统产生的最终医疗档案具有可靠电子签名 （2）最终医疗档案的电子签名记录中有符合电子病历应用管理规范要求的时间戳	6
（1）全部电子病历系统在数据产生过程可实现可靠电子签名，如每个医嘱、每段病程记录、每个阶段的检查报告等 （2）全部医疗记录的电子签名记录中有符合电子病历应用管理规范要求的时间戳	7
有医疗信息交换与共享相关的医疗机构之间的电子病历中的电子签名可互认	8

安全可信是互联网医疗有序开展的基础保障

《关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26号）

- 强化医疗质量监管：“推进网络可信体系建设，加快建设全国统一标识的医疗卫生人员和医疗卫生机构可信医学数字身份、电子实名认证、数据访问控制信息系统，创新监管机制，提升监管能力。”

类别	核心要求	管理规范条款
可信身份要求	推进**网络可信体系建设**， 实现医务人员**电子实名认证、数据访问控制**	**《互联网诊疗管理办法（试行）》**第十四条 **《互联网医院管理办法（试行）》**第十六条
可信数据要求	在线开具的处方必须有**医师电子签名，**互联网诊疗活动**全程留痕、可追溯、防泄漏**	**《互联网诊疗管理办法（试行）》**第十八、二十四条 **《互联网医院管理办法（试行）》**第二十条

目 录

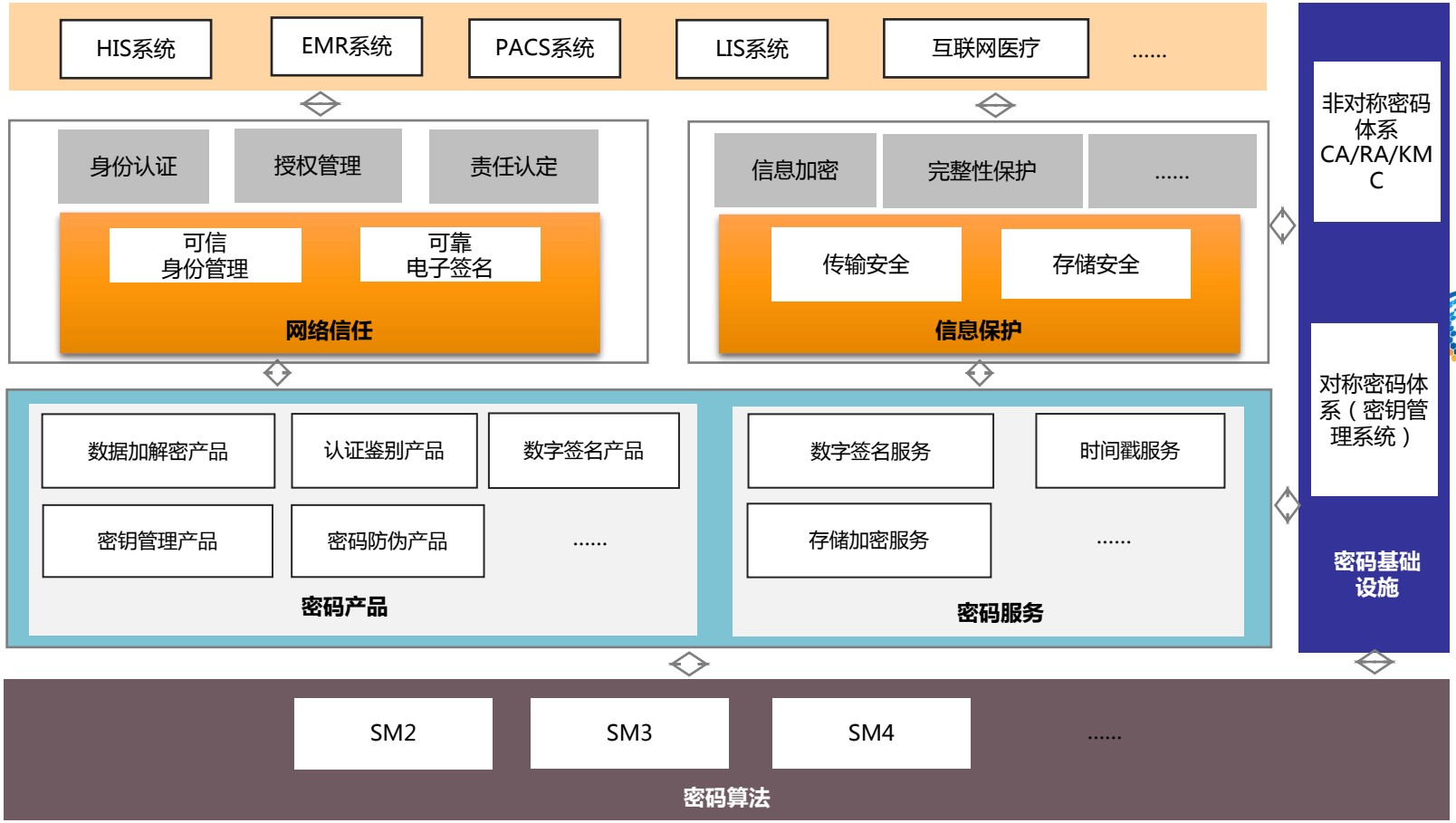
CONTENTS

一、医疗网络空间面临的安全风险与需求

二、国家法律规范高度重视医院安全可信问题

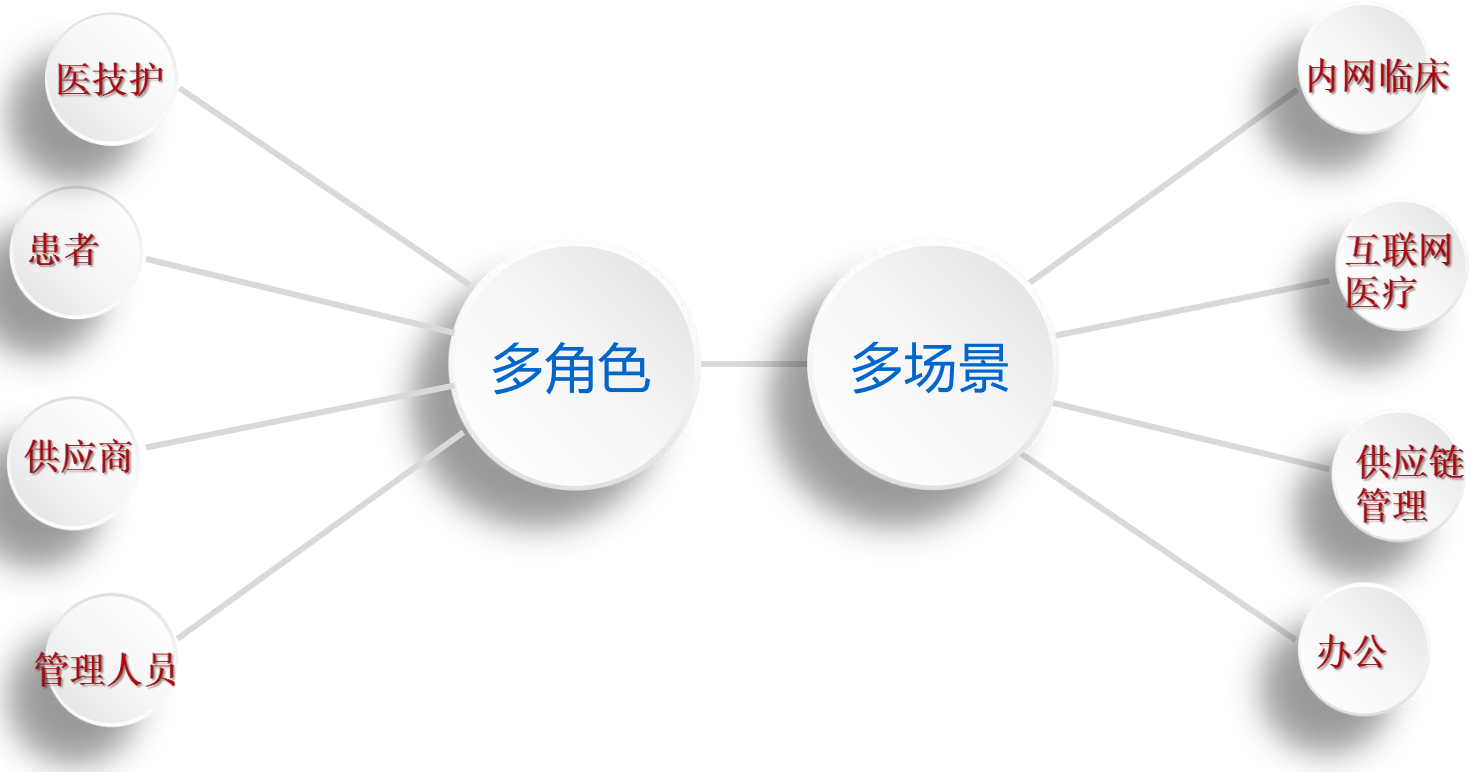
三、构建医院安全可信网络空间的框架思路

电子病历密码应用总体框架



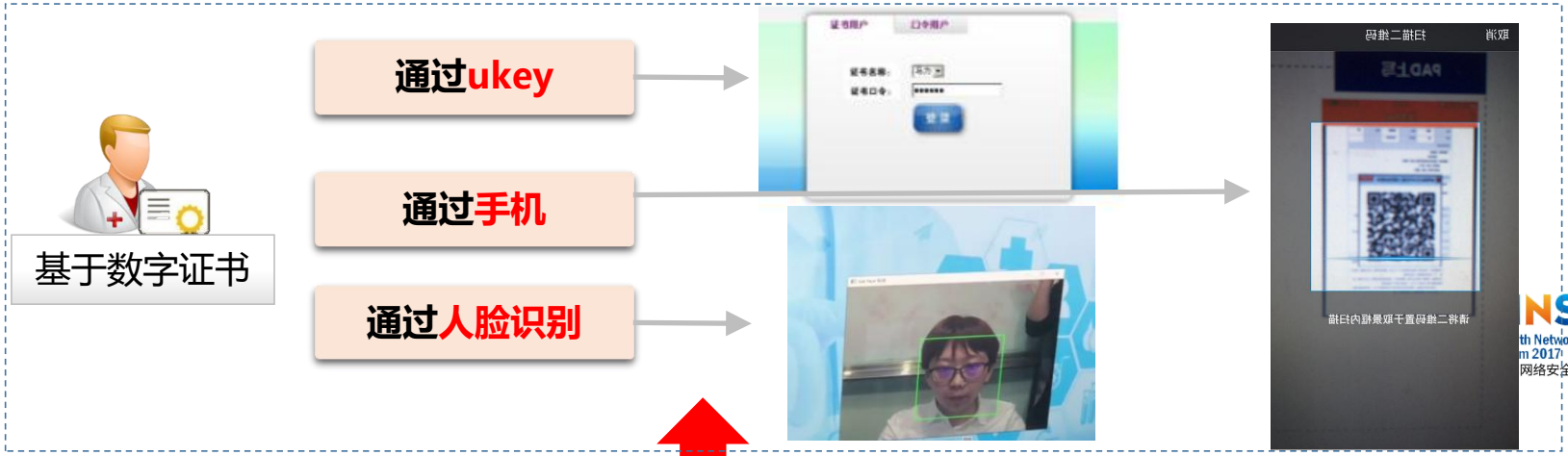
HNSF Health Network Security Forum 2017 医疗网络安全论坛

涵盖多场景、多角色



HNSF Health Network Security Forum 2017 医疗网络安全论坛

医患可信数字身份


通过ukey
通过手机
通过人脸识别
基于数字证书


实名核验
实人核验
实证核验
CTID
网证核验
基于数字证书
公安CTID平台

医技护电子签名

涉及各类电子病历：

- 门(急)诊病历记录
- 门诊处方
- 住院病程记录
- 医嘱单
- 护理记录
- 会诊意见记录
- 手术记录
- 检验报告单
- ……

- 为医生、护士等颁发**数字证书**，实现身份可信，确保身份认证；
- 部署集成应用**身份认证、数字签名、时间戳、电子签章**等产品，实现诊疗服务过程可靠电子签名应用。

PC终端签名场景：

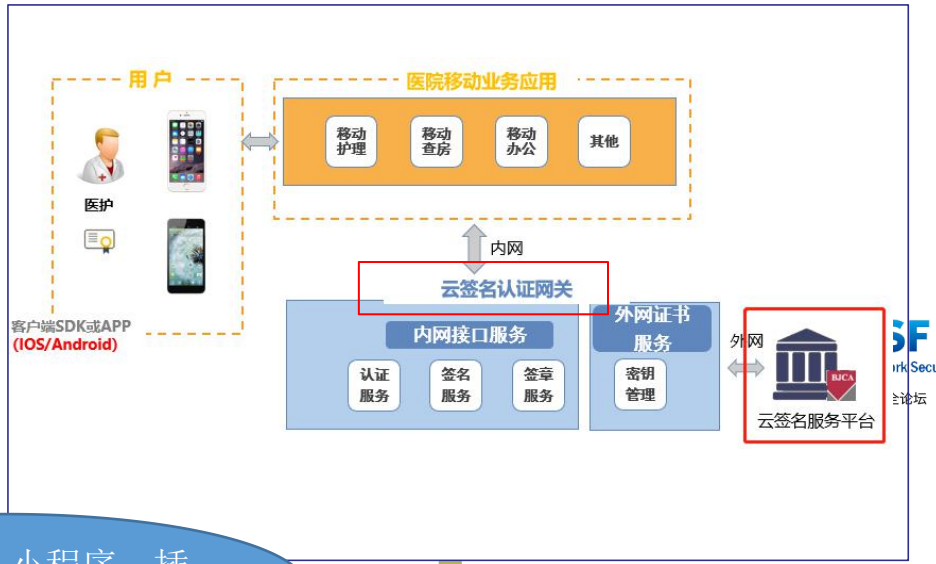
医生、护士工作站、各科室使用**USBKey**在PC终端完成电子签名。

移动终端签名场景：

平板、手机

HINSF Health Network Security Forum 2017 医疗网络安全论坛

医护移动电子签名



SDK、APP、小程序、插件等多种方式

应用背景：医院网络禁止外联，院内应用

服务方式：本地服务模式

应用场景：院内基于移动端开展的业务

应用产品：移动SDK、终端与服务器**协同签名服务系统**（硬件）

应用背景：医院应用可连接互联网服务，云服务

服务方式：云服务模式

应用场景：院外手机安全登录、院外手机流程审批、院外手机签名

应用产品：移动SDK、云签名认证服务网关、云签名服务平台

患者手写电子签名

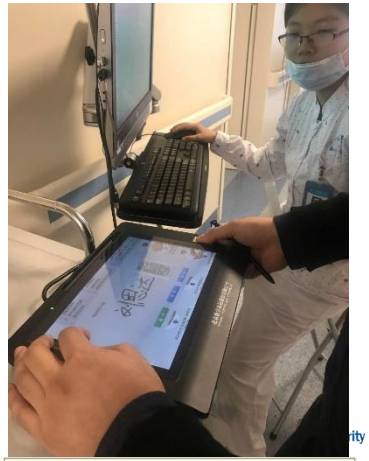
BJCA发明专利

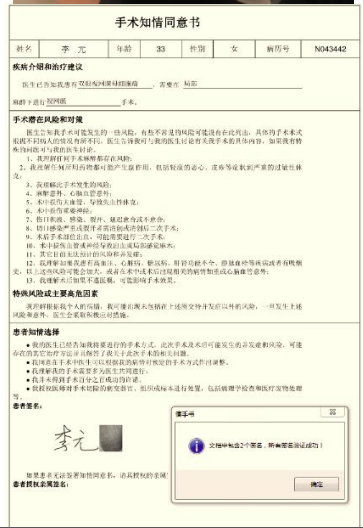
- 电子知情同意书原文
- 时间、地点
- 身份信息
- 指纹、照片
- 手写签名笔迹采集

可靠电子签名

具备法律效力的电子协议

医疗纠纷中作为电子证据使用





手术知情同意书

姓名	李 元	年龄	33	性别	女	病历号	N043442

疾病介绍和治疗建议

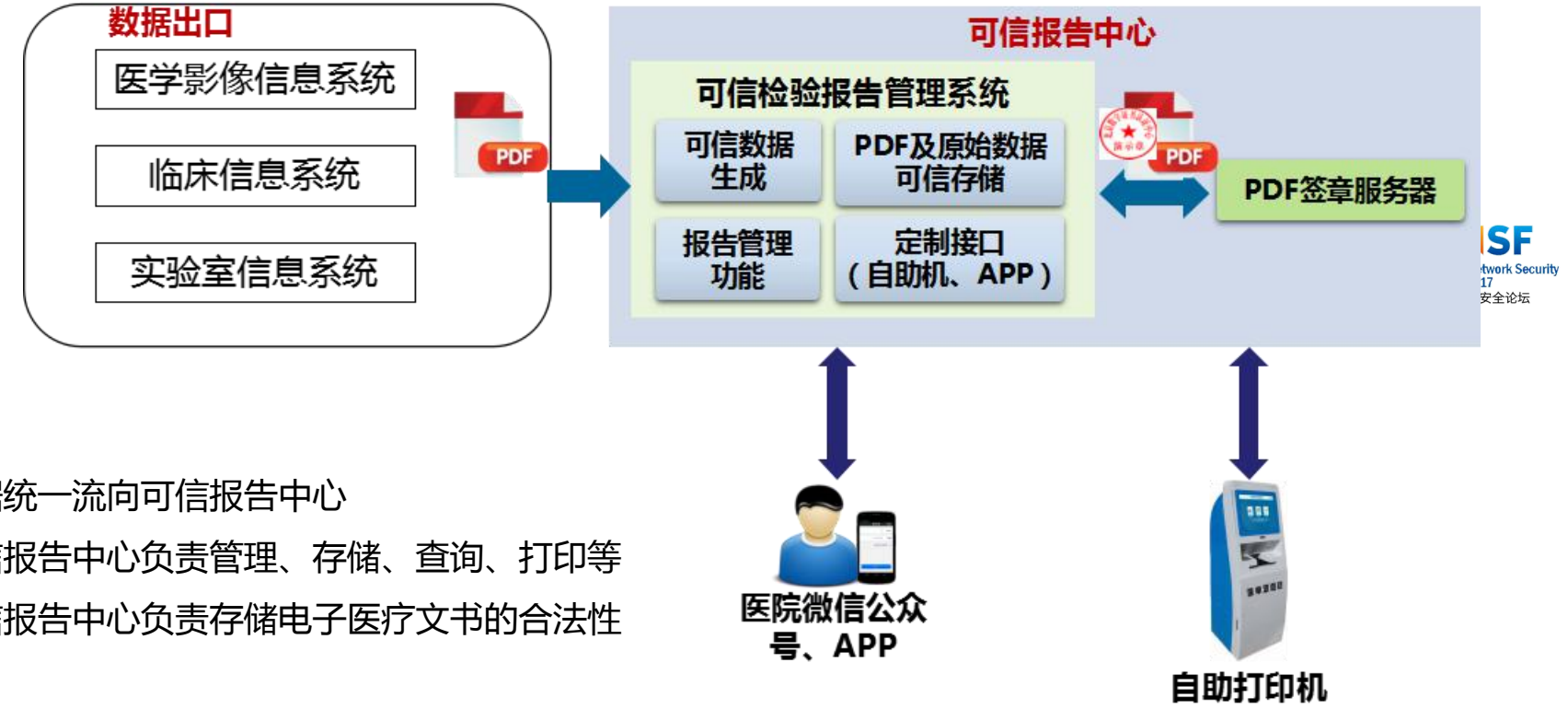
手术潜在风险和对策

特殊风险或主要高危因素

患者知情选择

患者签名：

检查检验报告可信中心

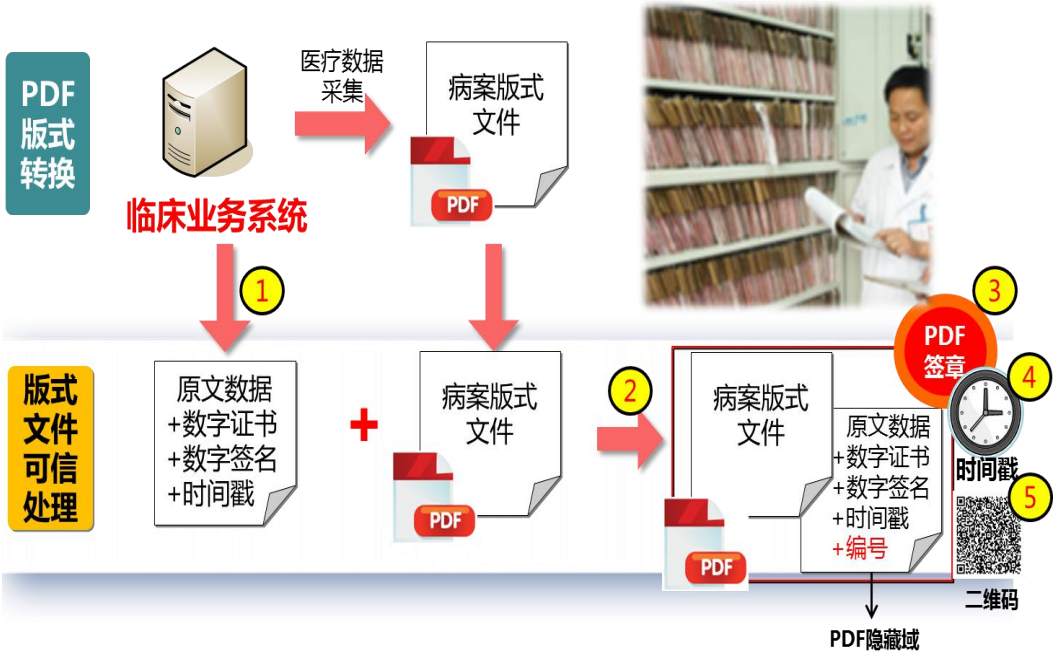


1.数据统一流向可信报告中心

2.可信报告中心负责管理、存储、查询、打印等

3.可信报告中心负责存储电子医疗文书的合法性

电子病案归档电子签名



可信可管理

电子病历归档数字签名的要求：

- ✓ 电子病历归档前应通过数字签名服务系统验证待归档电子病历中所含数字签名数据的有效性，保障电子病历内容的真实性、完整性；
- ✓ 数字签名验证成功后，由病案室（医疗机构）对符合归档标准的电子病历执行数字签名。

可信电子病案管理建设

如何做到可信

归档前

- 建立索引
- 电子病历采集
- 扫描
- 扫描录入

归档中

- 质控
- 返修
- 回收、归档
- 编目

归档后

- 打印
- 科研借阅
- 临床借阅
- 上报信息

- 签名信息采集
- 签名补全
- 版式文件转化
- 扫描质量评测采集
- 日志采集

- 档案标准化
- 签名验证
- 版本管理
- 归档签名
- 全流程日志

- 水印、防拷屏
- 保密级别
- 隐私保护
- 第三方保全
- 访问控制
- 全流程日志

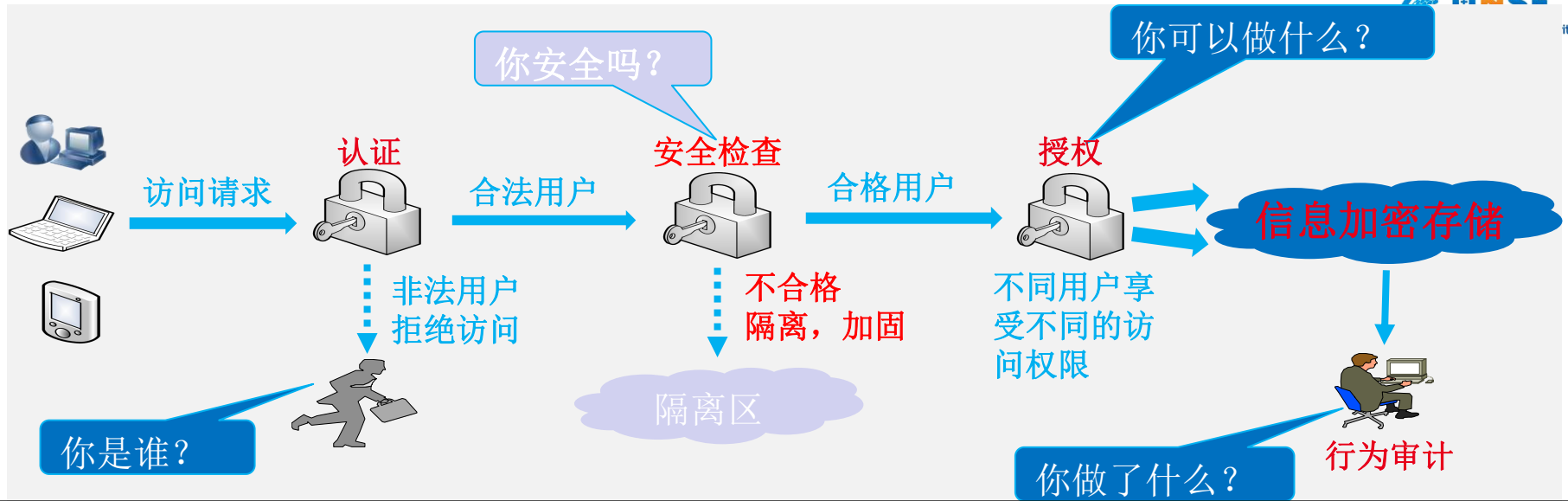
医院敏感数据保护

- 身份认证
- 授权控制：

- 传输加密
- 存储加密/脱敏

- 责任追溯
- 安全审计

事前　　事中　　事后



非医疗类业务可信安全应用主要内容

电子单据
合法化/无纸化

登录系统
用户身份真实

多场景
电子签名应用

易管理
电子合同应用

小结

安全可信医院网络空间
核心要素

- 身份核实与认证
- 行为明确与责任
- 数据合法且安全
- 隐私保护应用
- 适应多场景满足各类角色需要

谢 谢

THANKS