




ORACLE®

医疗信息安全需要关注的问题和探讨

王海彤

haitong.wang@oracle.com

Oracle 医药与卫生行业总监



很多父母都有这样的经历，当孩子刚出生，很快就有人直接打他的手机推销婴儿用品。

为什么很多人在就诊时对留下非常详细的个人信息有顾虑？



议题 Agenda

国外医疗信息安全建设思路和体系

- 医疗信息安全需要关注的内容
- 医疗信息安全的最佳实践分享

医疗信息安全的核心内容

- **Privacy (隐私):**

通过赋予患者控制他们个人识别信息和健康/治疗信息使用的权利，使得患者可以设置健康/治疗信息的使用、共享、被访问以及如何保护的规则

- **Security (安全):**

通过一系列管理、技术和物理的安全防护措施以及相关的策略/规章制度（Policies）和操作规程（procedures）来保证ePHI（受保护的健康信息）的安全性。

隐私问题

被授权的用户对信息做不适当的披露

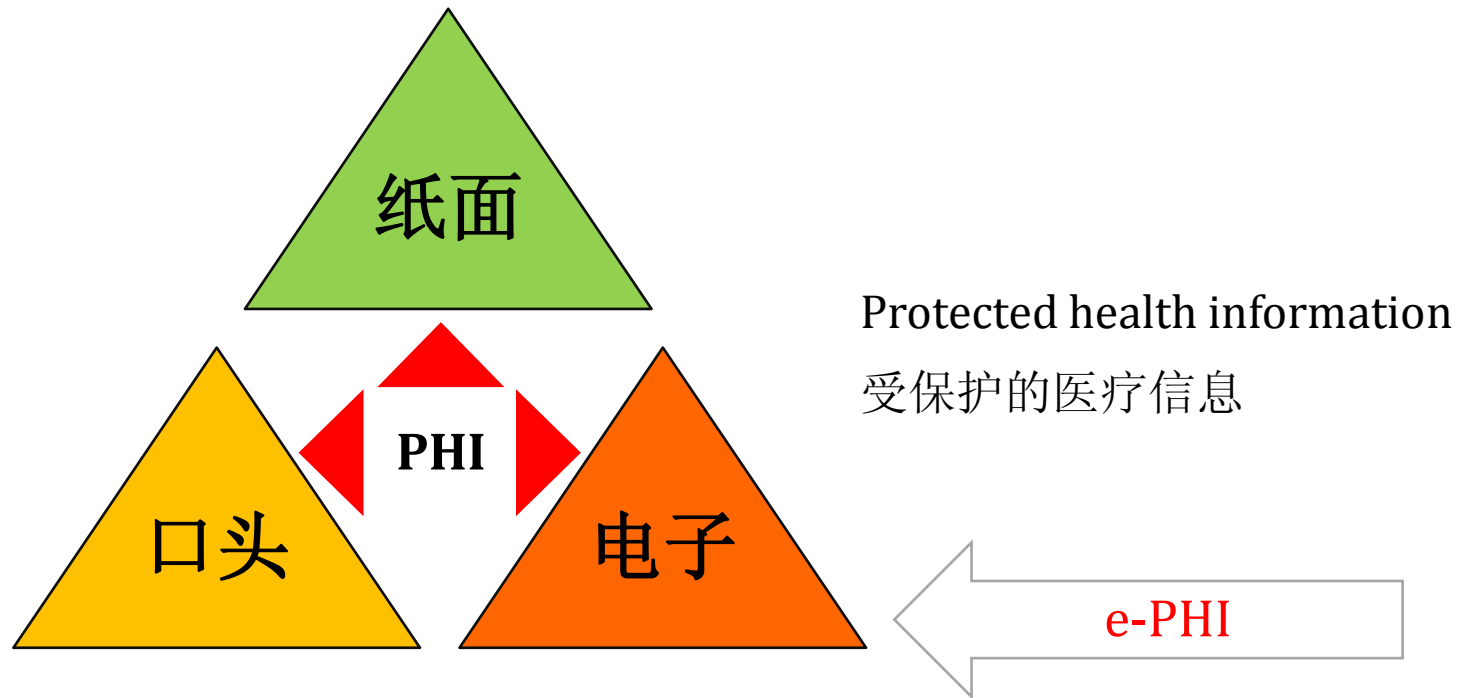
安全问题

未被授权的用户对信息作不适当的披露

使用目的
(Purpose)

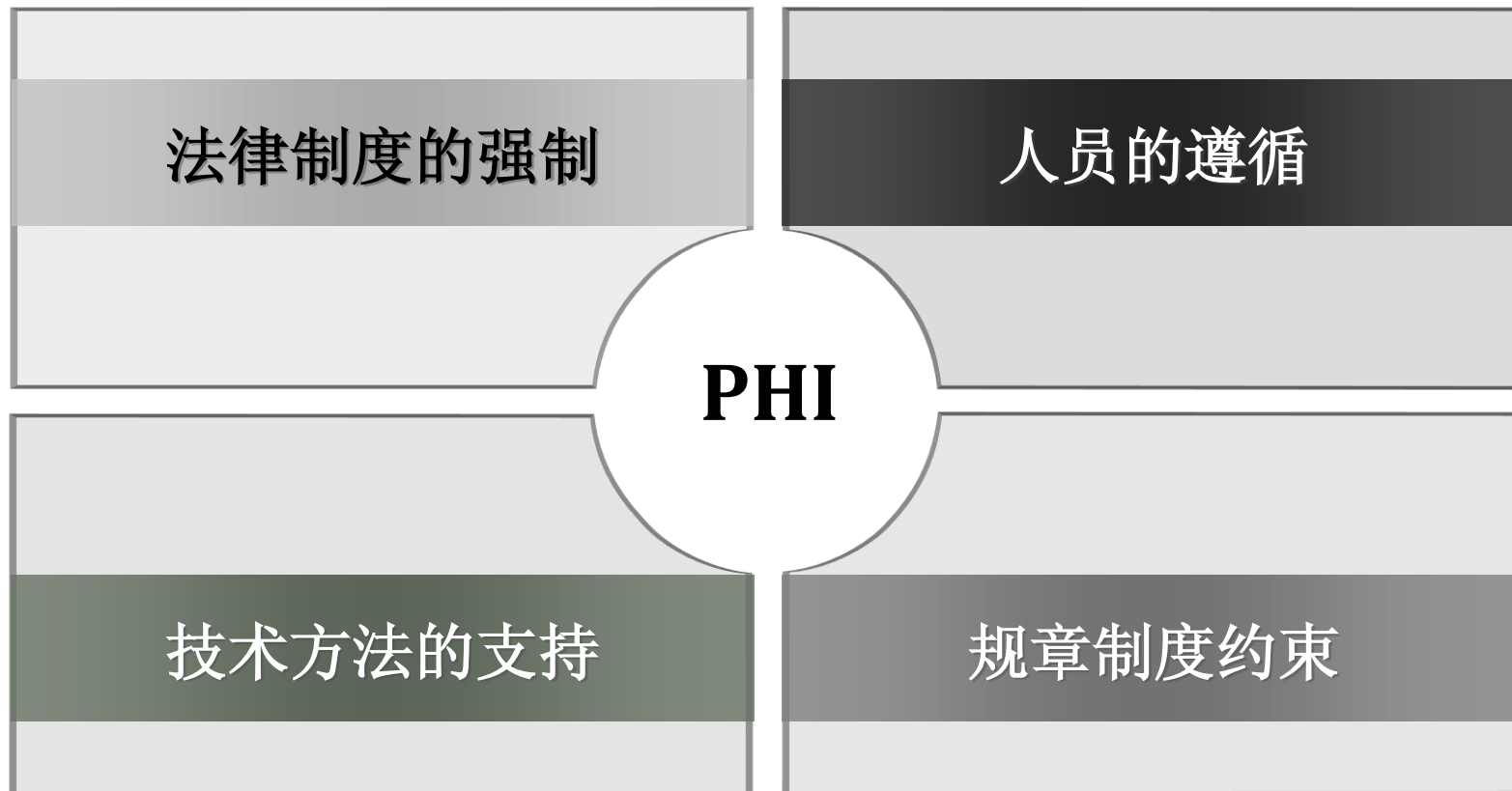
业务行为或者任务的分类，授权用户是否不适当的使用
数据取决于使用目的（PURPOSE）

受保护的医疗信息 (PHI)



- 明确 **标识个人**（或有合理的可用于识别个人）的信息
- 包括过去，现在或将来的身体或精神**健康状况，治疗状况，或医疗支付**等

医疗信息的安全性是一个“系统”问题



美国医疗信息的安全法律体系

法律制度

HIPPA:

Healthcare Insurance Portability and Accountability Act

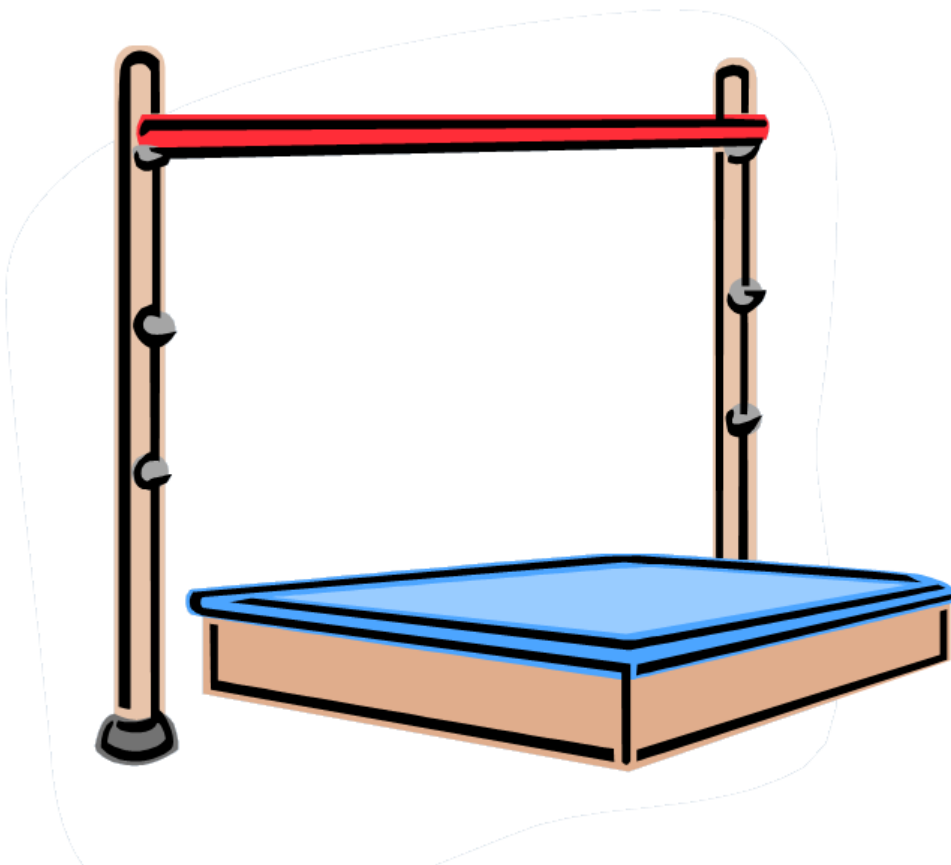
- 保证健康保险流通性，降低医疗欺诈行为，保证健康信息的安全及隐私，并强制卫生信息标准。
- 要求“涵盖实体”实施的具体程序和安全保障，以保护“电子保护的健康信息”（ePHI）安全和隐私。

HITECH:

Health Information Technology for Economic and Clinical Health Act

- 包含新的关于“涵盖实体”和商业伙伴如何管理医疗信息的隐私和安全的要求

美国医疗信息安全体系要求



- 合规性评估，最后的合规期限
- 自我评估，基于评估方案选择

- 安全意识和培训是信息安全的一个非常重要的事项
- 定期的回顾和检查信息安全技术控制手段和使用操作规范

管理和技术文档

技术保障措施

物理环境保障措施

行政管理保障措施

规章制度/操作规范

组织架构

美国HIPAA 信息安全技术规范 and 标准

- 行政管理保障措施 (Administrative Safeguards) 55%
 - 12 Required, 11 Addressable
- 物理环境保障措施 (Physical Safeguards) 24%
 - 4 Required, 6 Addressable
- 技术保障措施 (Technical Safeguards) 21%
 - 4 Required, 5 Addressable

Addressable 实施说明要求设计实体必须基于以下因素，评估一个实施说明是否合理和合适：

- 风险分析和缓解策略
- 当前的安全控制适当情况
- 实施成本

美国HIPAA 信息安全技术规范 and 标准

规范和标准	实施说明	规范和标准	实施说明
安全管理流程	R 风险分析 R 风险管理 R 处罚策略 R 信息系统活动评估	安全评估	R
安全责任分配	R	访问控制设施	A 应急业务 A 设施保安计划 A 访问控制和验证程序 A 维修记录
人员信息访问安全	A 授权和/或监督 A 人员机密性信息授权程序 A 终止程序	工作站使用	R
信息存取管理	R 医疗信息交换功能的隔离 A 访问授权 A 访问建立与修改	工作站安全	R
安全意识和培训	A 安全提醒 A 保护免受恶意软件 A 登录监察 A 密码管理	设备和介质控制	R 废弃处置 R 介质重新使用 A 问责制 A 数据备份和存储
安全事故的程序	R 响应和报告	访问控制	R 唯一的用户标识 R 紧急情况信息访问程序 A 自动注销/退出 A 加密和解密
应变计划	R 数据备份计划 R 灾难恢复计划 R 紧急模式操作计划 A 测试和修订程序 A 应用程序和数据的危害性分析	审计控制	R
商业合作伙伴合同和其他	R 书面合同或其他安排	完整性	A 电子PHI验证机制
		个人和实体认证	R
		传输安全性	A 完整性控制 A 传输加密



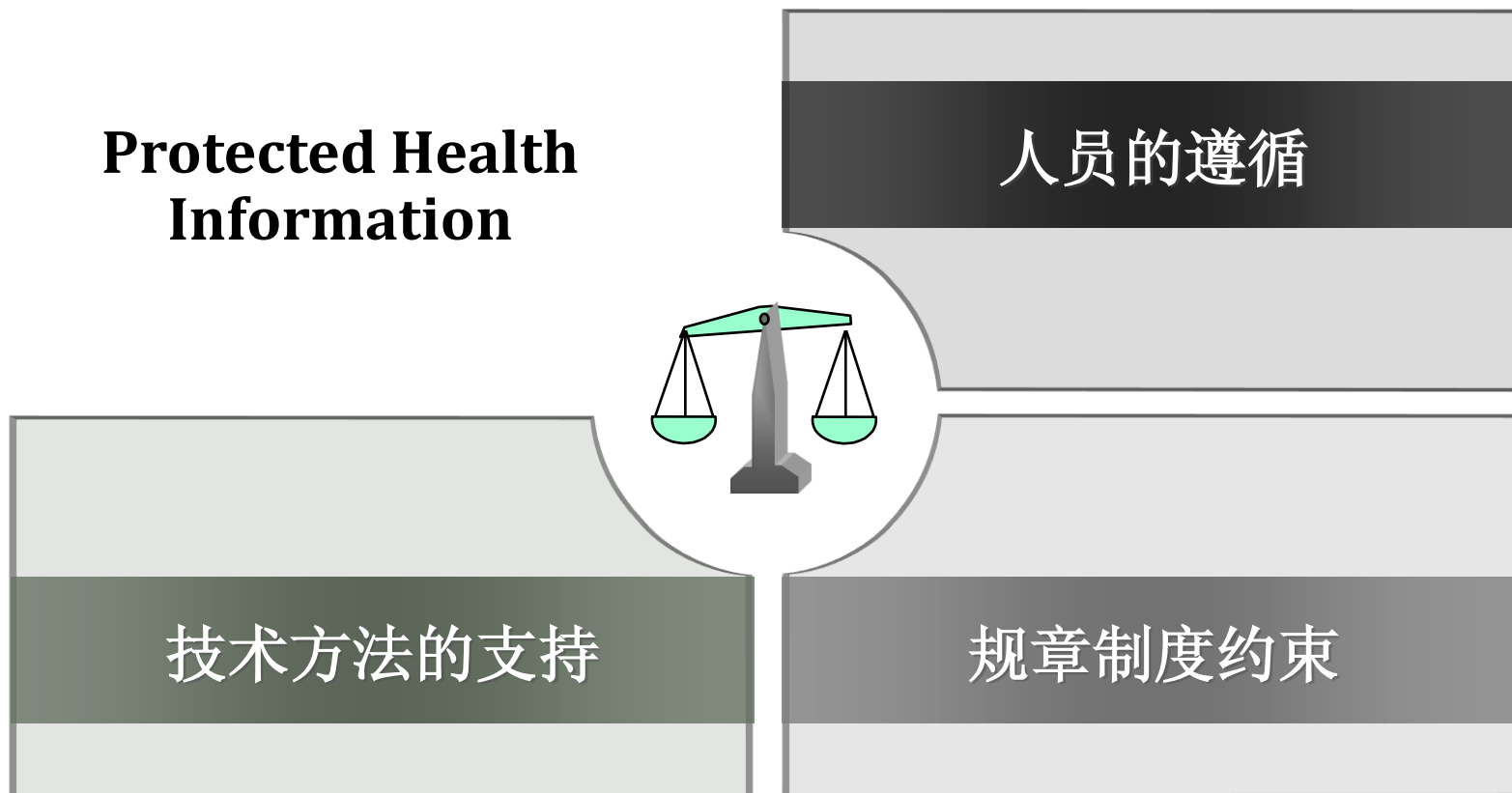
议题 Agenda

- 国外医疗信息安全建设思路和体系

医疗信息安全需要关注的内容

- 医疗信息安全的最佳实践分享

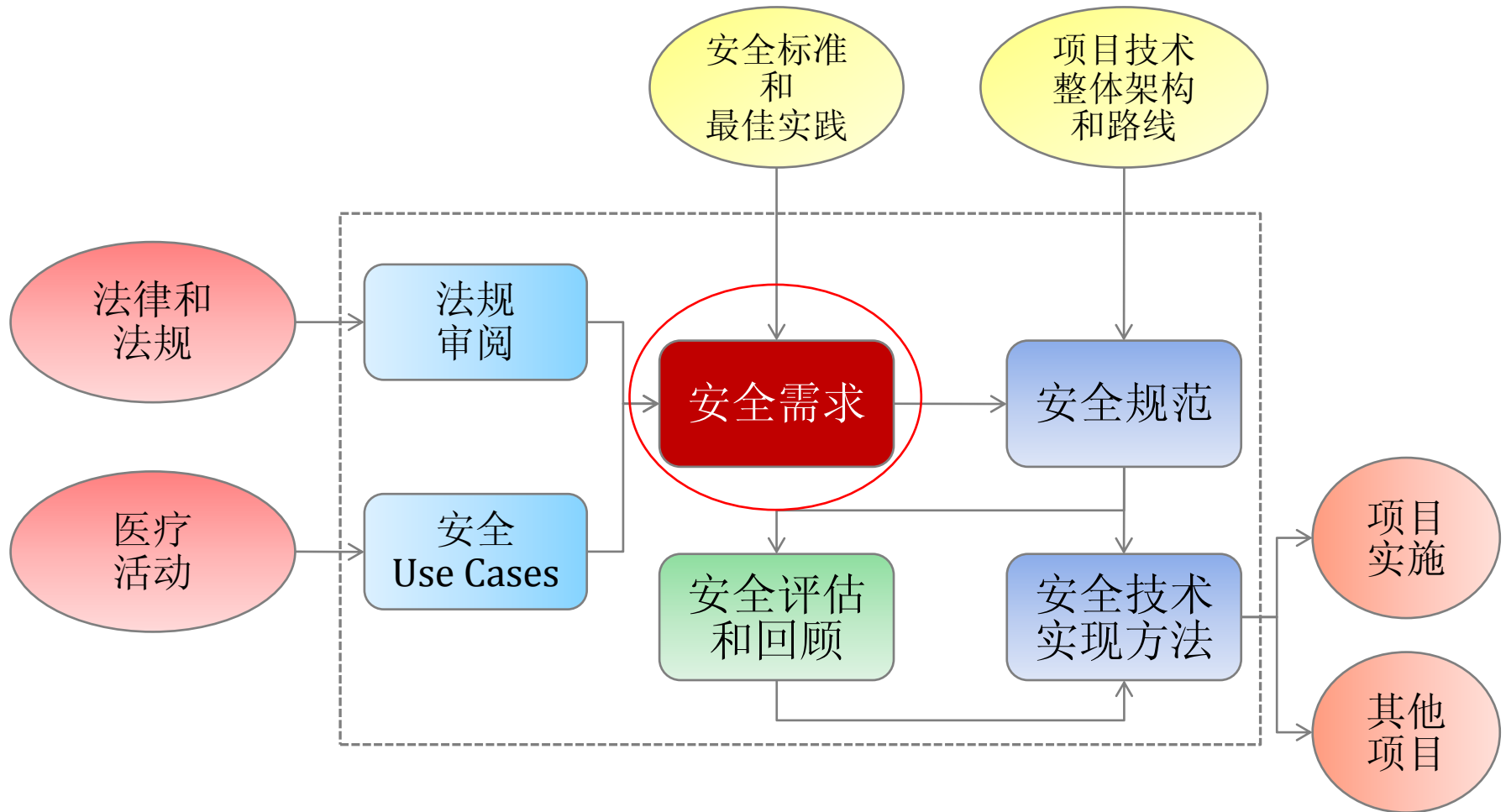
医疗信息的安全性需要“平衡”



医疗信息的安全性需要“平衡”

- 信息的安全性不意味只考虑保护而不考虑成本的昂贵。
 - 在信息可识别的风险及脆弱性和实现各种保护措施的成本之间平衡
 - 操作的复杂性，技术复杂性之间的平衡
-
- 组织机构可以决定自己的技术方案选择来减轻其风险，但不意味着组织有完整的自由决定权权，制定自己的规则。

项目信息隐私和安全策略制定



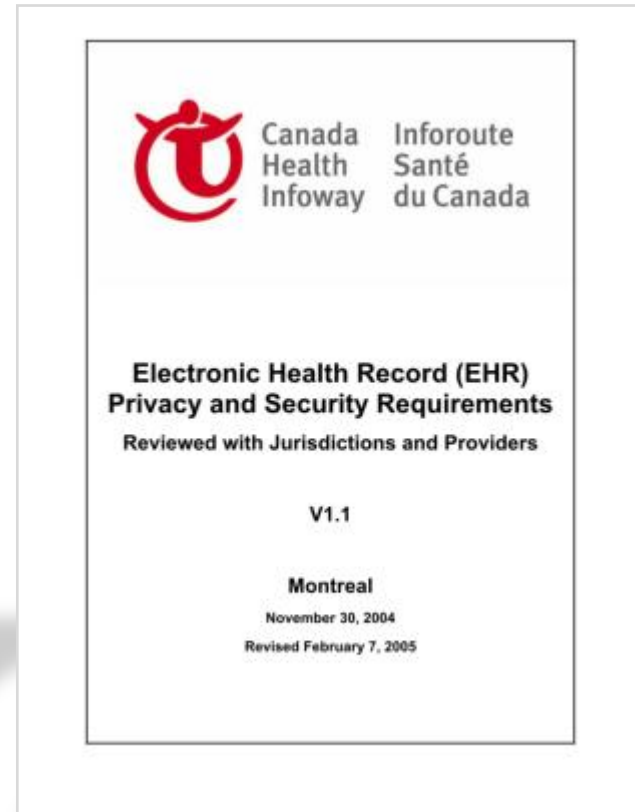


议题 Agenda

- 国外医疗信息安全建设思路和体系
- 医疗信息安全需要关注的内容

医疗信息安全的最佳实践分享

项目信息隐私和安全策略制定



加拿大 Infoway 电子病历隐私和安全需求框架

加拿大 Infoway: 隐私和安全服务架构

JURISDICTIONAL INFRASTRUCTURE

COMMON SERVICES

INTEROP

Interoperability Services

Search/Resolution Services

INTEGRATION

Service Catalogue Services

Broker Services

Mapping Services

Queuing Services

CONTEXT

Caching Services

Session Mgmt Services

PRIVACY & SECURITY

Identity Protection Services

Identity Mgmt Services

Access Control Services

Anonymization Services

User Authentication Services

Secure Auditing Services

General Security Services

Consent Directives Mgmt Services

Encryption Services

Digital Signature Services

SUBSCRIPTION

Alert/Notification Services

Pub/Sub Services

MANAGEMENT

Management Services

Configuration Services

Policy Mgmt Services

GENERAL

Auditing Services

Log Mgmt Services

Exception/Error Handling Services

Data Warehouse

Mgmt a

Privacy Data

Configuration

POINT OF SERVICE

ORACLE®

医疗信息安全架构建设需要关注内容

用户身份管理

- 创建、登记、注册一个用户（可能是医护人员、患者、系统管理员等），暂停/撤销用户的使用权限等。

用户认证管理

- 鉴定用户的合法性，支持不同的鉴别机制，用来进行会话过程中的权限。

访问控制管理

- 管理和协调数据访问的规则，控制用户访问数据和用户的权限。
- 定义用户的角色、工作组

同意指令管理

- 基于“病人知情/同意”原则的对数据访问规则的设定

去标识管理

- 根据业务应用的目的，去除或者隐藏受保护的格式识别信息

医疗信息安全架构建设需要关注内容

加密管理

- 密钥的管理。
- 数据、数据文件、数据存储、数据传递的加密解密

数字签名管理

- 数字签名密钥管理，数字证书管理、校验
- 数字时间标记和数字公证

安全审计管理

- 对关键数据的访问、更新和删除的工作的记录，为所有的关键数据信息使用行为保留痕迹

基础安全管理

- 恶意软件保护
- 数据备份和恢复
- 数据的长期保存
- 数据从介质上（硬盘/光盘）上完全的被擦除和毁掉的机制

美国医疗信息安全调查

Security Tool	Hospital Use	Medical Practice Use
Audit Logs	48.10%	52.60%
Biometric Technologies	15.20%	13.30%
Data Encryption (Storage)	47.50%	39.50%
Data Encryption (Transmission)	54.00%	39.40%
Data Loss Prevention	30.90%	20.80%
Disaster Recovery	72.70%	63.60%
eDiscovery*	24.50%	6.50%
Electronic Signature	47.90%	42.90%
Email Encryption	63.60%	48.80%
Firewalls*	20.00%	33.30%
Intrusion Prevention	43.80%	36.10%
Mobile Device Encryption*	53.20%	33.30%
Network Encryption	25.00%	21.60%
Off-Site Electronic Data Storage	31.30%	24.00%
Public Key Infrastructure	12.80%	6.80%
Single Sign On*	46.50%	15.70%
Two-Factor Authentication	26.80%	20.80%
User Access Controls	40.00%	28.60%
Wireless Security Protocols	38.20%	27.30%

2010 HIMSS Security Survey

隐私安全保护的最佳实践

PHI信息的限制使用

- 保证PHI信息的必要情况下才能够(有限的)使用
- 针对业务需要实现最少的必要的信息提供
- 确保患者和公众的知情和自愿授权

物理环境安全保障

- 机房等核心区受控访问
- 专用线路（或VPN）提供公众的访问使用
- 专用网关和门户网站
- 全面的访问使用控制；包括授权、认证、访问控制和日志记录
- 保安员管理和携带物品检查
- 访客通行证及陪送制度
- 封闭电脑的USBs，存储驱动器，网络接入卡及调制解调器等
- 网络访问被限制在专用的路由器和网络，禁止Internet访问
- 在相关的区域设置信息安全警示板
- 视频监控
- 物理设备的维护和库存规定
- 打印控制和资料销毁
- 正式的设备处置程序

隐私安全保护的最佳实践

逻辑安全

- 数据分类和相应的安全规范
- 系统边界定义
- 应用功能限制
- 及时安装关键的应用补丁和升级
- 应用程序开发，测试和生产环境保持清晰的边界

数据安全

- 专线连接或安全分区，根据业务需要设置访问控制
- 数据加密或者使用数据蒙蔽
- 与服务提供商建立安全漏洞相应机制
- 文件销毁机制
- 用户帐户管理，添加/删除机制
- 确立的审计追踪

隐私安全保护的最佳实践

人员培训

- 在安全防范放在，以及操作规范对人员进行持续的培训
- 人员内部安全认证
- 合法和非法披露意识
- 人员信息保密协议

数据安全

- 专线连接或安全分区，根据业务需要设置访问控制
- 数据加密或者使用数据蒙蔽
- 与服务提供商建立安全漏洞相应机制
- 文件销毁机制
- 用户帐户管理，添加/删除机制
- 确立的审计追踪

隐私安全保护的最佳实践

安全工具和程序

- 入侵检测和阻止
- 日志分析
- 木马和病毒检测工具
- 防火墙

灾难恢复和业务连续性

- 多层次的灾难恢复和业务连续性机制
- 每日、每周、每月的备份
- 离线数据备份
- 冗余存储和镜像
- 紧急处置程序

Oracle信息安全解决方案及产品

Oracle 联邦身份管理		Oracle医疗安全管理	
Oracle身份分析	Oracle Web服务管理		Oracle角色管理
Oracle 身份管理		Oracle权限管理	
Oracle 高级安全	Oracle 单点登录服务		Oracle 目录服务
Oracle 标签安全		Oracle 审计 Vault	
Oracle 数据库屏蔽	Oracle 全面回忆		Oracle 安全备份
Oracle 数据库防火墙		Oracle 数据库 Vault	
Data Guard	Golden Gate		集群服务器

Oracle信息安全防护体系及方案

Hardware and Software

Engineered to Work Together