大成 DENTONS

《通用数据保护条例（GDPR）》背景下医疗大数据质量管控思考

邓　勇

国家中医药管理局　　常年法律顾问

北京中医药大学法律系　　医药卫生法副教授

北京大成律师事务所　　合伙人律师

中国政法大学法学院　　法学博士

2018-9-18

目 录 CONCENTS

GDPR

（General Data Protection Regulation）

——（通用数据保护条例）于2018年5月25日正式施行

目标：保护欧盟公民免受隐私和数据泄露的影响，同时重塑欧盟的组织机构处理隐私和数据保护的方式。

GDPR新规将影响哪些企业？

任何存储或处理欧盟国家内有关欧盟公民个人信息的公司，即使在欧盟境内没有业务存在，也必须遵守GDPR。有关必须遵守GDPR新规的公司的具体标准如下所示：

- 在欧盟境内拥有业务；
- 在欧盟境内没有业务，但是存储或处理欧盟公民的个人信息；
- 超过250名员工；
- 少于250名员工，但是其数据处理方式影响数据主体的权利和隐私，或是包含某些类型的敏感个人数据。

这也就意味着，GDPR新规几乎适用于所有的公司。普华永道提供的调查结果显示，92%的美国公司认为GDPR将成为最重要的数据保护措施。

哪些类型的隐私数据将受到GDPR保护？

- 基本的身份信息，如姓名、地址和身份证号码等；
- 网络数据，如位置、IP地址、Cookie数据和RFID标签等；
- 医疗保健和遗传数据；
- 生物识别数据，如指纹、虹膜等；
- 种族或民族数据；
- 政治观点；
- 性取向。

判断中国企业是否适用 GDPR

如果企业没有满足GDPR的合规性要求将导致什么后果？

每一单GDPR违规行为将受到高达2000万欧元的严重处罚，或者上一年全球年营业额的4%，以较高者为准。根据Ovum公司提供的调查报告显示，52%的受访IT决策者预计他们会因为违规行为而面临罚款。管理咨询公司奥利弗·怀曼（Oliver Wyman）预测，欧盟在第一年可能会收到高达60亿美元的罚款金额。

一、医疗大数据的安全风险

中华人民共和国中央人民政府
www.gov.cn

国务院 | 总理 | 新闻 | 政策 | 互动 | 服务

首页 > 信息公开 > 国务院文件 > 卫生、体育 > 卫生

索 引 号：	000014349/2016-00132	主题分类：	卫生、体育\卫生
发文机关：	国务院办公厅	成文日期：	2016年06月21日
标　　题：	国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见		
发文字号：	国办发〔2016〕47号	发布日期：	2016年06月24日
主 题 词：			

国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见

国办发〔2016〕47号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

健康医疗大数据是国家重要的基础性战略资源。健康医疗大数据应用发展将带来健康医疗模式的深刻变化，有利于激发深化医药卫生体制改革的动力和活力，提升健康医疗服务效

本报告以解放军总医院医疗大数据质量管控为报告和分析蓝本，在此致谢！

安全是医疗大数据的首要问题

医疗数据泄漏事件不断发生

- 2016年，两百多名艾滋患者因信息泄漏而遭遇诈骗
- 2016年，深圳多家医院万条产妇数据泄漏而遭遇推销
- 过去几年，“统方”等医疗数据滥用案例屡见不鲜

大数据环境下数据安全风险及影响增大

- 数据集中、量大，目标明显，泄漏后果更为严重
- 应用环境多元化，泄漏风险增加
- 泄漏后果既涉及个人隐私，也涉及医院秘密，还可能涉及国家机密

坚持规范有序、安全可控是国家发展医疗大数据的基本原则

- 国办发[2016]47号文：强化标准和安全体系建设，强化安全管理责任，妥善处理应用发展与保障安全的关系，增强安全技术支撑能力，有效保护个人隐私和信息安全

安全是医疗大数据的核心基础和首要问题

- “万无一失，一失万无”
- 安全保护是一个复杂的技术和管理问题

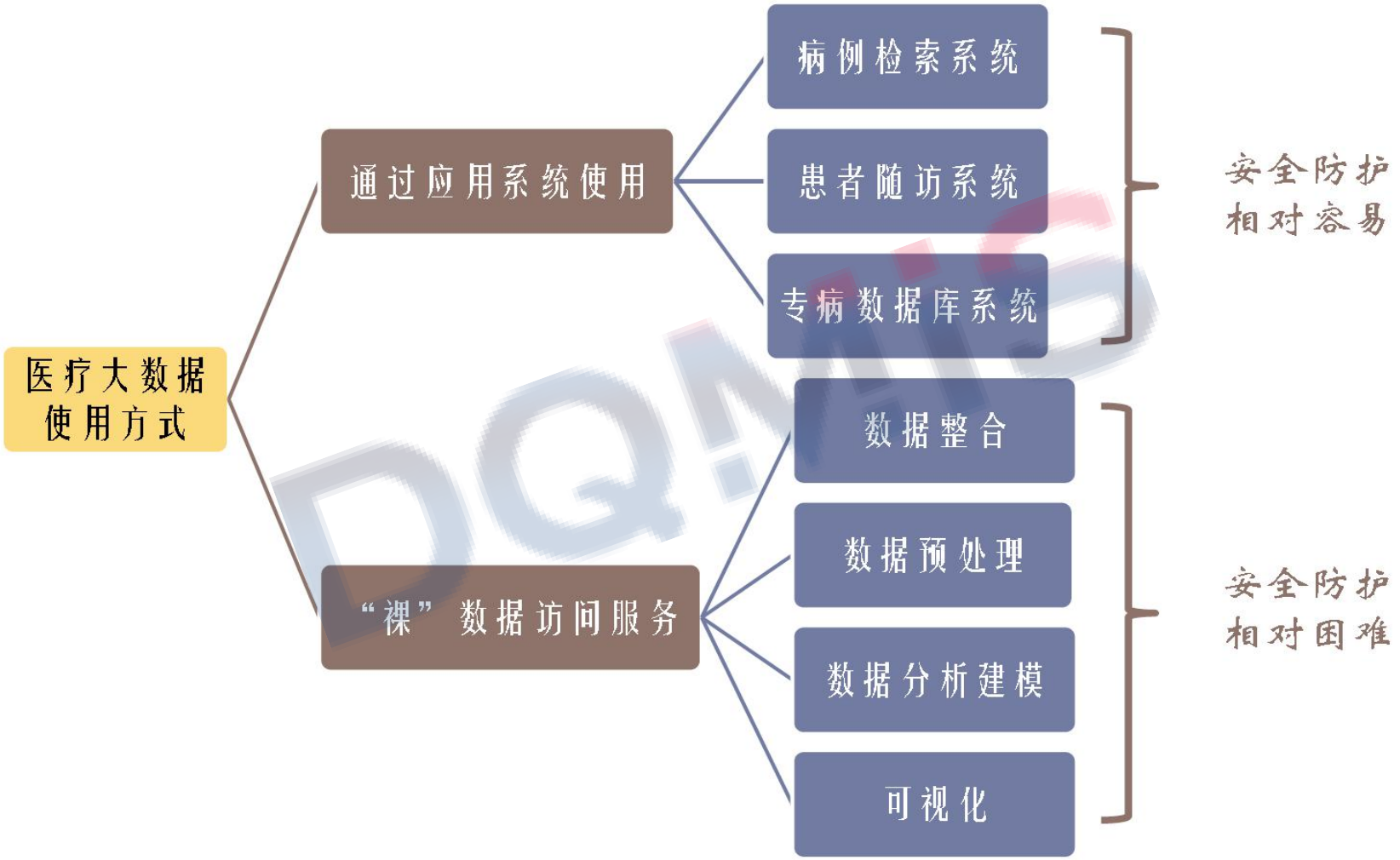
医疗大数据的界定

- 不同语境下的医疗大数据安全问题特点

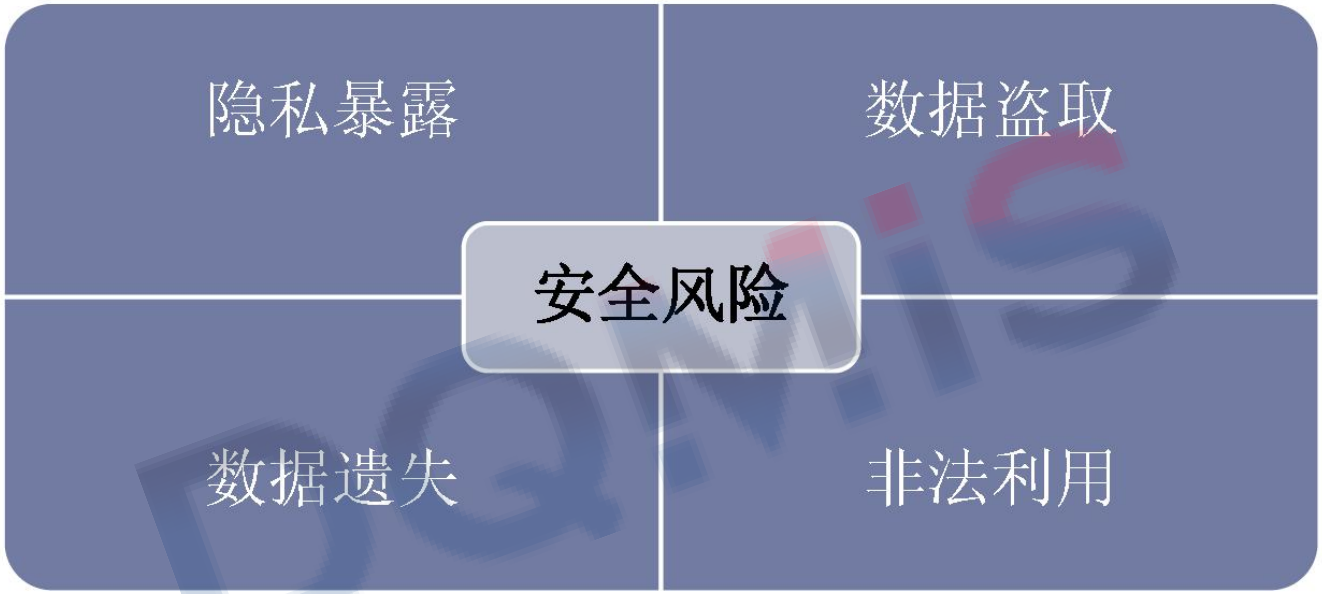
场景	典型应用	安全重点
区域卫生业务应用系统	健康医疗数据共享 居民服务	防网络攻击 隐私保护
区域卫生数据管理与再利用	管理决策 第三方数据共享	隐私保护 数据资产保护
医院数据中心业务数据管理	各类业务系统	防滥用 防篡改
医院数据整合与再利用	科研应用 管理决策	隐私保护 数据资产保护

- **我们的讨论聚焦在医院数据的整合与再利用**

医疗大数据的应用形式


医疗大数据使用方式
通过应用系统使用
病例检索系统
患者随访系统
专病数据库系统
安全防护相对容易
“裸”数据访问服务
数据整合
数据预处理
数据分析建模
可视化
安全防护相对困难

主要安全风险



既要防外：合作单位、外部厂商

更要防内：科室用户、技术人员

医疗大数据环境下的安全管理难点

数据使用者的多元化
- 各类业务研究人员
- 内部服务技术人员
- 外部合作人员

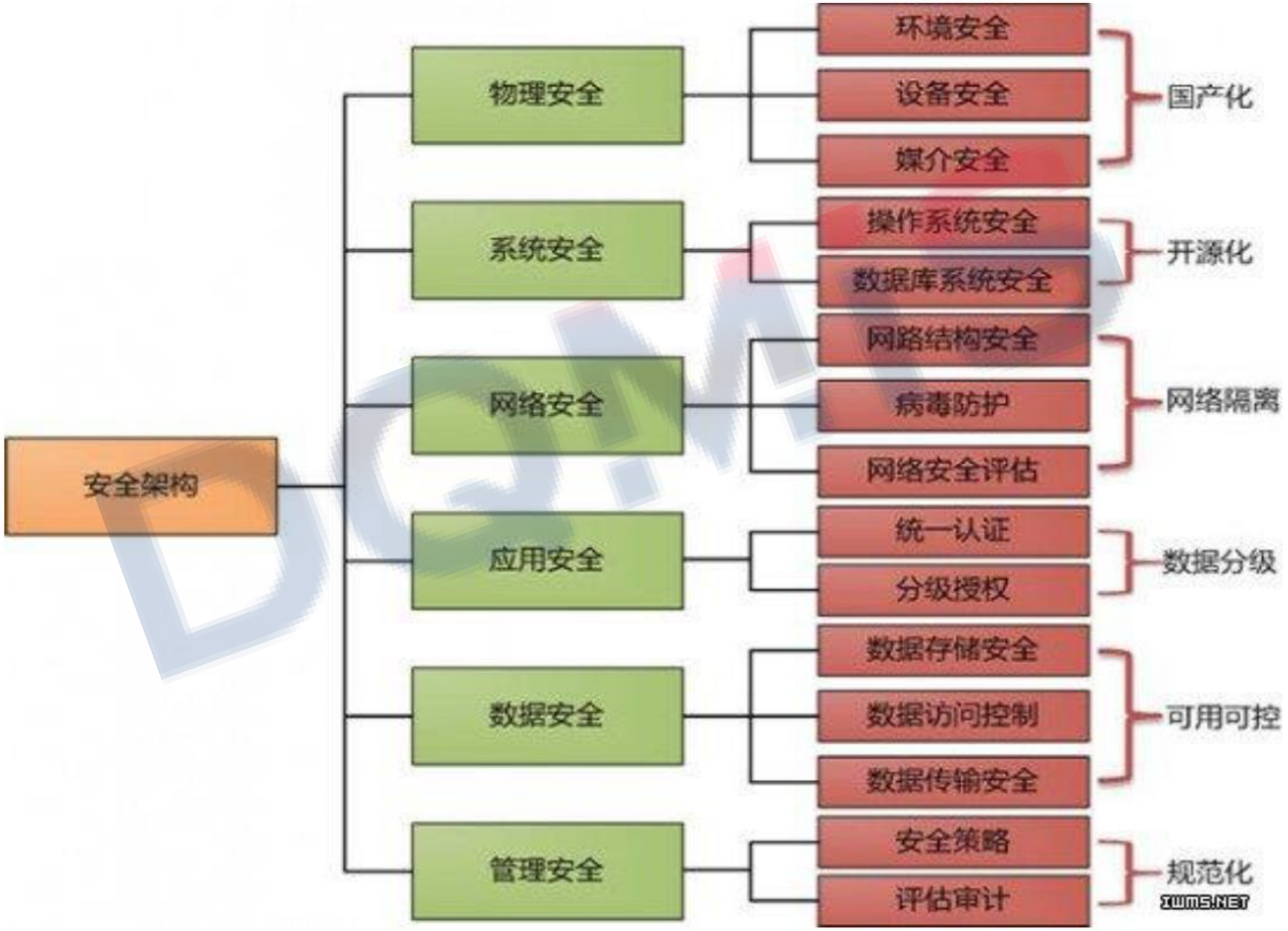
数据使用方式的多样化
- 多样化的软件工具
- 本地处理需求多

数据需求的多样化
- 数据需求随机性大
- 缺乏明确的用户角色
- 隐私/去隐私数据共存

技术环境的多样化
- 传统数据库
- Hadoop/NoSQL数据库
- 文件数据

安全防护的重点

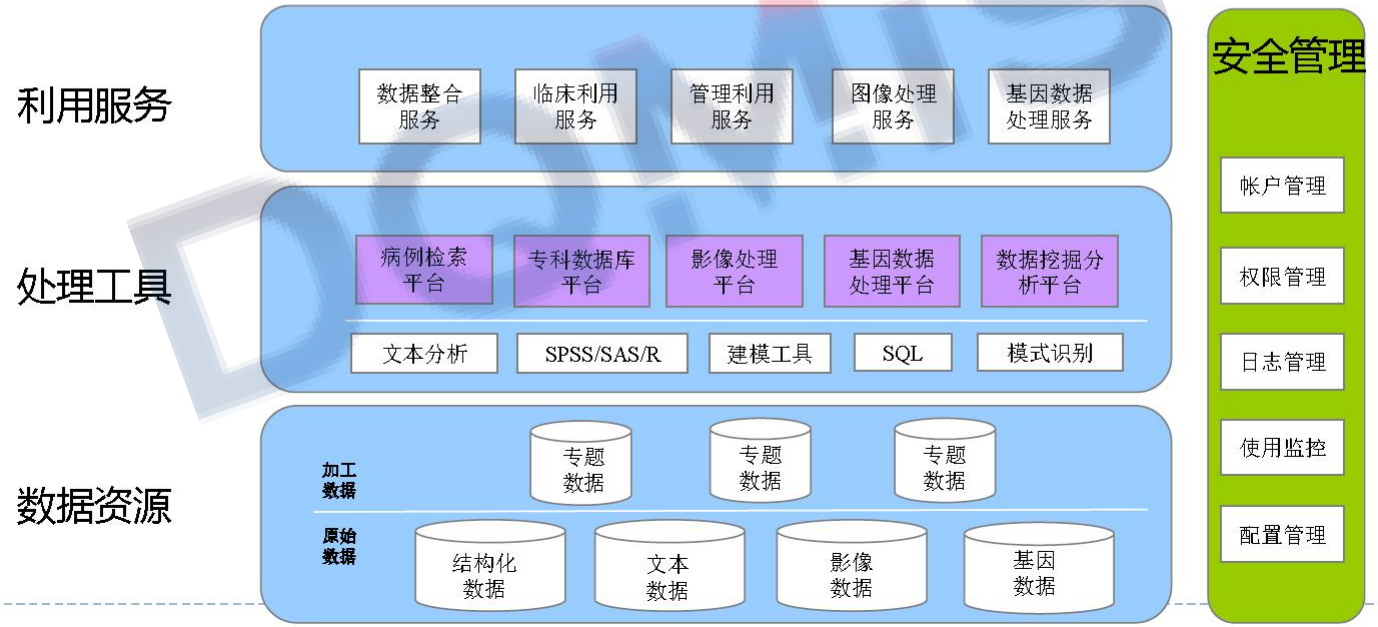
- 医疗大数据安全需要建立防护体系，重点是数据安全



二、医疗大数据的技术防护

之一：建立集中化的平台与服务机制

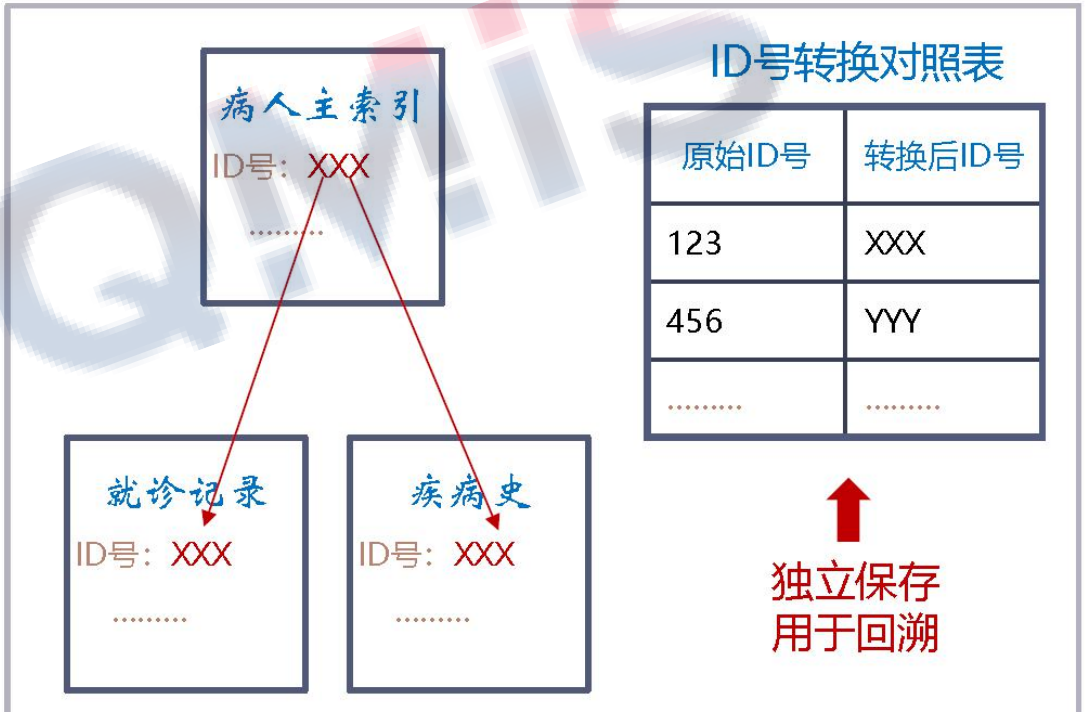
- 统一平台，改变数据管理使用各自为政的局面
  - 数据资源集中管理，避免分散流失
  - 处理能力统一提供，减少脱机下载
  - 数据安全统一防护，降低安全风险
  - 数据服务有序开展，规范数据利用



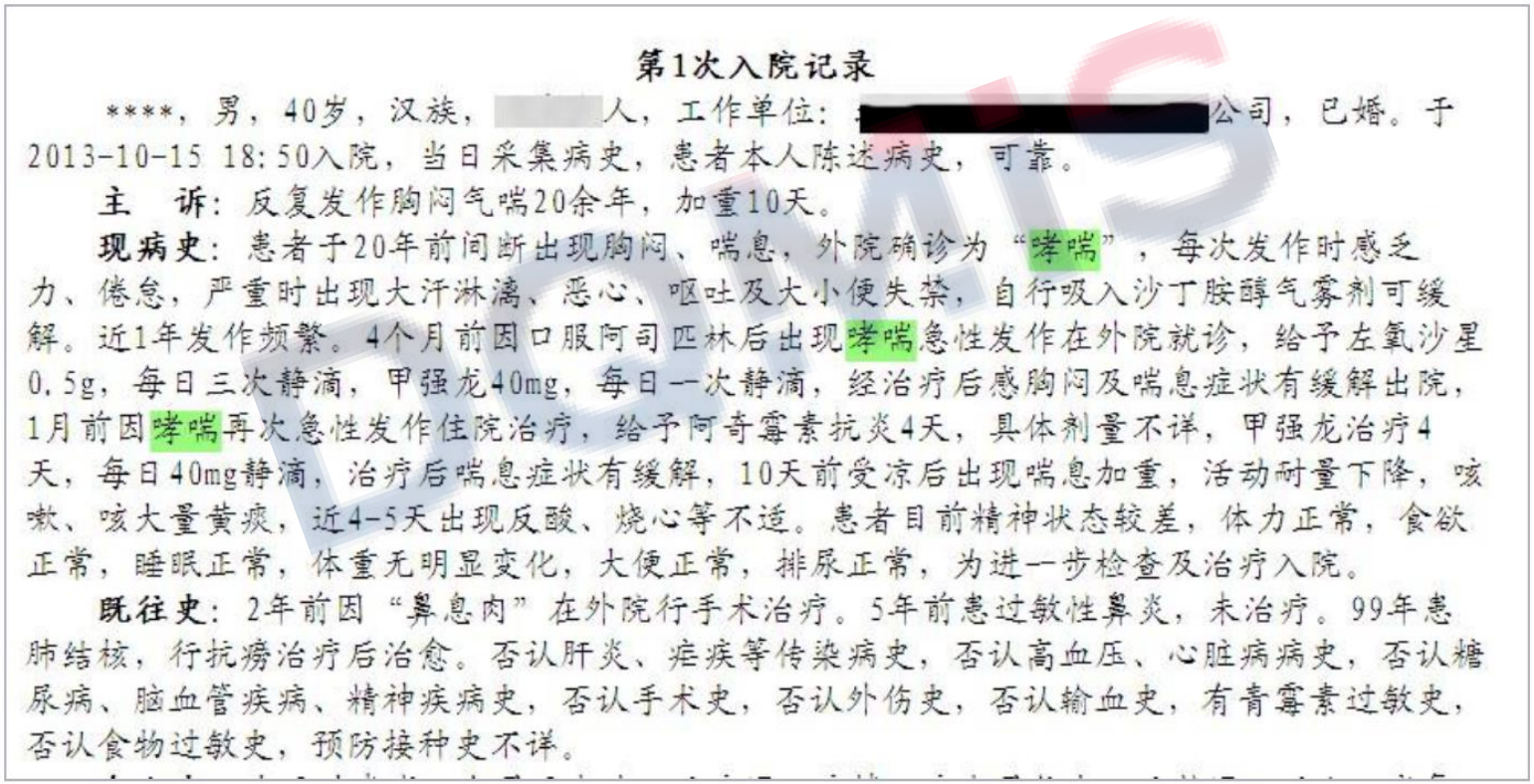
之二：去隐私—降低数据敏感度

- 去除或变换医疗数据中的患者识别信息
- 不同应用目的对患者识别信息有不同需求
- 结构化数据：直接替换

数据项	常用处理方式
患者ID号	变换
姓名	匿名、重新生成
出生日期	年龄、去除日期
身份证号	去除
居住地	泛化
联系电话	去除



- 文本数据
  - 主要包含姓名、居住地等识别信息
  - 需要采用自然语言处理技术进行识别与替换



第1次入院记录

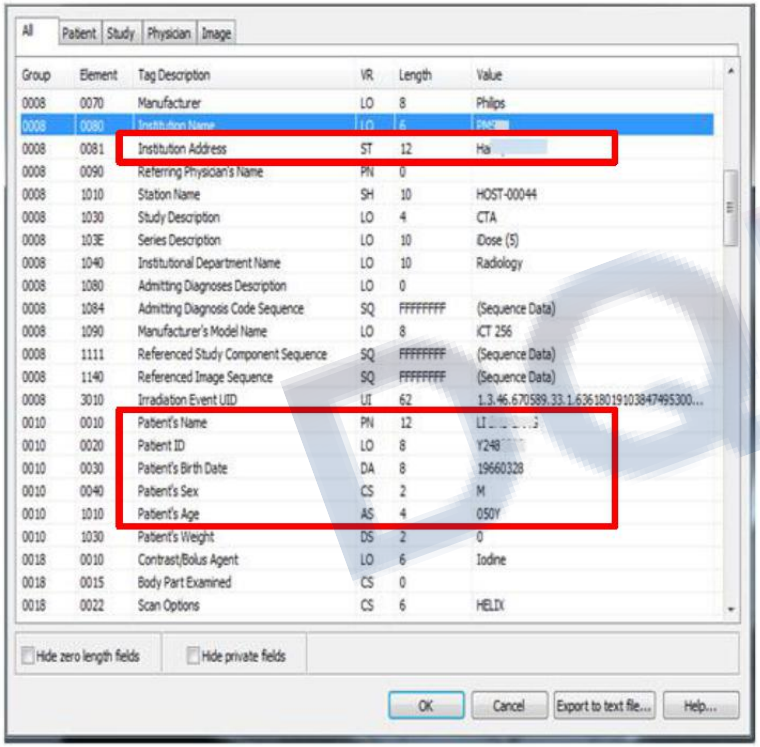
****，男，40岁，汉族，[redacted]人，工作单位：[redacted]公司，已婚。于2013-10-15 18:50入院，当日采集病史，患者本人陈述病史，可靠。

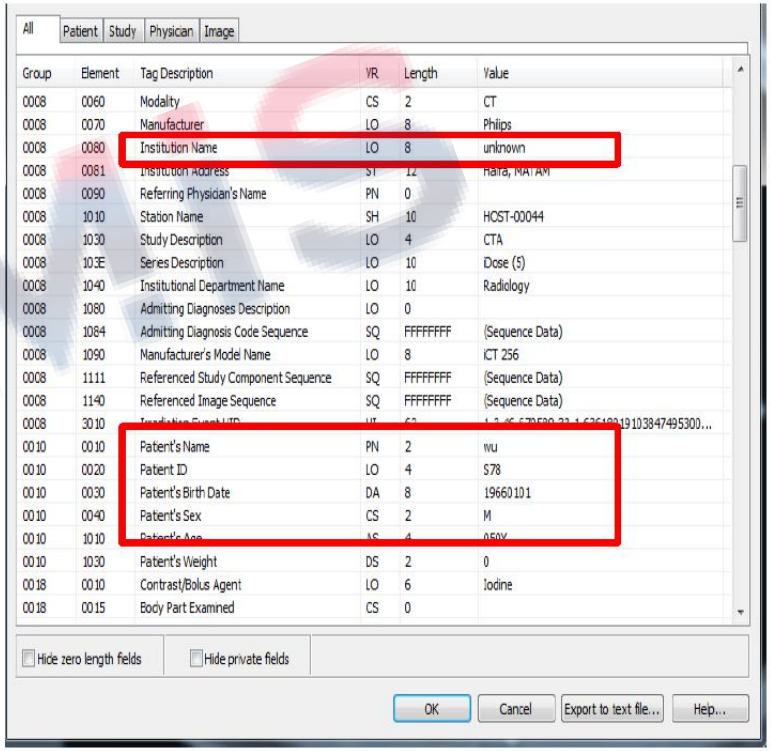
主　诉：反复发作胸闷气喘20余年，加重10天。

现病史：患者于20年前间断出现胸闷、喘息，外院确诊为“哮喘”，每次发作时感乏力、倦怠，严重时出现大汗淋漓、恶心、呕吐及大小便失禁，自行吸入沙丁胺醇气雾剂可缓解。近1年发作频繁。4个月前因口服阿司匹林后出现哮喘急性发作在外院就诊，给予左氧沙星0.5g，每日三次静滴，甲强龙40mg，每日一次静滴，经治疗后感胸闷及喘息症状有缓解出院，1月前因哮喘再次急性发作住院治疗，给予阿奇霉素抗炎4天，具体剂量不详，甲强龙治疗4天，每日40mg静滴，治疗后喘息症状有缓解，10天前受凉后出现喘息加重，活动耐量下降，咳嗽、咳大量黄痰，近4-5天出现反酸、烧心等不适。患者目前精神状态较差，体力正常，食欲正常，睡眠正常，体重无明显变化，大便正常，排尿正常，为进一步检查及治疗入院。

既往史：2年前因“鼻息肉”在外院行手术治疗。5年前患过敏性鼻炎，未治疗。99年患肺结核，行抗痨治疗后治愈。否认肝炎、痢疾等传染病史，否认高血压、心脏病病史，否认糖尿病、脑血管疾病、精神疾病史，否认手术史，否认外伤史，否认输血史，有青霉素过敏史，否认食物过敏史，预防接种史不详。

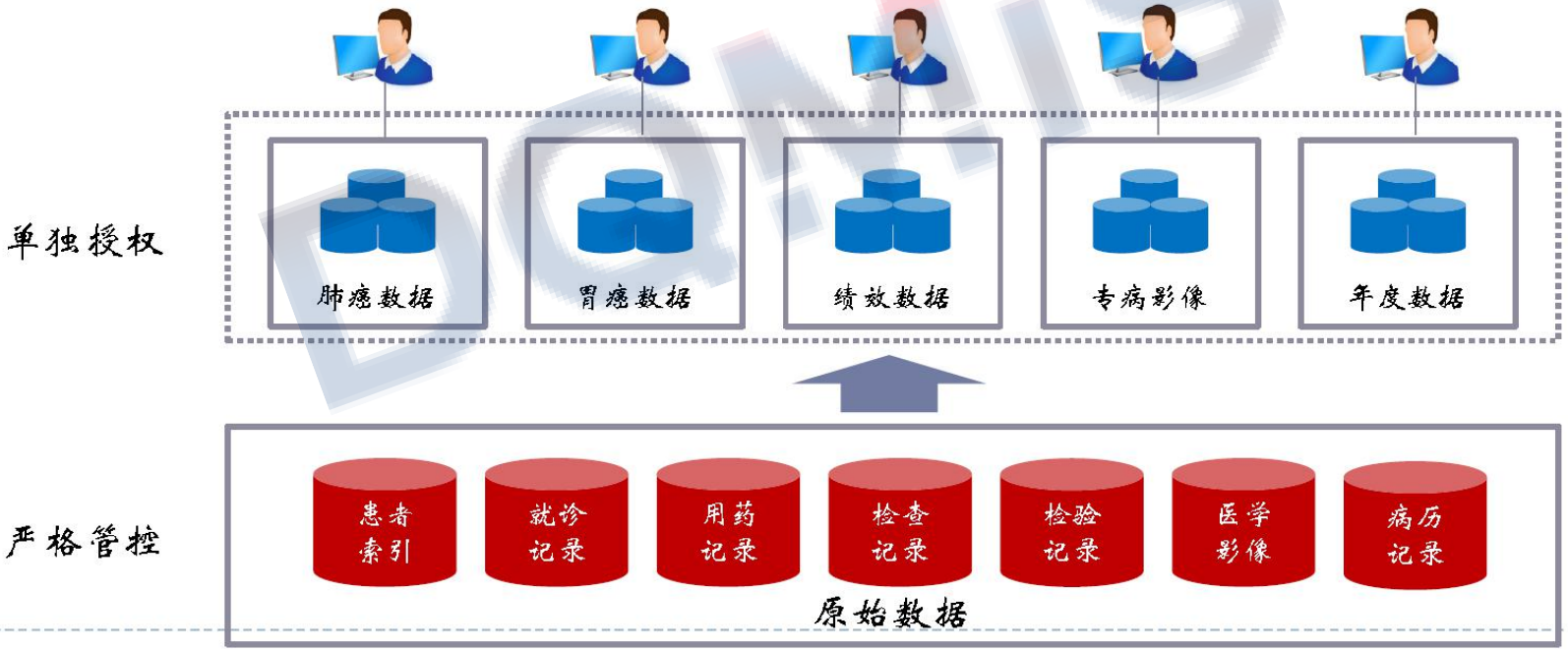
- 医学影像数据
  - DICOM影像：读取数据文件进行结构化替换
  - 模拟影像：使用模版遮蔽



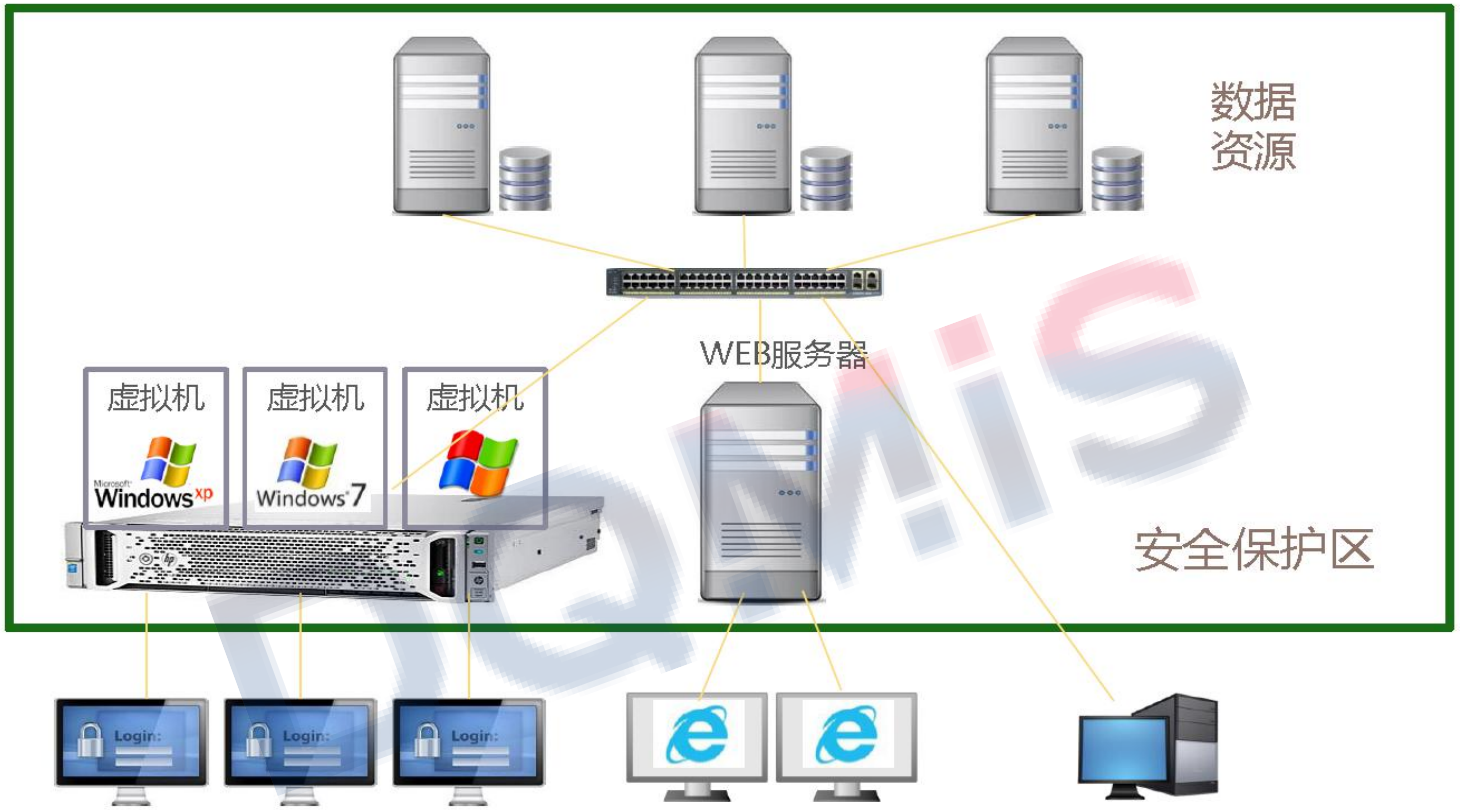


之三：按资源授权分解安全风险

- 数据资源“化整为零”
  - 原始医疗数据内容全、范围大，但每个研究主题明确，所需数据范围有限
  - 为不同的专科、病种建立数据资源库
  - 为每个临时研究抽取建立临时数据资源
  - 按照独立的数据资源授权



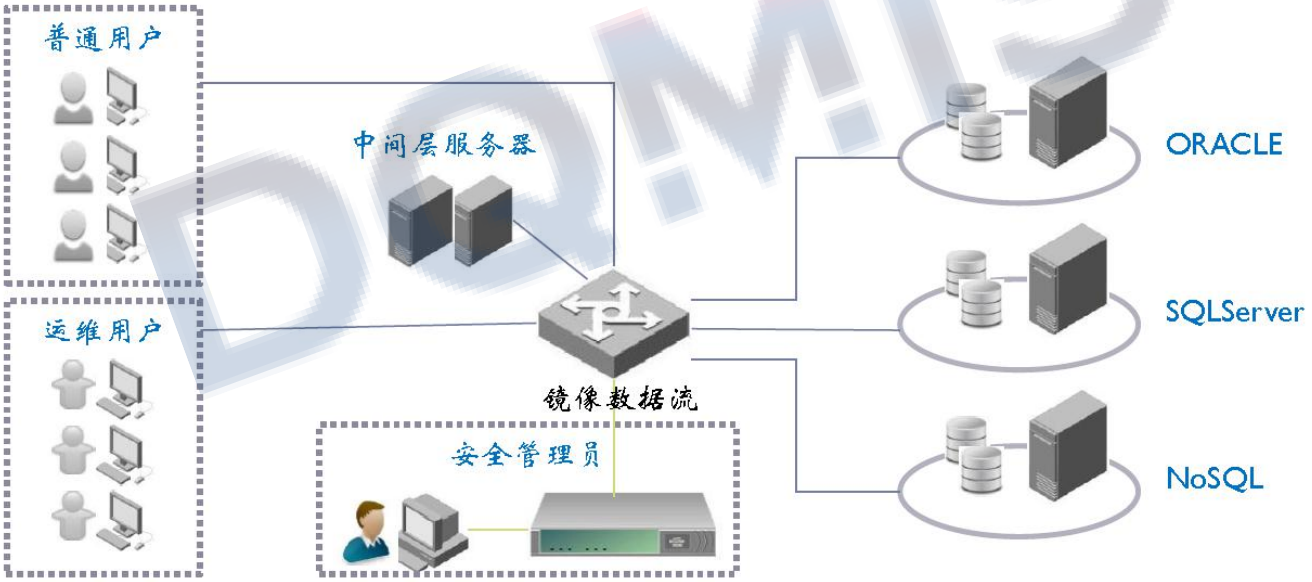
之四：虚拟桌面建立安全围墙



首选：虚拟桌面	其次：B/S应用	再次：受控计算机
数据处理部署于服务器	固定应用易于数据授权	封锁USB端口、邮件等
杜绝数据从本地复制	数据难以批量下载	控制数据复制

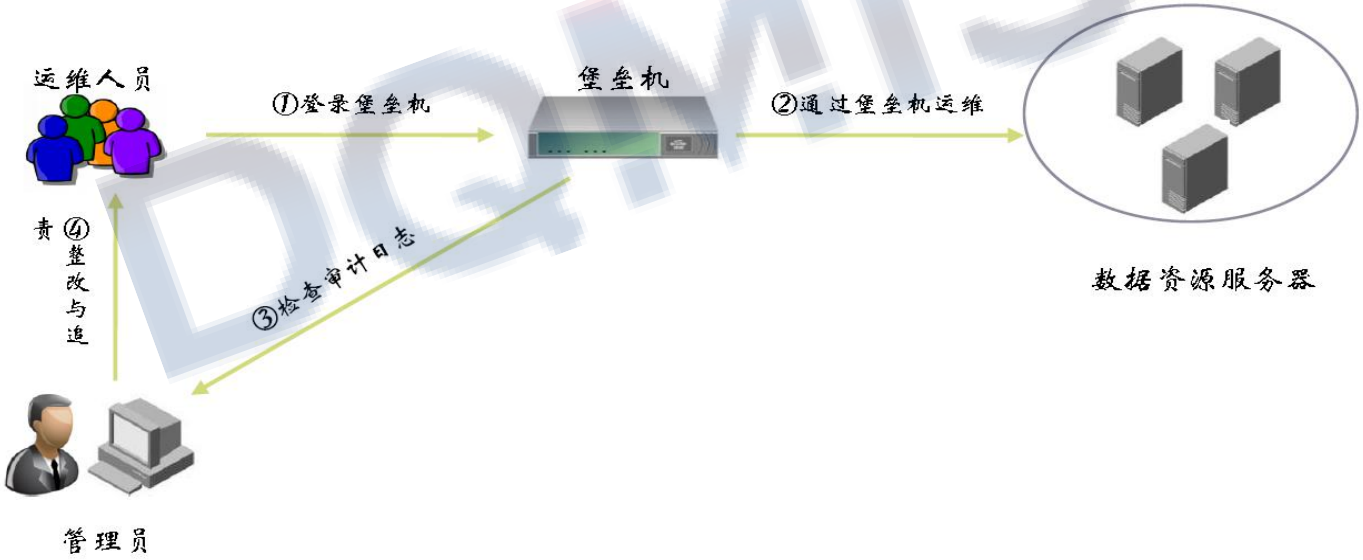
之五：数据库审计追踪使用行为

- 数据利用“监”重于“控”
  - 数据范围随意性大，“控”更难
  - 前置规定+事后审计，灵活简便
- 审计日志的安全分析是关键



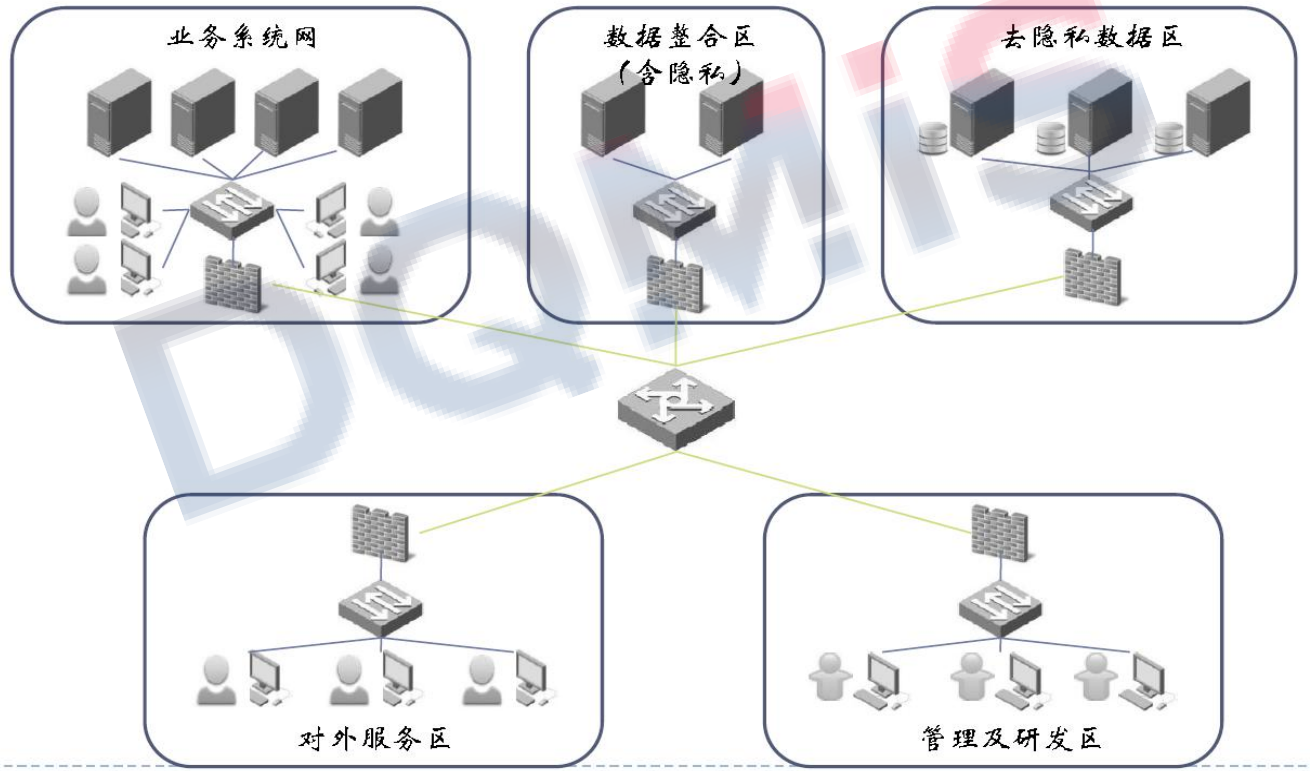
之六：堡垒机实现运维监控

- 对运维操作的监管是数据安全的重要方面
- 堡垒机技术
  - 实现对运维操作的记录与回放
  - 实现对运维权限的统一管理



之七：网络隔离划分安全区域

- 从网络层面管理访问权限
  - 按照不同的安全等级划分网络
  - 通过防火墙限制访问权限



之八：物理安全防止底层漏洞

- 物理安全是最基础的安全防护
  - 技术实现最简单
  - 安全事件后果最严重
  - 最容易被忽视
- 物理安全防护内容
  - 机房安全：门禁、监控
  - 机柜安全：加锁
  - 服务器：安全强度高的密码
  - 网络连接：防止非法接入

之九、依靠数据治理技术与服务提供商进行质量管控

华矩科技

- ——以华矩科技对某综合医院提供的数据治理服务为例

服务宗旨：解决医疗大数据质质量、标准化与结构化问题

概述：同种病症叫法不一，编码库对码困难。

具体问题：

1.病种数据录入问题严重影响正确对码；

2.错误数据发现慢，处理时间长；

3.没有及时维护标准病种数据库（对标ICD）；

4.没有全面智能的医疗术语业务规则，病种名称编码难匹配。

（2）解决方案

- 概述：自动化数据清洗与匹配；
- 具体方案：
  - 数据质量诊断；
  - 数据清洗与标准化；
  - 数据补全与去重；
  - 数据校对及匹配。

（3）客户获益

- 减少数据处理成本，提升数据使用效率；
- 建立医疗数据匹配业务规则，提高数据匹配率；
- 基于ICD-10建立全面、标准的病种分类数据库，强化医院病案管理；
- 促进跨界数据整合，推动医疗大健康生态发展。

三、医疗大数据的制度保护

建立和落实安全管理制度

- 管理与技术相辅相承
  - 人防与技防同等重要，离开管理，防护技术失效
- 建立安全制度很重要
  - 规定能做什么、不能做什么
  - 规定工作职责和安全责任
  - 规定如何做的流程
  - 规定违规后的处罚
- 落实安全制度更重要
  - 检查是否按制度落实，形成管理闭环
  - 定期检查审计日志
- 安全制度例子
  - 《数据资源管理办法》《数据安全管理制度》
  - 《数据服务管理制度》《员工守则》

建立安全风险评估与持续改进机制

- 安全风险评估
  - 参照国家标准“信息安全技术 信息安全风险评估规范”
  - 结合医疗大数据应用方式特点
  - 对数据资源分布、平台构成、数据利用过程等进行分析
  - 对可能的威胁进行识别
  - 提出针对性的防护措施
- 建立持续改进机制
  - 定期开展评估分析
  - 发现漏洞及环境变化
  - 提出改进措施
- 平衡风险与防护成本
  - 在安全与便利之间取得平衡
  - 在风险与投入之间取得平衡

依靠专业组织进行质量管控

——中国卫生信息学会健康医疗大数据医疗质量管理与监督专业委员会

（1）成立时间：2017年9月2日召开成立大会；

（2）筹建与组建：依据中国卫生信息学会章程及相关规定，“专委会”的筹备与组建工作由国家卫生计生委医院管理研究所负责完成；

（3）委员组成：专业化、多元化，第一届委员将由来自全国健康医疗领域卫生政策研究者、医疗机构管理者、医务人员、信息管理人员、计算机工程技术人员、医学科研机构、医学高等院校、相关行业企业等各界人士担任常务委员及委员。

- （4）专委会职责：
  - 将致力于健康医疗大数据在医疗质量评价、持续改进、监督体系建设等方面的理论方法与标准研究；
  - 将专注于开展健康医疗大数据在医疗质量管理与监督领域的应用研究；
  - 提升以电子病历为核心的医院信息化建设与应用水平；
  - 大力培养医疗管理与大数据应用的复合型人才；
  - 积极推动健康医疗大数据领域的国际交流与合作。

小结

数据安全是医院开展医疗大数据应用的基础性问题。医疗大数据具有用户类型复杂、访问权限随机、使用方式多样、技术多元化等特点，安全防护难度大。

医疗大数据的安全管理需要针对其风险特点，多种技术并用，技术与管理并重，监、控、管结合，实现方便应用与风险防控的统一，为医疗大数据利用保驾护航。

谢谢

Thank you

大成 DENTONS

中国
北京市
朝阳区东大桥路9号
侨福芳草地D座7层
邮编：100020

7/F, Building D
Parkview Green FangCaoDi
No.9, Dongdaqiao Road
Chaoyang District
100020, Beijing, China

大成是世界上第一家全球多中心的律师事务所，坚持超越自我，以客户需求为中心，始终如一地提供专业、全面、及时、高效的服务，荣膺“Acritas 2015全球顶尖20家精英品牌律所”称号。
我们知道，深谙本地文化对于达成交易、解决纠纷以及化解商业风险都至关重要，这促使我们深入客户业务所在的各个地区，让客户保持竞争优势。大成--全球最大的律师事务所--全球服务团队现在更加灵活，在遍及全球50多个国家超过125个地区，为个人及公共客户提供量身定制的解决方案，满足客户在本地、本国及全球的法律服务需要。

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways. Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries.
www.dentons.com.