新技术与新应用对医疗数据安全的挑战

云计算、大数据、移动互联网、穿戴式设备、BYOD、电子病历、区域卫生网路、临床数据中心、数据处理业务外包、远程医疗等一批IT新技术和新的应用模式在过去几年快速发展。它们的应用一方面创造了新的应用或商业模式，另一方面也对传统的医疗卫生数据安全带来新的挑战。

这些挑战包括：

1. 数据的所有者与数据的管理者分离。
2. 数据的生成和采集多渠道、分散化
3. 数据的用户多样化、复杂化和分散化
4. 数据的价值随着数据收集数量的增加迅速增加
5. 数据的安全愈来愈威胁连续、稳定提供医疗健康服务的安全
6. 病人隐私保护愈显重要
7. 数据的所有者管理者已超出医疗卫生行业范围外
8. 数据的互操作互联互通、共享对医疗数据安全的风险增加

IT新技术包括：

一、云计算

云计算技术通过把计算、存储、服务资源的网络虚拟化，可以改进系统的扩展性并降低部署和运营的成本。云模式开始在医疗卫生行业出现。特别是区域卫生信息化，面对众多的中小医疗机构和区域卫生数据中心，云模式有着天然的优越性，政府也加以引导和推动。云计算模式带来以下风险：

（1）公有云，基础设施由第三方市场化管理，数据高度集中，运营者成为数据安全保密的重要责任者。

（2）由于公有云由多个部门使用，如果安全管理不善，可能导致无关者获取或毁坏医疗数据。

（3）公有云部署于公共网络，医疗机构通过网络访问，增加了网络外来入侵的风险。

私有云、混合云？

二、大数据

随着信息化水平的提高，所收集的医疗数据种类越来越丰富，数据潜在的价值越来越大。过去几年，数据的科研、管理、制药、公共卫生等利用得到重视。同时，大数据及其分析利用对数据安全带来以下风险：

（1）数据利用需求增多，接触人员已远超出临床医疗人员，数据泄漏的风险也随之加大。

（2）用于分析的数据批量大、内容信息量更大，通过综合分析获得的信息价值更高，一旦泄漏，不仅涉及个人隐私，还涉及医院运营情况、地区医疗资源利用、发病及疫情等信息，泄漏损失更大。

三、移动互联网

移动计算发展方兴未艾。既有医疗机构内部医疗服务对信息化的需要，也有医疗机构外部面对居民的改进服务要求。移动互联网增加了以下安全风险：

（1）无线网络自身的安全性，由于为开放介质，易受外来攻击，通信内容较容易被截获。

（2）与公共网络连接开展面向公众的服务，给权限控制提出较高要求，受攻击和冒用的可能性增大。

四、BYOD

移动终端的发展，使医护人员使用自带设备的需求增加。管理难度和安全风险随之增加：

（1）允许BYOD，必然降低终端认证和终端安全防护，外来非法设备接入的可能性大大增加。

（2）设备在办公地点和个人混用，容易出现信息下载到个人终端，存在脱机数据安全风险。

五、穿戴式设备

穿戴式设备和医疗物联网快速发展，个人的生命体征情况处于实时监控之下。带来的风险是：

由于穿戴式设备多采用蓝牙等无线技术传输，生命体征数据泄漏的可能性增大。