

人口健康信息安全建设思考

主讲人：宁义

引言

近年来，随着国家医改深入发展，对人口健康信息化建设提出了更高的要求，我国人口健康信息化建设全面推进、快速发展，为提高卫生计生服务和管理水平发挥了重要作用，已经成为医疗卫生现代化建设不可或缺的基本要素。

在人口健康领域信息化建设快速发展过程中，伴随着信息安全的现实威胁与巨大隐患，人口健康信息安全问题也日益突出，提到重要地位上来。近年来，国家和各地区分别发布了一系列相关文件、技术标准和指南，要求大力加强卫生信息安全，各级医疗卫生机构和卫生信息人员做了大量工作，取得了一定成效。

但目前我国卫生信息安全形势依然不容乐观，特别是随着移动医疗、物联网、大数据、云计算等新技术应用，卫生信息安全面临更为复杂的局面。

人口健康信息安全建设思考

- ◆ 卫生信息安全的作用意义
- ◆ 卫生信息安全的现状
- ◆ 卫生信息安全的原因分析
- ◆ 卫生信息安全建设的对策与措施

卫生信息安全的作用意义

（一）国家信息安全的重要组成部分

大范围的卫生信息集成数据涉及到我国种族群体健康信息，除具有极高的科研和商业价值外，更涉及到种族的人类生物学特征（人群易感性、DNA攻击靶点等），这些信息在任何国家都属于核心秘密，某些别有用心的团体或人群对此极有兴趣，一旦泄露可能被用于非法用途而带来不可想象的严重后果。

国家领导人或特殊贡献人群的健康、疾病信息也对国家、社会具有重要价值，一旦泄露可能对国家政治、经济和军事安全带来严重后果，需要高度保密。

这都使得卫生信息安全具有国家安全的特性，应站在国家信息安全的高度来看待卫生信息安全问题。

卫生信息安全的作用意义

(一) 国家信息安全的重要组成部分

(二) 医疗卫生业务运行的可靠保证

信息化已经成为医疗卫生业务全领域覆盖、全流程贯通、全环节监控的基本要素，在日常业务工作中不可或缺、不可替代。如果一旦信息系统因软硬件故障而中断，医疗卫生机构将运行瘫痪、业务无法正常运行；如数据丢失损坏，同样使业务流程不能连续，诊疗信息无法利用，对医疗卫生机构和患者都构成严重的业务与经济损失。

因此，医疗卫生信息安全是业务可靠运行的“保护神”。

卫生信息安全的作用意义

(一) 国家信息安全的重要组成部分

(二) 医疗卫生业务运行的可靠保证

(三) 居民个人健康隐私的保护屏障

随着我国经济发展和人文建设的进步，个人隐私保护越来越受到国家、公众和个人的重视。居民健康与疾病信息属于个人隐私的一个部分，特别在区域卫生信息共享的条件下，如果发生医疗卫生个人隐私数据泄漏，对患者医疗安全、声誉损害和医疗机构的信誉度等都会有严重影响，有的需要承担法律责任。

因此，卫生信息安全对居民个人健康数据保护具有十分重要的作用和价值。

卫生信息安全的现状

(一) 形势很严峻

美国国际数据公司 (ICD) 在《未来图景》报告中对2015年的HIT做出预测, 其中指出卫生信息安全问题更加突显。在2015年, 约有50%的医疗机构在12个月内将遭受1—5次网络攻击, 其中三分之一攻击成功。这一预测可能不完全适用我国情况, 但其对卫生信息安全趋势和问题严重性的判断非常值得我们重视。

我国尚无专门调研卫生信息安全事件的机构和专题研究, 故缺乏较为完整、权威的相关数据。

卫生信息安全的现状

(一) 形势很严峻

1. 业务数据泄露

多为内外联手行为，其中部分涉及违法犯罪。例如：药品统方，患者或妇幼个人信息、医院运营管理数据等窃取；

典型案例：

2008年5月，香港连续爆发1.6万名病人资料、16万银行客户资料、4.4万市民个人资料等泄密事件；

同年，国内某市的孕产妇信息库泄露，含孕产妇个人信息10万余例，并将预产期内的4万多条孕妇信息制成光盘销售，一张光盘1.2万元；

近年来，全国各地多起因统方而被处理、甚至获刑的案例；

某医院工作人员向境外盗卖重要领导干部病历信息获刑。

卫生信息安全的现状

(一) 形势很严峻

1. 业务数据泄露

2. 外部入侵攻击

包括恶意攻击、木马病毒等，以及破解密码、伪造获益等。

典型案例：

2013年吉林白城一女子售卖“克隆”自某医院的优惠医疗卡1300多张，诈骗钱财2万多元；

许多医院都自行制发可预存和支付医疗费用的门诊就诊卡，其中缺乏有效的信息安全机制，密码极易破解，存在外部大量复制售卖的漏洞；后台监管不严难以发现。

卫生信息安全的现状

(一) 形势很严峻

1. 业务数据泄露

2. 外部入侵攻击

3. 软件与数据库故障

包括数据丢失、数据库死锁、服务器宕机等，几乎每个网络化信息系统的医疗卫生机构都遇到过此类事件。

典型案例：

2012年7月14日，江苏某医院信息系统数据库文件损坏、主服务器瘫痪，灾备只有1月份数据，医院业务停了3天。（是所知医院信息系统停机时间最长的事件）；

2013年7月，南方某市10天内6所（次）医院信息系统故障，主要原因是数据库死锁、服务器宕机。

卫生信息安全的现状

(一) 形势很严峻

1. 业务数据泄露
2. 外部入侵攻击
3. 软件与数据库故障

4. 网络与硬件设备故障

包括光缆、交换机、服务器、存贮设备等损坏故障，多数医疗卫生机构的信息系统都遇到过此类事件。

典型案例：

2014年11月24日，是我国首个信息安全周的第一天，就有南方、北方各1所医院信息系统发生故障而瘫痪。

卫生信息安全的现状

(一) 形势很严峻

1. 业务数据泄露
2. 外部入侵攻击
3. 软件与数据库故障
4. 网络与硬件设备故障

5. 自然或外部灾害

包括雷电、水火灾害、地震、电力故障、工程施工等损害信息系统设施设备。

典型案例：

2012年7月，南方某医院因雷击和断电，导致服务器损坏，医院信息系统瘫痪5小时后才恢复运行；

2014年9月，南方某医院建筑工程施工挖断光缆，信息系统瘫痪。

卫生信息安全的现状

(一) 形势很严峻

上述案例只是已报道的卫生信息安全事件中的冰山一角，医疗卫生机构未见诸报道的事件更是屡见不鲜，已经成为行业内的“公害”，且随着卫生信息化普及程度而日趋严重。

幸运的是，由于我国各地的区域卫生数据中心基本还在建设过程中，因此尚未见区域批量数据泄露的消息。预计随着我国区域卫生信息平台的逐步投入运行，这方面的威胁将更为严重。

卫生信息安全的现状

美国已建成的区域性卫生数据中心则已成为信息安全的焦点环节。美国HIPAA机构发布的近年10大人口健康信息泄露事件。

机构名称	泄露方式	波及人数	泄露时间
福尔斯彻奇市医疗保险公司	丢失	4901432	2011.09.13
健康网集团	丢失	1900000	2011.01.21
南岸医院	丢失	800000	2010.02.06
助力健康与医院集团	被盗	4029530	2013.07.15
田纳西州蓝十字蓝盾集团	被盗	1023209	2009.02.10
北部布朗克斯医疗网络	被盗	1700000	2010.12.23
AvMed公司	被盗	1220000	2009.12.10
内穆尔集团	被盗	1055489	2011.08.10
萨特医疗集团	被盗	943434	2011.10.15

卫生信息安全的现状

(一) 形势很严峻

(二) 政策有要求

我国信息安全是由公安部统一牵头，制订相关法规政策和督导各行业领域实施相关工作，已发布一系列相关文件与法规制度等。如：

《关于全面开展卫生行业信息安全等级保护工作的通知》、《卫生行业信息安全等级保护工作的指导意见》等，针对医疗卫生行业的信息系统的信息安全等级保护工作发出要求，指导医疗卫生行业开展等级保护建设工作。

卫生信息安全的现状

(一) 形势很严峻

(二) 政策有要求

原卫生部要求医疗卫生行业全面开展等级保护建设，其中明确要求“要根据信息系统定级备案情况开展等级测评工作，查找安全差距和风险隐患，并结合自身安全需求，制订安全建设整改方案。要于2015年12月30日前完成信息安全等级保护建设整改工作”。近期，国家卫计委再次发文，要求全国医疗卫生机构按照国家相关要求，开展信息安全等级保护工作。

5月7日，国家卫计委办公厅下发了《关于开展卫生计生领域信息安全隐患排查工作的通知》，要求采取自查、整改和抽查方式，对信息安全管理、技术防护、数据与信息系统，以及信息突发事件应急等方面进行全面排查与上报。

卫生信息安全的现状

(一) 形势很严峻

(二) 政策有要求

(三) 技术有标准

为保障信息安全等级保护制度有效实施，经公安部会同有关部门组织专家制定了包括《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》等几十个国家和部颁标准、技术指导文件，初步形成了信息安全等级保护标准体系，基本能够满足国家信息安全等级保护制度全面实施的需求。医疗卫生系统也遵循这些相关标准。

卫生信息安全的现状

- (一) 形势很严峻
- (二) 政策有要求
- (三) 技术有标准
- (四) 实际进展慢

根据国家统一部署和行业主管部门要求, 部分医疗卫生机构开始实施信息安全等级保护工作。2011年10月, 卫生部卫生监督中心顺利通过信息安全等级保护第三级测评, 成为全国第一家通过第三级测评的卫生机构; 2012年11月, 北京阜外心血管病医院顺利通过信息安全等级保护第三级测评, 成为全国第一家通过第三级测评的医院。近几年又有部分医疗卫生机构陆续通过信息安全等保测评。

卫生信息安全的现状

- (一) 形势很严峻
- (二) 政策有要求
- (三) 技术有标准
- (四) 实际进展慢

但总体来看，医疗卫生行业信息安全等保工作进展缓慢，投入较少、人才急缺、体系化建设缺口很大，信息系统未进行信息安全准备就上马、上马后也不进一步落实信息安全措施等现象比比皆是。卫生信息安全总体形势不容乐观，还有很艰巨的工作尚待完成。

卫生信息安全的原因分析

(一) 认识不到位

“先污染、后治理”，先建信息系统，后考虑信息安全问题。

“经费紧张，信息安全先放一放”。

“专业的事让专业的人去做”，“批了经费，你们自己去做吧”

各种认识误区的存在，以及面对新时期信息化快速发展中仍然存在的惯性、惰性思维，是卫生信息安全工作的最大障碍。

卫生信息安全的原因分析

(一) 认识不到位

卫生信息安全工作在具体实施中，应该认识几个要点：

1. 卫生信息安全不是单纯技术问题，更多是管理问题，“三分技术、七分管理”是信息安全规律；
2. 卫生信息安全不是单一方法问题，而是体系配套问题；
3. 卫生信息安全是动态、发展、相对的，不是固化、绝对的，适应当前需求即可；
4. 卫生信息安全不仅是信息技术人员的责任，更是卫生管理层和卫生业务人员的责任。

卫生信息安全的原因分析

(一) 认识不到位

(二) 推动力不足

任何事物发展都是动力与阻力的角力，只有推动力大于阻力，才能促进事物的发展。与信息安全的各种阻力相比，我们的推动力还显不足，需要进一步发挥我们举国体制的优势，加大行政、经济和技术综合动力，更强有力地推进卫生信息安全工作的快速发展，切实保障信息安全。

卫生信息安全的原因分析

(一) 认识不到位

(二) 推动力不足

(三) 落实跟不上

政策法规向下传递落实的关键在于执行力。目前在卫生信息安全工作方面，国家高度重视，政策相继出台，但越到基层医疗卫生机构则执行程度越低。客观因素上看，基层医疗卫生机构的经费、专业人才和技术能力等条件有限，面对卫生信息安全这类高技术要求的执行力欠缺；但主观上的认识与思维定式，才是导致落实不力更主要的因素。

卫生信息安全建设的对策与措施

(一) 大力宣传，形成重视卫生信息安全的大环境

1. 进行信息安全专项宣传。将卫生信息安全列为医疗安全的重要内容进行宣传，使医疗卫生部门和业务机构管理者高度认识信息安全对保障医疗卫生业务的价值；

2. 营造远程医疗社会氛围。通过社会媒体进行宣传，形成卫生信息安全的社会氛围，提高社会公众的整体卫生信息安全意识和关注度，社会督促与舆论监督卫生信息安全建设的落实。

卫生信息安全建设的对策与措施

(一) 大力宣传，形成重视卫生信息安全的大环境

(二) 健全规则，建立卫生信息安全法规体系

制定卫生信息安全管理规则体系，明确相关管理办法与标准制度，包括管理制度、业务流程规范、技术标准、技术运维要求与考评标准等细则，以供所有医疗卫生机构具体执行。

卫生信息安全建设的对策与措施

(一) 大力宣传，形成重视卫生信息安全的大环境

(二) 健全规则，建立卫生信息安全法规体系

制定卫生信息安全管理规则体系，明确相关管理办法与标准制度，包括管理制度、业务流程规范、技术标准、技术运维要求与考评标准等细则，以供所有医疗卫生机构具体执行。

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境**
- (二) 健全规则，建立卫生信息安全法规体系**
- (三) 强化培训，建立卫生信息安全的骨干队伍**

探索外包服务模式。鉴于卫生计生行业信息安全人才面临长期匮乏的现状，可考虑借助社会信息安全人才提供专业化支撑服务的模式。以信息安全外包合同形式，由具有国家认证资质的专业化机构或企业，承担卫生计生机构信息安全技术任务，积极探索卫生信息安全社会化保障模式。

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍

相比其他信息化程度较高的国民经济领域，卫生计生行业的信息安全需求强烈与人才匮乏的矛盾更为突出。需要下大力气，引进和培训一批本行业信息安全专业人才骨干，形成规模化队伍，作为卫生计生信息安全的基础建设。

各卫生计生机构也应根据自己信息安全实际需要，采取“送出去、请进来”的方式，引进和培训出自己的信息安全人才，保障自身信息化建设的发展。

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍
- (四) 加强管理，落实卫生信息安全配套措施

从卫生计生行业角度，要进行卫生信息安全整体设计，从政策法规、管理制度、技术标准、实施推进多方面组织系列配套工作，综合治理信息安全问题，推动卫生信息安全建设规模化、标准化、法规化发展。

从卫生计生机构角度，要依据政策法规，细化管理制度，遵从技术标准，落实具体措施，综合配套解决本单位信息安全问题，达到国家统一要求和自身业务建设需求。

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍
- (四) 加强管理，落实卫生信息安全配套措施

1. 明确任务责任。卫生计生主管部门与各医疗卫生机构签订任务责任书，将卫生信息安全基本任务指标内容列入医改信息化要求，定期表彰先进、通报后进等。未在任务时间节点达到信息安全标准要求的医疗卫生机构单位领导应问责；

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍
- (四) 加强管理，落实卫生信息安全配套措施

1. 明确任务责任。

2. 检查督导验收。由主管部门或远程医疗管理中心组织对入网医疗机构网上或现场进行项目建设、管理、应用与运维的检查督导，重点突出应用效果；

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍
- (四) 加强管理，落实卫生信息安全配套措施

1. 明确任务责任。

2. 检查督导验收。

3. 强化认证考评机制。在转变卫生信息安全观念的前提下，强有力的行政督导就成为卫生信息安全落实的关键环节。应以行政手段推进卫生信息安全等级保护制度，并列入管理考评指标体系，确保卫生计生机构按国家统一要求抓好落实。

卫生信息安全建设的对策与措施

- (一) 大力宣传，形成重视卫生信息安全的大环境
- (二) 健全规则，建立卫生信息安全法规体系
- (三) 强化培训，建立卫生信息安全的骨干队伍
- (四) 加强管理，落实卫生信息安全配套措施

1. 明确任务责任。
2. 检查督导验收。
3. 强化认证考评机制。

4. **提供专业技术指导。** 鉴于人口健康信息安全人才与技术薄弱的现状，应组织信息安全专家对各地各级卫生计生机构远程或就近划区分片巡回，指导信息安全计划方案制订，协助实施、认证和评审，以提供卫生信息安全的专业化技术指导，确保工作落实。

人口健康信息安全建设思考

谢谢！