在信息技术深入广泛应用环境下医疗卫生数据安全的政策研究

版本 V 1.0

2014年6月30日

目 录

[1. 概述、术语定义、目的范围 3](#_Toc391914452)

[ 1.1 概述及目的 3](#_Toc391914453)

[ 1.2 术语定义 3](#_Toc391914454)

[2. 新的IT技术对医疗卫生数据安全的挑战 4](#_Toc391914455)

[3. 国际上的应对与现状 4](#_Toc391914456)

[ 3.1 欧盟政策及现状 4](#_Toc391914457)

[ 3.2 美国政策及现状 6](#_Toc391914458)

[4 框架 8](#_Toc391914459)

[ 4.1 个人数据处理的原则 8](#_Toc391914460)

[ 4.2 病人的权利 8](#_Toc391914461)

[ 4.3 使用医疗隐私信息的规则 9](#_Toc391914462)

[ 4.4 相关的医疗标准的建立 9](#_Toc391914463)

[ 4.5 电子病历系统（EHR）的安全性要求 10](#_Toc391914464)

[ 4.6 保护医疗隐私信息的措施 10](#_Toc391914465)

[ 4.7 对泄露隐私行为的处罚 11](#_Toc391914466)

[ 4.8 隐私泄露报告制度 11](#_Toc391914467)

[ 4.9 建立相关监管机构 11](#_Toc391914468)

[ 4.10 HIT安全从业队伍的培养 11](#_Toc391914469)

[ 4.11 HIT 安全系统的开发 12](#_Toc391914470)

[5. 角色与权力限制Matrix 12](#_Toc391914471)

[ 5.1 病人 12](#_Toc391914472)

[ 5.2 医院 12](#_Toc391914473)

[ 5.3 医务人员 12](#_Toc391914474)

在信息技术深入广泛应用环境下医疗卫生数据安全的政策研究

# 1. 概述、术语定义、目的范围

## 1.1 概述及目的

医疗涉及到国家的根本利益，关系到民生及社会稳定。而医疗卫生数据安全一直是医疗中的重大挑战之一。随着医疗信息化、云计算及移动设备等IT技术的飞速发展，这项挑战在世界范围内都变得更加复杂和困难。

在美国，仅2013年就有超过700万份病人的记录被暴露，比2012年报道的数据增加了138%。所有数据持有者、病人、医生和保险公司面临的保护医疗数据隐私及安全的负担越来越大。

我国医疗信息化的起步较晚，相关法律法规，技术标准都还没建立，面临的形势更为严峻。诸如信息保护的概念及信息类型（哪些信息需要保护）、保护的目的、保护的技术手段等最基础性问题都急待解决。

本报告的目的是研究国内外IT技术对医疗卫生数据安全的挑战，并借鉴欧美等发达国家的应对策略，提出适合我国国情的解决方案。本报告只研究规范，提出管理办法草案，对于法律、惩罚的界定不予考虑。

报告首先对信息安全的术语进行定义；紧接着介绍新的IT技术对医疗卫生数据安全的挑战；第三章研究国际上应对这些挑战的途径，以及现状；第四章提出了我国医疗卫生数据安全的框架；最后一章列举了医疗行业的不同角色（医生、卫生局、医院、数据提供者、患者等）涉及到的具体医疗数据安全的问题，以及相应的权利限制措施。

以下是本报告中所使用到的术语的定义：

## 1.2 术语定义

**隐私（Privacy）**

个人控制自己的医疗信息披露的意愿。（个人隐私的内容涉及到生活的多方面，本报告特指个人的医疗信息。）

**安全（Security）**

保护个人隐私和机密的政策、流程以及保障措施。

**受保护的医疗信息**（protected health information，简称**PHI**）

PHI指的是任何**含有个人身份标识的医疗信息**。

PHI包含口头的、书面的、录音或者电子信息（传真、Email）等格式。个人身份标识（18类）指以下的信息：病人姓名，邮编地址，所有日期信息，电话号码，传真号码，Email地址，个人网站，IP地址，社保卡号，其他卡号，证件号码，病历号码，医保信息，设备标识及序列号，车牌号，生物标示符（指纹及声音），可识别的照片，其他的唯一身份标识号码及特征。

**受保护的电子医疗信息**（Electronic Protected Health Information，简称**E-PHI**）

E-PHI指的是任何以电子形式保存的受保护的电子医疗信息（PHI）。

# 2. 新的IT技术对医疗卫生数据安全的挑战

由薛万国完成。

# 3. 国际上的应对与现状

目前世界许多国家都在积极研究应对医疗卫生数据安全的策略。长期以来，欧盟和美国走在了个人信息安全和隐私保护的前列。本报告重点对欧洲和美国的医疗信息安全方面的措施和现状进行分析，以便借鉴学习。

## 3.1 欧盟政策及现状

根据欧盟法规，任何可识别的自然人的信息均为“个人数据”。个人数据必须依照相关的个人信息保护法规中规定的法律框架予以保护。其中个人健康信息属于敏感数据范畴，必须加以严格保护和监管。

其中，欧盟在1995年颁布的个人信息数据保护法案构筑了个人数据保护历史上的里程碑。此法案的基本原则，旨在确保欧盟内部市场的正常运作情况下对个人数据和个人基本权利的有效保护。它于近20年前制定，在今天依然有效。

欧盟现行的个人信息保护法案包括：

* **欧洲人权公约**（European Convention on Human Rights of 1953，简称ECHR)。ECHR第八条规定尊重“个人的隐私，家庭生活，住宅及信件”的权利。
* 个人信息**数据保护法案**（Data Protection Directive 95/46/EC）由欧洲议会和理事会在1995年10月24日颁布。其法案调了欧盟成员国的相关国家法律，要求“数据控制者”需要保障高质量的个人数据保护和管理实践，以及一系列的保障个人权利的规定。
* **隐私和电子通信法案**（ePrivacy Directive 2002/58/EC）于2002年7月12日颁布的隐私和电子通信法案保障个人资料的处理和在电子通讯业中保护个人隐私。
* European Commission Directive 95/46/EC (EC, 2007)。该法律有严格的规则，只允许在病人同意或高度具体的情况下(如：法律义务，公共医疗的必要性)进行医疗数据处理。
* 欧盟理事会于2008年11月27日颁布的框架决定（2008/977/JHA）针对警察和刑事事项的司法合作框架处理个人数据的保护做出了相关规定。
* 2000年12月18日颁布的针对社区机构和团体处理个人数据的保护规章（Regulation 45/2001）并且对由社区机构和团体处理个人数据过程中产生的个人数据的自由流动提出了规定。
* 此外，数据保留法案（Data Retention Directive 2006/24/EC），针对在公共通信网络与公共电子通信服务产生或处理的数据的保留问题予以详细的规定。这也是欧洲议会和理事会于2006年3月15日对法案2002/58/EC进行的合并修订。

当前问题是每个欧盟国家实施法律的方式不同导致了个人数据保护水平参差不齐 ——这取决于个人在哪个成员国生活或消费。另外由于目前的规则在制定的时候互联网还处于起步阶段，此法规也需要现代化的改革。技术的迅速发展和全球化带来一系列数据保护的新挑战。随着社交网站，云计算，基于位置的服务（location-based services）和可穿戴设备的推广，我们每一个举动都留下数字轨迹。在这个“勇敢新数据世界”里，我们需要一个强大而统一的规则。

欧盟目前正在推进数据保护的改革，旨在推进欧盟范围内统一的新法案，面向未来发展趋势并适合于数字时代。针对新法案——**通用数据保护条例**（General Data Protection Regulation）——欧洲议会和部长理事会于2012年1月之后提出了众多的修正案，计划在2014年实行，并在两年过渡期后生效，用来取代现行的**数据保护法案**。

另外，关于欧盟的个人数据转移到欧盟以外的区域，美国商务部和欧盟委员会针对就数据保护原则和常见问题达成了一致意见，相互认“**安全港原则**”（Safe Harbor Principles）。基于此的安全港认证确使个人数据被美国公司从欧洲经济区（EEA）转移到美国时遵守欧盟法律规定，并且美国公司为这些个人信息提供充分的保护。

## 3.2 美国政策及现状

和欧盟类似，美国也出台了众多的法律法规来保护病人信息的隐私及安全。

1996年，克林顿政府签署了经过参议院和众议院通过的医疗保险改革法案：**HIPAA**/1996，Public Law 104-191. HIPAA要求医疗服务部为特定医疗信息的电子传输制定全国统一的标准。这是美国医改历史上里程碑式的立法。HIPAA主要解决了以下问题：

* 为了确保换工作的人仍然有获得高质量的医疗保健的覆盖面。因为在过去，很难或根本无法更改，尤其在换工作的时候；
* 医疗数据的安全和隐私问题，以及数据交换；
* 预防医疗欺诈和滥用，行政简化，医疗责任改革。

HIPAA隐私法建立业务流程来保护**受保护的医疗信息**（protected health information，以下简称**PHI**）的使用和披露。HIPAA隐私法的生效日期是2003年4月14日。

**《美国复苏与再投资法案》**（American Reinvestment and Recovery Act of 2009，简称**ARRA**）于2009年9月23日生效，它为医疗、教育、住房等各方面规定了资金数量，为医疗方面总共提供了**1551亿美元**的资金。**HITECH**法是ARRA中的一部分内容（DIVISION A: TITLE XIII以及DIVISION B: TITLE IV）。HITECH扩展了HIPAA对商业组织的隐私和安全的条款，包括了最新的对商业组织的民事和刑事处罚，它还包括了同这些商业组织签协议的任何商业组织。

ARRA是美国医改的又一里程碑。HITECH Act为采用EHR的医师提供了奖金，旨在吸引更多的人采用EHR技术（即**EHR奖励计划**或Meaningful Use，简称**MU**）。Medicare 和 Medicaid EHR奖励计划将为EPs，EHs和CAHs提供奖金，前提是他们要“adopt, implement, upgrade or demonstrate”（采用，实施，更新或者演示）经认证的EHR技术。ARRA对HIPAA的安全及隐私法规进行了加强，加重了惩罚力度，并增加了对个人身份盗用的保护等条款。

美国医疗相关的法规罗列如下：

* **隐私法**【The Privacy Act of 1974 (PL 93-579)】。该法律旨在建立一套公平的信息实践代码，用于管理带有个人标识的信息的收集、维护、使用和传播，这些信息在联邦机构的记录中进行维护。
* **计算机安全法**【The Computer Security Act of 1987 (PL 100-235)】。该法律旨在提高联邦计算机系统中敏感信息的安全性和保密性，以及为这样的系统建立一个最低可接受的安全措施。它要求创建计算机安全计划，并为敏感信息系统的用户或者所有者提供适当的培训。
* **计算机反欺诈和滥用法**【The Computer Fraud and Abuse Act of 1986 (PL 99-474)】 该法初次颁布于1986年，该法的主要目的是保护联邦政府以及金融和医疗机构等“受保护的计算机”。该法禁止为了获取敏感信息如有关国防的信息、金融和消费者信用记录等信息，未经授权而进入“受保护计算机系统”。非法买卖传输由美国政府使用的或者为美国政府服务的计算机的口令密码的行为，也在被禁之列。该法是惩处计算机欺诈和与计算机有关的犯罪行为，被称为惩治计算机黑客犯罪的里程碑。曾进行过多次修订或补充。
* **医保流通和责任法案**【Health Insurance Portability and Accountability Act of 1996 (PL 104-191)，即HIPAA】。
* **反基因歧视法**【Genetic Information Nondiscrimination Act of 2008 (GINA)】。该法在2008年5月底，由美国总统布什签署。该法禁止人寿保险公司以某人具有对某种疾病的易感基因为由，取消、拒绝对他进行保险或提高保险费用。同时，此项由美国白宫和参议院通过的法令禁止雇主以遗传信息为依据进行雇佣、解聘、升职、加薪，或做出任何与雇佣行为有关的决定。
* **经济和临床医疗的医疗信息技术法案**【Health Information Technology for Economic and Clinical Health Act of 2009，即HITECH】。
* **患者保护与平价医疗法案**（Patient Protection and Affordable Care Act，简称**PPACA**），通常也被称作奥巴马医疗法案，是由美国总统奥巴马在2010年签署的一个联邦法。这部法案的主要目的是由美国政府主导增加美国人民的医疗保险覆盖率以及降低美国的医疗费用。根据平价医疗法案，美国的医疗保险市场将发生重大改变。主要是联邦政府和州政府将建立政府医疗保险市场（Health Insurance Exchange），允许个人和小企业在政府的医疗保险市场为个人／家庭和企业员工购买医疗保险。从2014年起，没有医疗保险的个人，或者符合条件的雇主不提供医疗保险，政府将给予罚款。

当然，美国医疗信息化及EHR的发展中也面临着不少问题。例如：

* 隐私概念的精确定义。隐私的概念在网络飞速发展的情况下很难精确定义，权利和义务有时候模棱两可，富有争议。
* 每个诊所的医疗信息交换的独特性（人员结构、软硬件、工作流及管理方式、人际关系、资金等）及多样性，使得安全及隐私问题变得困难。
* 医疗数据的多样性及标准问题等。

**我国**的医疗信息安全起步晚，发展较缓慢。除了面临美国同样的问题外，还面临以下更实际的问题：

* 医疗法律的缺失及滞后；
* 全国性医疗标准的空白；
* 执法机构及标准管理机构的建立；
* 医疗文化的建立；
* 地方垄断主义；
* 资金的缺乏等。

综上，我国应该借鉴欧美在医疗信息安全方面取得的成果及面临的困难，通过总结和思考，提出适合我国国情的解决方案。

# 4 框架

医疗数据的安全涉及到方方面面，如何进行保护是个复杂的问题。

以下就从数据处理的原则，病人的权利，医疗信息使用的规则，医疗系统的标准，保护医疗隐私的措施等多方面进行全面的讨论。

## 4.1 个人数据处理的原则

* **1.** **数据采集限制原则。**个人数据的采集应该有限制，并且任何此类数据都应通过合法和公平的方式进行,在适当的地方要经过个人知情或同意。
* **2. 数据质量原则。**个人数据的采集在某种程度上应该与使用目的一致，并且数据应该是准确、完整和最新的。
* **3.** **目的明确原则。**收集个人资料的目的应不迟于数据收集的开始，随后的数据使用仅限于实现这些目的；目的不符合或者改变时候，每次都要做出具体说明。
* **4.** **使用限制原则。**除了事先同意，或者法律的授权以外，不能泄露个人数据或者用于其他目的。
* **5.** **安全保护原则。**个人数据应该采取安全措施受到合理保护，防范各种风险（例如：丢失，未经授权的访问、破坏、修改等）。
* **6. 公开性原则。**这应该是数据收集和使用的总体方针，体现了尊重个人数据的原则。这意味着建立个人资料的途径和性质，数据使用的主要目的，数据控制者的身份及场所应该是现成的。
* **7.** **个人参与原则。**个人应该有权获得及交流与自己相关的数据(在合理的时间内,可接受的费用，并且是简单易懂的形式)；个人能够挑战拒绝他的请求的行为；个人应该能质疑有关的数据，如果挑战成功，用户可以删除、纠正、完善或修改自己的数据。
* **8. 责任义务原则。**应该有数据控制者负责监督指标的遵守情况，以及指标对上述原则产生的影响。

## 4.2 病人的权利

病人对自己的医疗信息应获得如下的权利：

* 有权要求补充修改医疗记录；
* 有权访问PHI；
* 有权请求了解他们的PHI在过去的披露情况；
* 有权利投诉违反隐私和安全行为。

## 4.3 使用医疗隐私信息的规则

采用如下规则使用病人的信息：

* 最低限度的使用和披露病人的医疗信息；
* 要求医疗提供者获得病人签署的知情同意书，以便在**治疗、付款和医疗保险**中使用和披露病人的医疗信息。
* 医院从现有资源中及时获取的信息能支持**医疗、教育、科研及管理工作**；
* 任何**其他目的**（如：市场营销）中使用或披露PHI需要**单独授权**。
* 医院制定有关记录、资料和信息保存期限的制度。（患者病历资料、信息必须保存足够长的时间，以符合法律、法规要求，并满足患者服务、医院管理、法律记录、科研和教育的需求。）
* 当保存期限结束时，可以对病历、其他资料、信息进行适当的销毁。
* 其他规则。

## 4.4 相关的医疗标准的建立

借鉴美国及国际的先进标准，建立国内的医疗标准（词汇标准，内容交换标准及安全标准等）。

|  |  |  |
| --- | --- | --- |
| 标准分类 | 标准名 | 备 注 |
| **信息安全标准** | 医疗信息加密和解密 | 待定 |
| 授权管理。（制度和程序规定只有经过授权的人员，才能获取数据和信息，并在工作职责和内容上做出定义，包括医院实习的学生。） | 待定 |
| 记录医疗信息相关的操作（用户登录记录以及用户进行的增删查改操作。） | 待定 |
| 验证医疗信息在传输中没有发生改变 | 待定 |
| 制度规定各类数据信息的安全级别。 | 待定 |
| **词汇标准** | RxNorm, ICD-10-CM, SNOMED CT, LOINC等 | 待定 |
| **内容交换标准** | CCD/CCR，HL7等。（以利于医疗信息在不同系统及机构间的顺利交流。） | 待定 |
| **标准升级维护** | 根据现实及实施情况，对采用的标准进行版本升级及更新。 | 待定 |

## 4.5 电子病历系统（EHR）的安全性要求

借鉴美国的标准，对EHR/EMR系统的隐私及安全采用以下标准：

* **访问控制**。提供唯一的用户名/号码用于标识及跟踪用户身份，并且进行控制，只有授权的用户可以访问医疗信息。
* **紧急登录**。允许授权的用户(有紧急情况授权)在紧急情况下访问电子医疗信息。
* **自动登出**。一段预定的时间内不活动的话（通常为5分钟），账号自动登出。
* **系统审计日志**。
	+ (1)记录用户行为。（在创建、修改、访问、删除电子记录信息的时候必须自动记录如下信息：日期、时间、病人的ID，用户的ID，以及进行的操作。）
	+ 生成修改的日志。用户可以基于具体的时间来生成日志，并根据日期、时间、病人的ID，用户的ID，以及进行的操作来进行排序。
* **信息完整性验证**。消息传输和验证的时候要使用安全的哈希算法。哈希算法的版本为SHA-1或者更高。
* **验证授权**。验证访问电子医疗信息的用户或实体是经授权的用户。
* **一般加密**。通常使用一个对称的128位固块加密算法，算法使用128，192或者256位的密钥。
* **信息交换加密**。
* **对信息的披露负责**。记录在治疗，支付和医疗操作中的信息的披露。

## 4.6 保护医疗隐私信息的措施

除了医疗软件自身的安全设计外，医疗机构必须采取**相应的管理措施**来保护其持有的病人医疗信息的完整性（特别是电子化的受保护的健康信息，即**e-PHI**）。防止未经授权泄露隐私（例如：发送数据丢失或破坏事故，有意偷窃，或由于失误而发送给错误等）。

可以借鉴美国推出以下三种保障措施：

* **行政管理措施**（如：访问医疗信息、用户名及密码的政策和程序，员工安全意识培训，应急方案，资料和信息保存期限的制度，资料销毁制度，或者违反法律的惩罚措施等）；
* **物理措施**（(如：报警及监控措施，房间和储存设施的上锁等)；
* **技术措施**（如：电子数据的加密，使用数字签名来验证用户登录身份，审计日志等）。

## 4.7 对泄露隐私行为的处罚

对于违反规定，将病人隐私泄露的行为进行民事以及刑事处罚。

## 4.8 隐私泄露报告制度

医院及其商业伙伴，在PHI泄密之后要向相关部门进行报告。

如果病人觉得自己的PHI未经允许而泄露了，可以进行投诉。

## 4.9 建立相关监管机构

建立相关的政策、法律法规、标准的制定及监管部门。

由于法律制定的范畴超出了范围，本报告对于法律、惩罚的界定不予考虑。

## 4.10 HIT安全从业队伍的培养

在中国职业序列里加入“医疗信息安全执业师”，借鉴美国医疗信息安全与隐私执业师培训与认证的经验，建立起我们自己的医疗信息安全执业师培训与认证体系。

## 4.11 HIT 安全系统的开发

美国已有一批此类软件系统的厂商，中国几乎为空白，此领域的发展空间很大。

# 5. 角色与权力限制Matrix

由赵韡完成。

## 5.1 病人

## 5.2 医院

## 5.3 医务人员

-------------------------------------本文档到此结束！-------------------------------------