HNSF
Health Network Security Forum 2017
医疗网络安全论坛

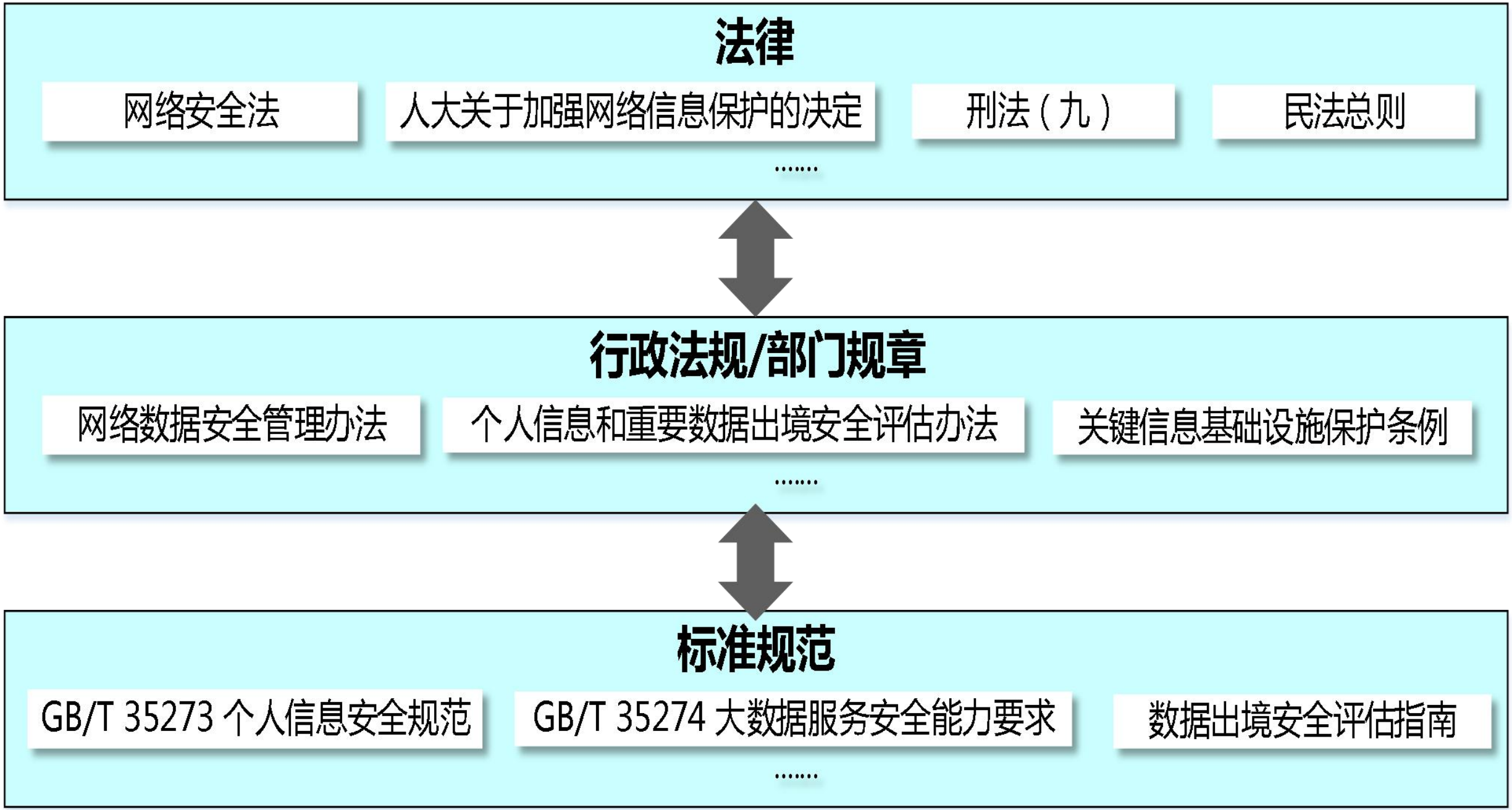
健康医疗数据安全指南

金涛

国家信安标委大数据安全标准特别工作组
大数据系统软件国家工程实验室
清华大学软件学院

提纲

- 背景介绍
- 标准定位
- 主要内容
- 意见处理
- 后续计划


法律
网络安全法
人大关于加强网络信息保护的决定
刑法（九）
民法总则
.....
行政法规/部门规章
网络数据安全管理办法
个人信息和重要数据出境安全评估办法
关键信息基础设施保护条例
.....
标准规范
GB/T 35273 个人信息安全规范
GB/T 35274 大数据服务安全能力要求
数据出境安全评估指南
.....

安全是发展的前提，发展是安全的保障

安全为先、保护隐私

标准是前提，安全是保障，服务是目的

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

坚持规范有序、安全可控。建立健全健康医疗大数据开放、保护等法规制度，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。

13. 加强健康医疗数据安全保障。加快健康医疗数据安全体系建设，建立数据安全管理责任制度，制定标识赋码、科学分类、风险分级、安全审查规则。制定人口健康信息安全规划，强化国家、区域人口健康信息工程技术能力，注重内容安全和技术安全，确保国家关键信息基础设施和核心系统自主可控稳定安全。开展大数据平台及服务商的可靠性、可控性和安全性评测以及应用的安全性评测和风险评估，建立安全防护、系统互联共享、公民隐私保护等软件评价和安全审查制度。加强大数据安全监测和预警，建立安全信息通报和应急处置联动机制，建立健全“互联网+健康医疗”服务安全工作机制，完善风险隐患化解和应对工作措施，加强对涉及国家利益、公共安全、患者隐私、商业秘密等重要信息的保护，加强医学院、科研机构等方面的安全防范。

健康中国是国家战略

中共中央 国务院印发
《“健康中国2030”规划纲要》

式，持续推进覆盖全生命周期的预防、治疗、康复和自主健康管理一体化的国民健康信息服务。实施健康中国云服务计划，全面建立远程医疗应用体系，发展智慧健康医疗便民惠民服务。建立人口健康信息化标准体系和安全保护机制。做好公民入伍前与退伍后个人电子健康档案军地之间接续共享。到2030年，实现国家省市县四级人口健康信息平台互通共享、规范应用，人人拥有规范化的电子健康档案和功能完备的健康卡，远程医疗覆盖省市县乡四级医疗卫生机构，全面实现人口健康信息规范管理和使用，满足个性化服务和精准化医疗的需求。

第二节　推进健康医疗大数据应用

加强健康医疗大数据应用体系建设，推进基于区域人口健康信息平台的医疗健康大数据开放共享、深度挖掘和广泛应用。消除数据壁垒，建立跨部门跨领域密切配合、统一归口的健康医疗数据共享机制，实现公共卫生、计划生育、医疗服务、医疗保障、药品供应、综合管理等应用信息系统数据采集、集成共享和业务协同。建立和完善全国健康医疗数据资源目录体系，全面深化健康医疗大数据在行业治理、临床和科研、公共卫生、教育培训等领域的应用，培育健康医疗大数据应用新业态。加强健康医疗大数据相关法规和标准体系建设，强化国家、区域人口健康信息工程技术能力，制定分级分类分域的数据应用政策规范，推进网络可信体系建设，注重内容安全、数据安全和技术安全，加强健康医疗数据安全保障和患者隐私保护。加强互联网健康服务监管。

规划发展与信息化司

强化标准、确保安全。按照法规为本、标准先行，安全为上、保护隐私的要求，妥善处理应用发展与安全保障的关系，健全政策法规标准体系和信息安全保障体系，增强安全技术支撑能力，确保应用有序推进，信息安全可控。

国家卫生计生委关于印发“十三五”全国人口健康信息化发展规划的通知

5.强化人口健康信息化和健康医疗大数据安全防护体系建设。坚持网络安全与信息化工作同谋划、同部署、同推进、同实施，加快制定人口健康信息化和健康医疗大数据管理办法等法规政策制度，加大技术保障力度，强化信息安全管理。按照相关政策法规要求，贯彻国家信息安全等级保护制度、分级保护制度和信息安全审查制度，完善安全管理机制。制定人口健康网络与信息安全规划及健康医疗大数据安全管理办法，加快健康医疗大数据安全体系建设，制定标识赋码、科学分类、风险分级、安全审查规则，落实《卫生计生行业国产密码应用规划》，推进国产密码在安全体系中的应用。定期开展网络安全风险评估，强化容灾备份工作，完善安全保障体系和运行维护方案，提高行业整体网络安全事件监测及动态感知能力。完善涉及居民隐私的信息安全体系建设，实现信息共享与隐私保护同步发展，确保系统运行安全和信息安全。

索 引 号：	000014349/2018-00061	主题分类：	卫生、体育\卫生
发文机关：	国务院办公厅	成文日期：	2018年04月25日
标　　题：	国务院办公厅关于促进“互联网+医疗健康”发展的意见		
发文字号：	国办发〔2018〕26号	发布日期：	2018年04月28日
主 题 词：			

（十四）保障数据信息安全。

1.研究制定健康医疗大数据确权、开放、流通、交易和产权保护的法规。严格执行信息安全和健康医疗数据保密规定，建立完善个人隐私信息保护制度，严格管理患者信息、用户资料、基因数据等，对非法买卖、泄露信息行为依法依规予以惩处。（国家卫生健康委员会、国家网信办、工业和信息化部、公安部负责）

2.加强医疗卫生机构、互联网医疗健康服务平台、智能医疗设备以及关键信息基础设施、数据应用服务的信息防护，定期开展信息安全隐患排查、监测和预警。患者信息等敏感数据应当存储在境内，确需向境外提供的，应当依照有关规定进行安全评估。（国家卫生健康委员会、国家网信办、工业和信息化部负责）

规划发展与信息化司

关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知

发布时间： 2018-09-13

国卫规划发〔2018〕23号

第三章 安全管理

第十六条 健康医疗大数据安全管理是指在数据采集、存储、挖掘、应用、运营、传输等多个环节中的安全和管理，包括国家战略安全、群众生命安全、个人信息安全的权责管理工作。

第十七条 责任单位应当建立健全相关安全管理制度、操作规程和技术规范，落实“一把手”责任制，加强安全保障体系建设，强化统筹管理和协调监督，保障健康医疗大数据安全。

涉及国家秘密的健康医疗大数据的安全、管理和使用等，按照国家有关保密规定执行。责任单位应当建立健全涉及国家秘密的健康医疗大数据管理与使用制度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

第十八条 责任单位应当采取数据分类、重要数据备份、加密认证等措施保障健康医疗大数据安全。责任单位应当建立可靠的数据容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复，实现长期保存和历史数据的归档管理。

第十九条 责任单位应当按照国家网络安全等级保护制度要求，构建可信的网络安全环境，加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力，确保健康医疗大数据关键信息基础设施和核心系统安全可控。健康医疗大数据中心、相关信息系统等均应开展定级、备案、测评等工作。

第二十条 健康医疗大数据相关系统的产品和服务提供者应当遵守国家有关网络安全审查制度，不得中断或者变相中断合理的技术支持与服务，并应当为健康医疗大数据在不同系统间的交互、共享和运营提供安全与便利条件。

第二十一条 责任单位应当依法依规使用健康医疗大数据有关信息，提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全。

第二十二条 责任单位应当按照《中华人民共和国网络安全法》的要求，严格规范不同等级用户的数据接入和使用权限，并确保数据在授权范围内使用。任何单位和个人不得擅自利用和发布未经授权或超出授权范围的健康医疗大数据，不得使用非法手段获取数据。

第二十三条 责任单位应当建立严格的电子实名认证和数据访问控制，规范数据接入、使用和销毁过程的痕迹管理，确保健康医疗大数据访问行为可管、可控及服务管理全程留痕，可查询、可追溯，对任何数据泄密泄露事故及风险可追溯到相关责任单位和责任人。

第二十四条 建立健全健康医疗大数据安全管理人才培养机制，确保相关从业人员具备健康医疗大数据安全管理所要求的知识和技能。

第二十五条 责任单位应当建立健康医疗大数据安全监测和预警系统，建立网络安全通报和应急处置联动机制，开展数据安全规范和技术规范的研究工作，不断丰富网络安全相关的标准规范体系，重点防范数据资源的集聚性风险和新技术应用的潜在性风险。发生网络安全重大事件，应当按照相关法律法规和有关要求进行报告并处置。

关于印发互联网诊疗管理办法（试行）等3个文件的通知

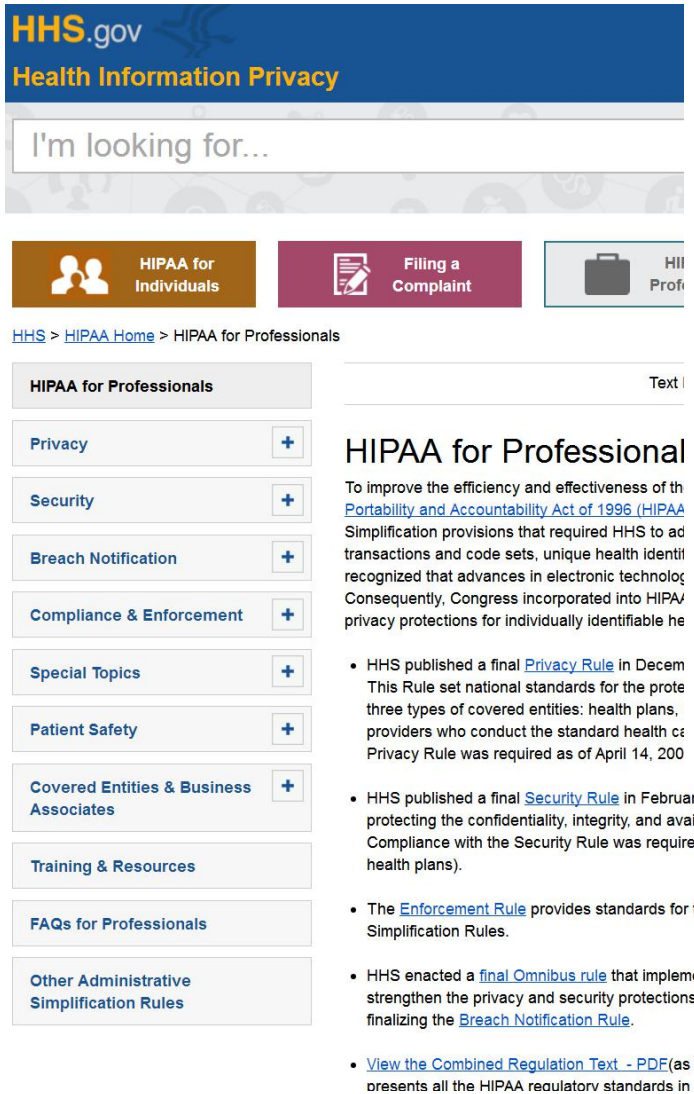
发布时间： 2018-09-14

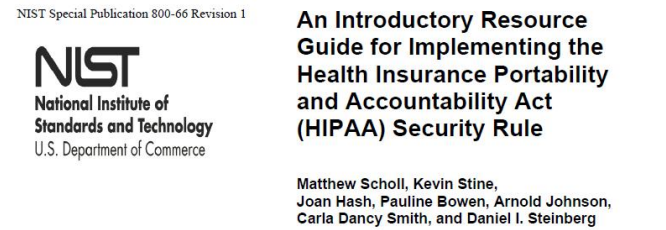
国卫医发〔2018〕25号

各省、自治区、直辖市及新疆生产建设兵团卫生计生委、中医药管理局：

为贯彻落实《国务院办公厅关于促进“互联网+医疗健康”发展的意见》有关要求，进一步规范互联网诊疗行为，发挥远程医疗服务积极作用，提高医疗服务效率，保证医疗质量和医疗安全，国家卫生健康委员会和国家中医药管理局组织制定了《互联网诊疗管理办法（试行）》、《互联网医院管理办法（试行）》、《远程医疗服务管理规范（试行）》，现印发给你们，请遵照执行。

国外法规标准代表


HHS.gov
Health Information Privacy
I'm looking for...
HIPAA for Individuals
Filing a Complaint
HHS > HIPAA Home > HIPAA for Professionals
HIPAA for Professionals
Privacy
Security
Breach Notification
Compliance & Enforcement
Special Topics
Patient Safety
Covered Entities & Business Associates
Training & Resources
FAQs for Professionals
Other Administrative Simplification Rules
HIPAA for Professional
To improve the efficiency and effectiveness of th
Portability and Accountability Act of 1996 (HIPAA
Simplification provisions that required HHS to ad
transactions and code sets, unique health identi
recognized that advances in electronic technolog
Consequently, Congress incorporated into HIPA
privacy protections for individually identifiable he
HHS published a final Privacy Rule in Decem
This Rule set national standards for the prote
three types of covered entities: health plans,
providers who conduct the standard health ca
Privacy Rule was required as of April 14, 200
HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.
HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.
View the Combined Regulation Text - PDF(as of March 2013). This is an unofficial version that presents all the HIPAA regulatory standards in one document. The official version of all federal

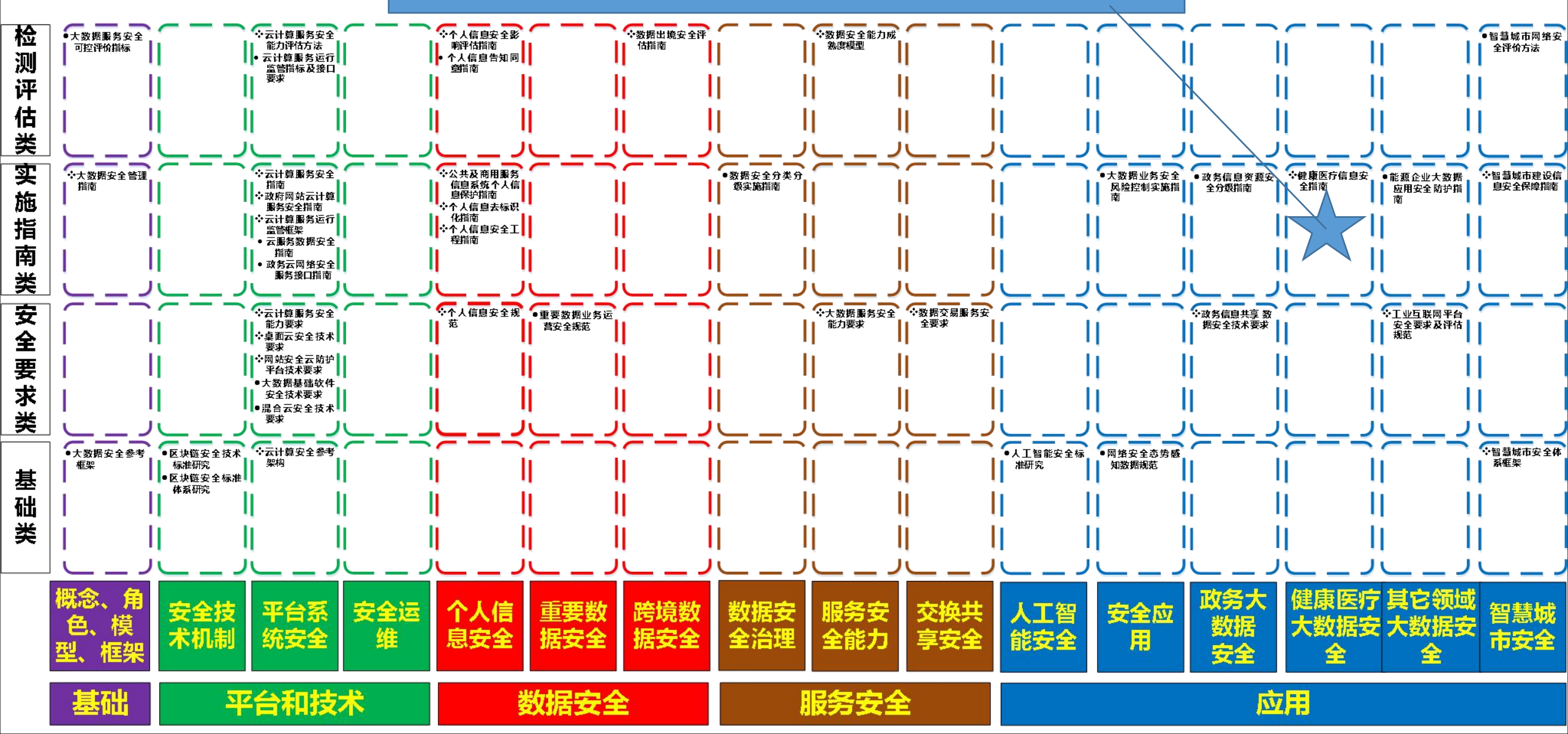

NIST Special Publication 800-66 Revision 1
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg
INFORMATION SECURITY


INTERNATIONAL STANDARD
ISO 27799
Second edition
2016-07-01
Health informatics — Information security management in health using ISO/IEC 27002


Computer Security Division
Information Technology Laboratory
National Institut
Gaithersburg, M
October 200
U.S. Departm
Carlos M. Gutier
National Inst
Patrick D. Gallag


标准化研究
Standardization Research
编辑：胡欣
E-mail: huxin@cesi.cn
个人健康信息保护标准综述
Review of Personal Health Information Protection Standards
清华大学[1] 中国电子技术标准化研究院[2]
周梦颖[1] 金 涛[1] 何延哲[2]
摘 要 通过分析国际标准化组织 (ISO)、欧盟标准化委员会 (CEN)、英国健康部门发布的个人健康信息安全的标准与规则，以及美国健康保险流通与责任法 (HIPAA) 的安全与隐私部分，总结出在安全管理、物理安全、安全技术与安全审计四个维度上个人健康信息的要求，对制定符合我国特色的健康信息保护标准提供借鉴。
关键词 健康信息 保护 标准 大数据 安全管理 物理安全 安全技术 安全审计

健康医疗数据安全指南


检测评估类
实施指南类
安全要求类
基础类
大数据服务安全可控评价指标
云计算服务安全能力评估方法
云计算服务运行监管指标及接口要求
个人信息安全影响评估指南
个人信息告知同意指南
数据出境安全评估指南
数据安全能力成熟度模型
智慧城市网络安全评价方法
大数据安全管理指南
云计算服务安全指南
政府网站云计算服务安全指南
云计算服务运行监管框架
云服务数据安全指南
政务云网络安全服务接口指南
公共及商用服务信息系统个人信息保护指南
个人信息去标识化指南
个人信息安全工程指南
数据安全分类分级实施指南
大数据业务安全风险控制实施指南
政务信息资源安全分级指南
健康医疗信息安全指南
能源企业大数据应用安全防护指南
智慧城市建设信息安全保障指南
云计算服务安全能力要求
桌面云安全技术要求
网站安全云防护平台技术要求
大数据基础软件安全技术要求
混合云安全技术要求
个人信息安全规范
重要数据业务运营安全规范
大数据服务安全能力要求
数据交易服务安全要求
政务信息共享 数据安全技术要求
工业互联网平台安全要求及评估规范
大数据安全参考框架
区块链安全技术标准研究
区块链安全标准体系研究
云计算安全参考架构
人工智能安全标准研究
网络安全态势感知数据规范
智慧城市安全体系框架
概念、角色、模型、框架
安全技术机制
平台系统安全
安全运维
个人信息安全
重要数据安全
跨境数据安全
数据安全治理
服务安全能力
交换共享安全
人工智能安全
安全应用
政务大数据安全
健康医疗大数据安全
其它领域大数据安全
智慧城市安全
基础
平台和技术
数据安全
服务安全
应用

健康医疗数据特点

- 生命健康强相关 —— 安全保护程度要高
- 高度敏感 —— 隐私保护力度要大
- 专业性强 —— 使用披露方面差异
- 公共福祉 —— 并不完全“私”
- 国家安全相关 —— “不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器”

个人信息安全原则的适配

- 权责一致原则
- 目的明确原则：探索性
- 选择同意原则：专业性
- 最少够用原则：难界定
- 公开透明原则
- 确保安全原则
- 主体参与原则：不能随意删除

信息高度不对称

健康医疗领域业务复杂

有时治愈，常常帮助，总是安慰

健康医疗信息安全指南标准定位

个人信息安全规范、大数据服务安全能力要求、
信息安全管理体系

健康医疗数据安全指南

重要数据管理　　涉密分级保护　　数据出境评估

等级保护
信息安全控制实践指南

云安全

标准拟解决问题

- 底线：什么能做，什么不能做？
  - 健康医疗数据使用和披露的原则要求

- 数据安全保护指导思想
  - 健康医疗数据分类分级，各级安全要点
  - 使用场景分类，各类场景安全要点
  - 开放形式分类，不同开放形式安全要点
  - 安全管理指南：组织保障、PDCA、应急体系
  - 安全技术指南：通用安全技术指南、去标识化指南
  - 各种常见典型场景数据安全重点措施

重要术语定义

- 个人健康医疗数据（保护内容）
  - 单独或者与其他信息结合后能够识别特定自然人或者反映特定自然人生理或心理健康的相关数据。
  - 个人健康医疗数据涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和支付的医疗保健服务费用等。
- 个人健康医疗数据主体（保护对象）
  - 个人健康医疗数据所标识的自然人。
- 健康医疗数据控制者（规范对象）
  - 能够决定健康医疗数据处理目的、方式及范围等的组织或个人。包括提供健康医疗服务的组织、医保机构、政府机构、健康医疗科学研究机构、个体诊所等，其以电子形式传输或处理健康医疗数据。

安全目标

保密性、完整性、可用性

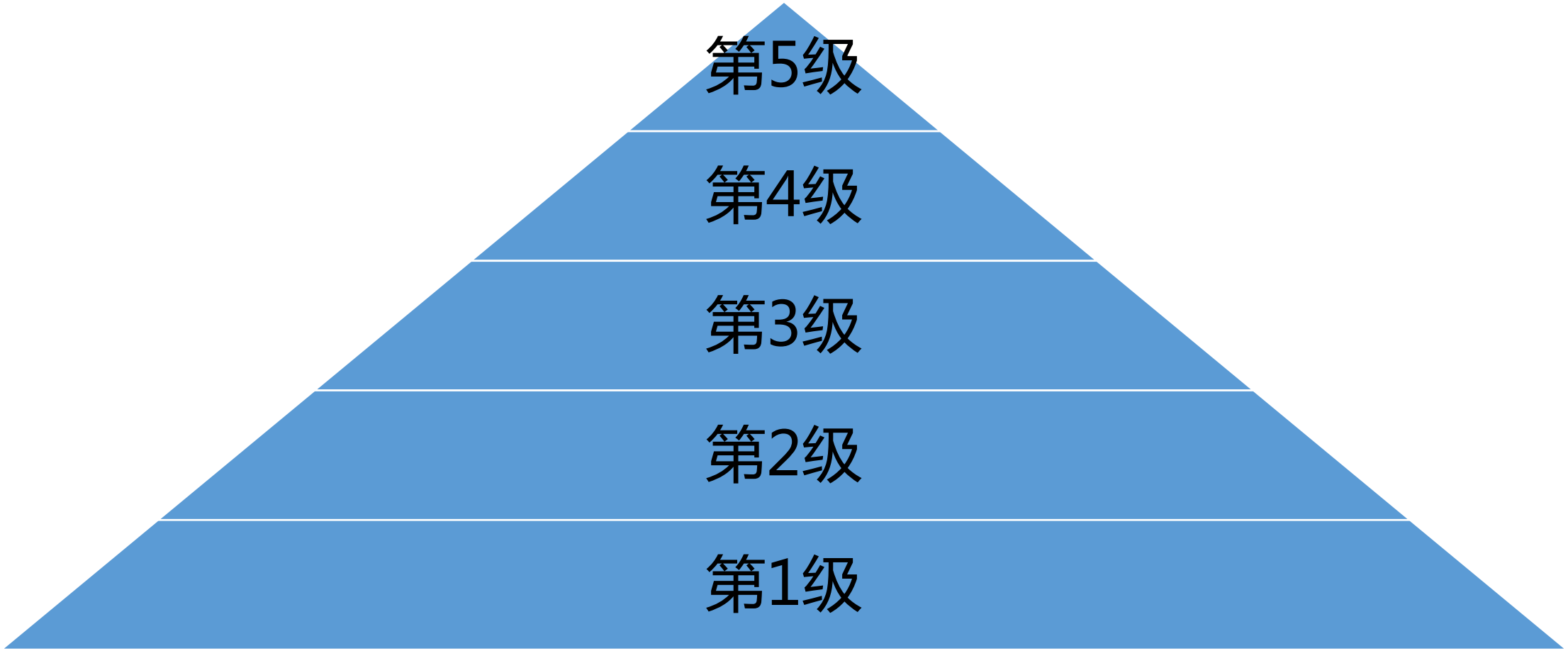
个人隐私、公众利益、国家安全

满足业务需要

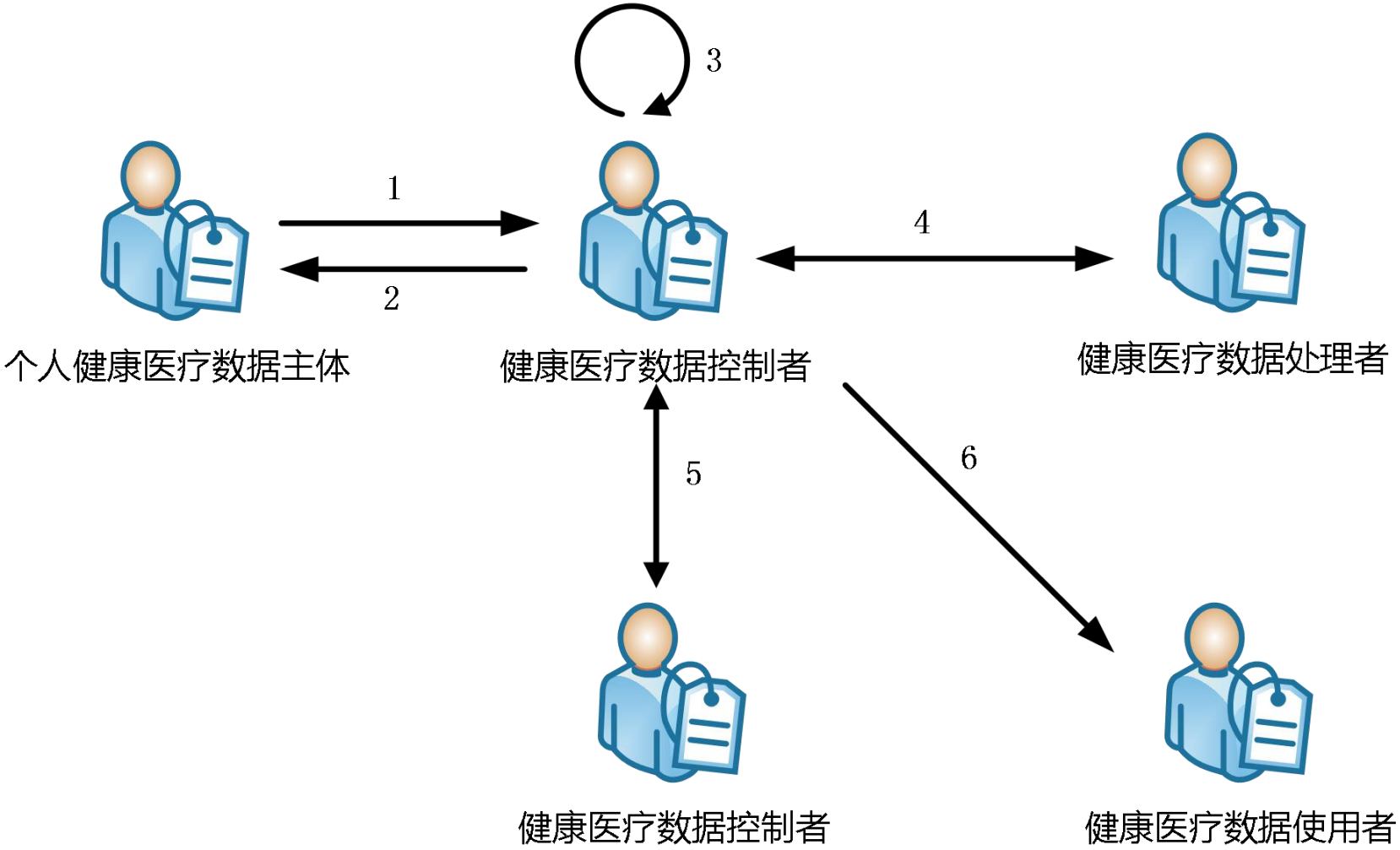
数据分类

个人属性数据	健康状况数据	医疗应用数据
医疗支付数据	卫生资源数据	公共卫生信息

非密、非重要数据分级



角色、数据流通使用场景分类



数据开放形式分类

网站公开

文件共享

API接入

在线查询

数据分析平台

安全指南

使用披露要求

- 主体-控制者间、控制者内部、控制者之间、控制者-处理者间、控制者-使用者间、…

安全管理指南

- 组织保障、PDCA管理体系、应急处置

安全技术指南

- 通用安全技术指南、去标识化指南

重点安全措施

安全措施要点

- 分级安全措施要点、场景安全措施要点、开放安全措施要点

典型场景数据安全

- 医生调阅、患者查询、二次利用、临床研究、健康传感、移动应用、商保对接、医疗器械

标准内容

典型场景数据安全

11.1 医生调阅数据安全
- 概述
- 涉及的相关方
- 涉及的数据
- 重点安全措施

11.2 患者查询数据安全
11.3 二次利用数据安全
11.4 临床研究数据安全
11.5 健康传感数据安全
11.6 移动应用数据安全
11.7 商保对接数据安全
11.8 医疗器械数据安全

安全指南

7 使用披露要求　8 安全措施要点　9 安全管理指南　10 安全技术指南

安全目标

5 安全目标
- 保密性、完整性、可用性
- 个人隐私、公众利益、国家安全
- 满足业务需求

分类体系

6 分类模型
- 6.1 数据类别
- 6.2 数据分级
- 6.3 角色分类
- 6.4 场景分类
- 6.5 开放分类

补充参考

附录A 个人健康医疗数据范围　附录B 卫生信息相关标准
附录C 数据使用管理办法示例　附录D 数据申请审批示例
附录E 数据处理使用协议模板　附录F 健康医疗数据安全检查表　附录G 数据元去标识化示例

参编单位32家

- 清华大学
- 北京清华长庚医院
- 中国医师协会智慧医疗专业委员会
- 中国网络安全审查技术与认证中心
- 中电数据服务有限公司
- 中国电子技术标准化研究院
- 上海市儿童医院
- 深圳市腾讯计算机系统有限公司
- 浪潮软件集团有限公司
- 东软集团股份有限公司
- 零氪科技（北京）有限公司
- 阿里巴巴（北京）软件服务有限公司
- 泰康保险集团股份有限公司
- 中国平安保险(集团)股份有限公司
- 北京邮电大学
- 四川大学华西医院
- 中国信息安全测评中心
- 北京天融信网络安全技术有限公司
- 上海市方达律师事务所
- 中国软件评测中心
- 中南大学
- 启明星辰信息技术集团股份有限公司
- 中国中医科学院
- 湖南科创信息技术股份有限公司
- 北京奇安信科技有限公司
- 陕西省信息化工程研究院
- 北京数字认证股份有限公司
- 中电长城网际系统应用有限公司
- 北京大学
- 浙江蚂蚁小微金融服务集团股份有限公司
- 北京协和医院
- 中国医院协会

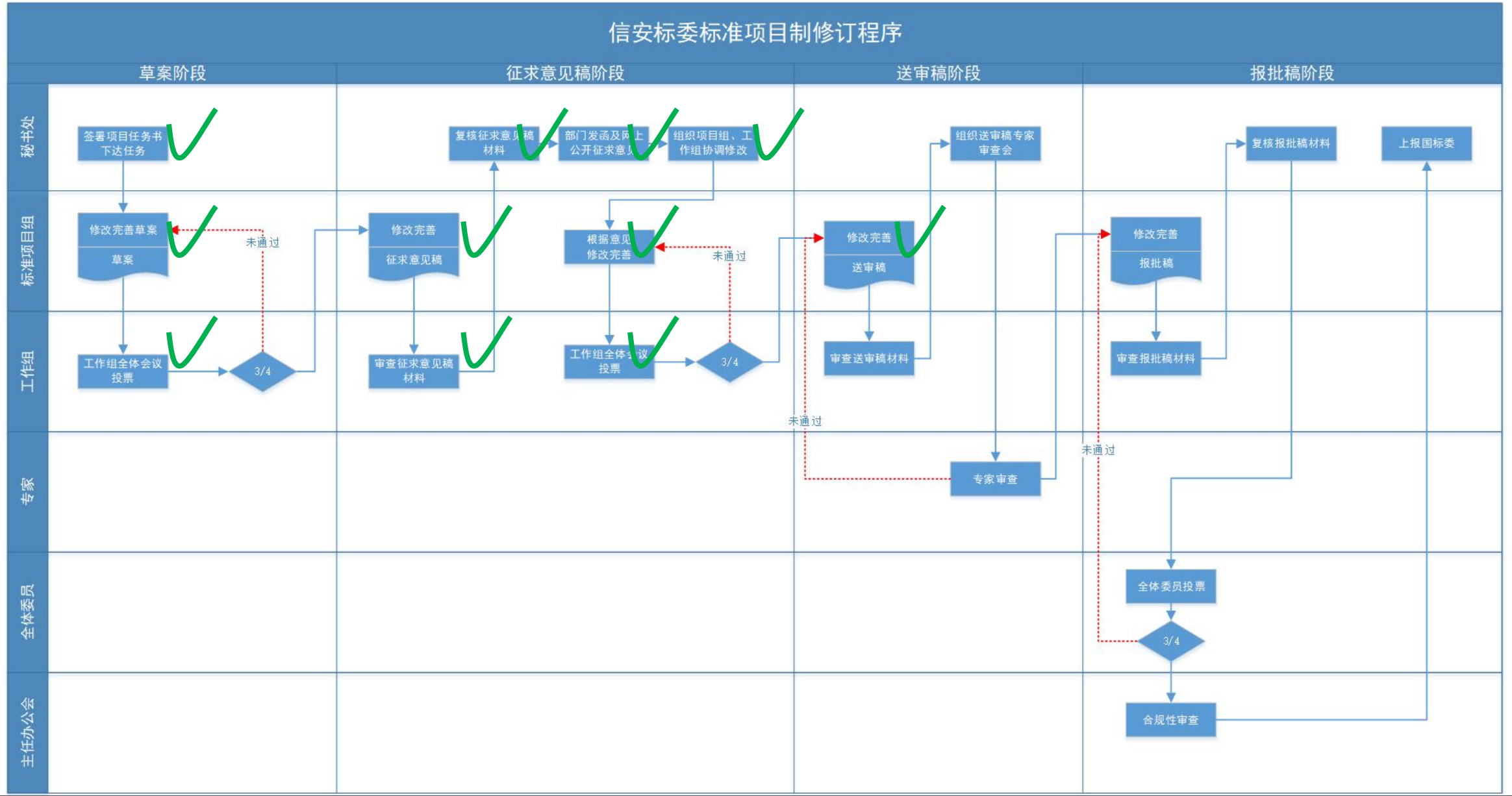
编制过程

- 2016年8月27日-28日清华研讨
- 2018年1月23日编制组会议
- 2018年2月6日编制组会议
- 2018年3月7日编制组会议
- 2018年3月15日领域专家会议
- 2018年3月20日编制组会议
- 2018年4月14日工作组全会
- 2018年9月14日编制组会议
- 2018年10月12日编制组会议
- 2018年10月17日编制组会议
- 2018年10月19日专家会议
- 2018年10月21日编制组会议
- 2018年10月24日工作组全会
- 2018年10月31日编制组会议
- 2018年11月7日编制组会议
- 2018年11月15日编制组会议
- 2018年11月21日领域专家会
- 2018年11月21日编制组会议
- 2018年11月28日编制组会议
- 2018年12月2日编制组会议

编制过程（续）

- 2018年12月07日上海平安研讨
- 2018年12月08日上海汉坤研讨
- 2018年12月26日编制组会议
- 2018年12月26日开始征求意见
- 2019年1月17日上海金杜研讨
- 2019年1月19日标准验证启动
- 2019年2月20日编制组会议
- 2019年3月20日编制组会议
- 2019年4月3日编制组会议
- 2019年4月22日工作组全会

标准状态

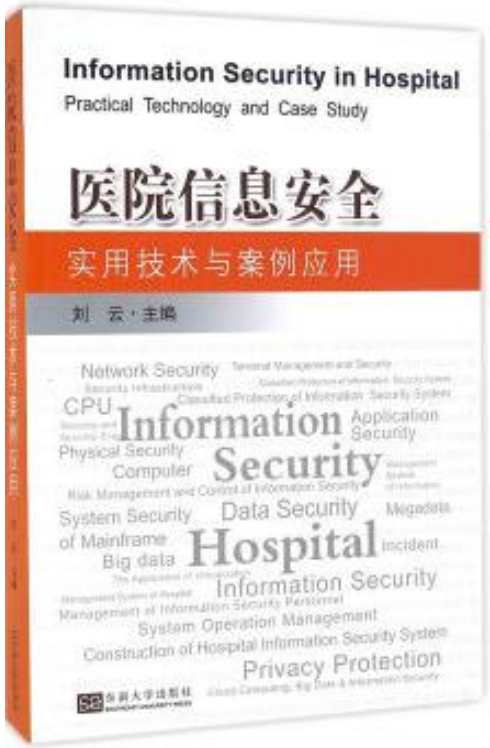

信安标委标准项目制修订程序
草案阶段
征求意见稿阶段
送审稿阶段
报批稿阶段
秘书处
标准项目组
工作组
专家
全体委员
主任办公会
签署项目任务书
下达任务
修改完善草案
草案
未通过
工作组全体会议
投票
3/4
修改完善
征求意见稿
审查征求意见稿
材料
复核征求意见稿
材料
部门发函及网上
公开征求意见
组织项目组、工
作组协调修改
根据意见
修改完善
未通过
工作组全体会议
投票
3/4
组织送审稿专家
审查会
修改完善
送审稿
审查送审稿材料
未通过
专家审查
复核报批稿材料
上报国标委
修改完善
报批稿
审查报批稿材料
未通过
全体委员投票
3/4
合规性审查

相关书目


医疗卫生行业
信息安全等级保护
YILIAO WEISHENG HANGYE
XINXI ANQUAN DENGJI BAOHU


数字卫生丛书
数字卫生标准化
数字卫生标准化


浙江省医疗卫生
信息安全管理案例集


Information Security in Hospital
Practical Technology and Case Study
医院信息安全
实用技术与案例应用
刘 云·主编
Network Security
CPU
Information
Application Security
Physical Security
Computer
Security
System Security
Data Security
of Mainframe
Big data
Hospital
Incident
Information Security
System Operation Management
Construction of Hospital Information Security System
Privacy Protection

- 2017年4月21日《福州市健康医疗大数据资源管理暂行办法》
- 2017年10月25日《福州市健康医疗大数据资源管理实施细则》
- 2018年10月15日《贵阳市健康医疗大数据应用发展条例》将于2019年1月1日起开始施行

硕 士 学 位 论 文

健康医疗可穿戴设备数据安全与隐私保护问题研究

所　　院：　医学信息研究所

姓　　名：　何晓琳

指导教师：　钱　庆　研究员

　　吴思竹　副研究员

学科专业：　情报学

研究方向：　医学信息学

完成日期：　二〇一七年五月

硕 士 学 位 论 文

在健康数据助推健康产业发展环境下

医疗数据安全开放应用框架研究

所　院　：　中国医学科学院阜外医院

姓　名　：　赵新蓉

指导教师：　赵鞬

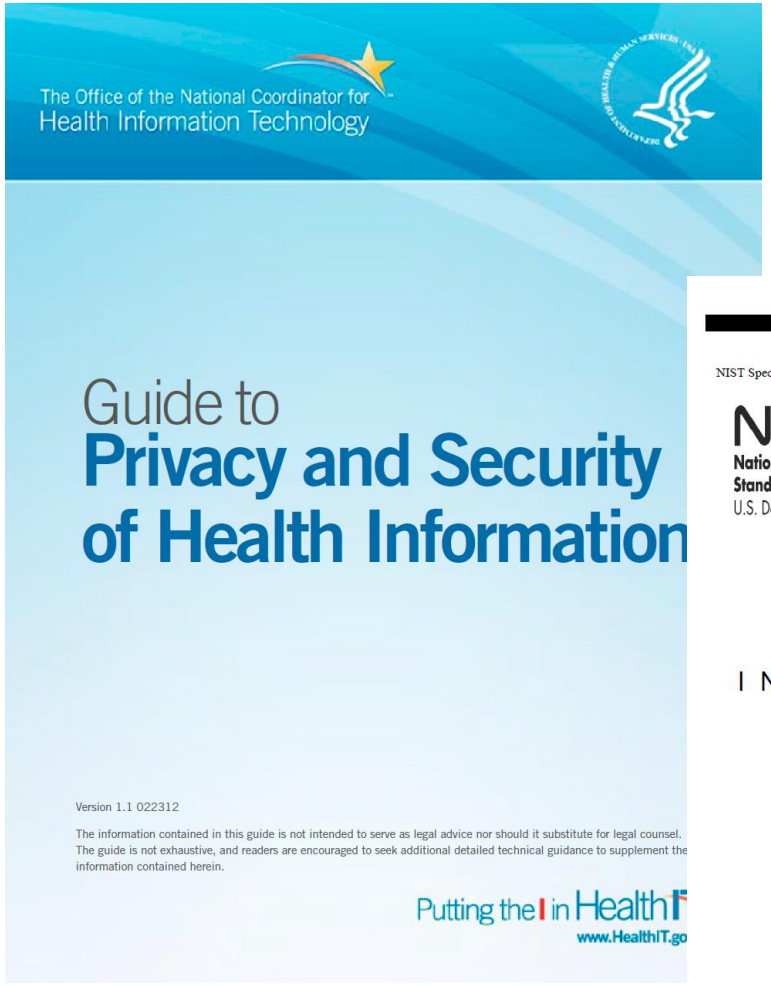
导师小组：　赵鞬　周洲　杨国胜

学科专业：　生物医学工程

研究方向：　医疗数据安全

完成日期：　2017 年 5 月

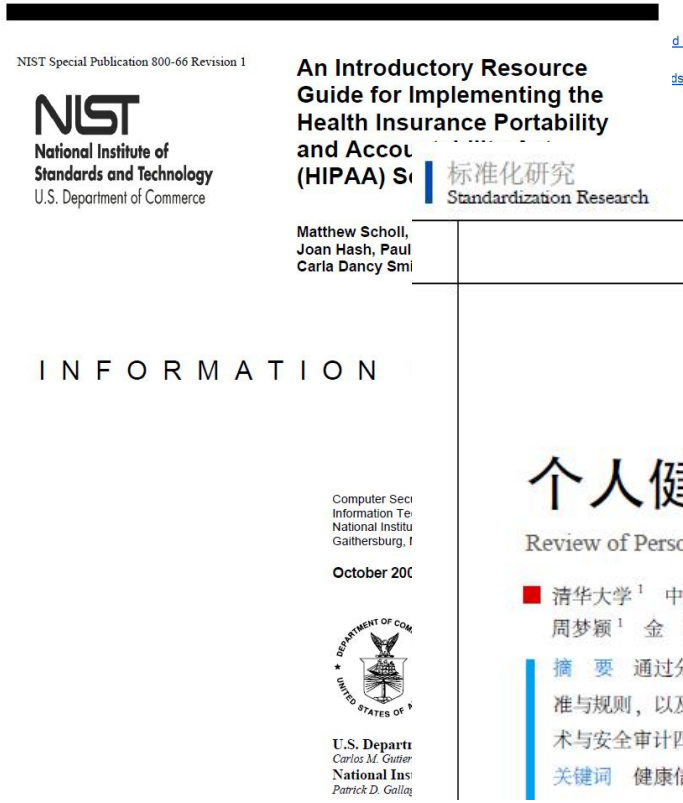
国外相关

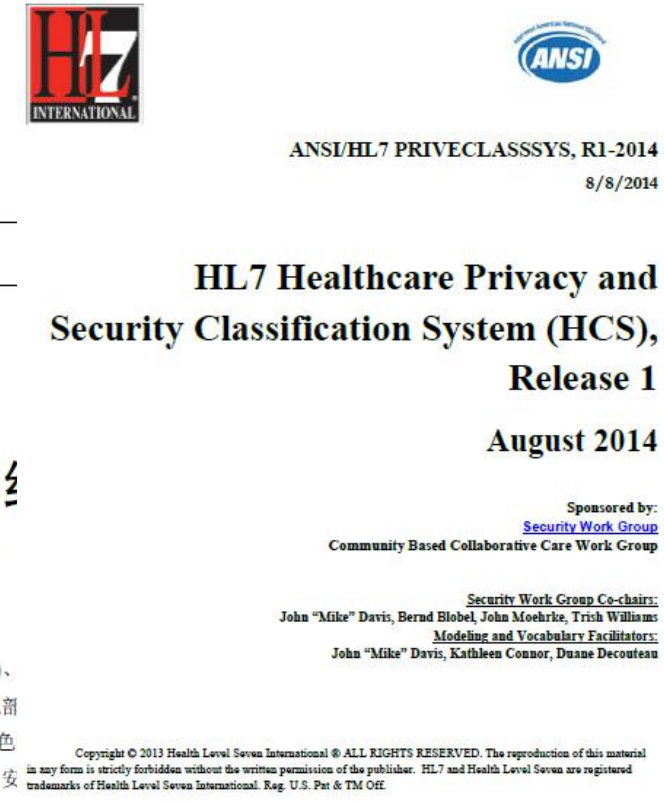

The Office of the National Coordinator for
Health Information Technology
Guide to
Privacy and Security
of Health Information
Version 1.1 022312
The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel.
The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the
information contained herein.
Putting the I in Health I
www.HealthIT.go


HHS.gov
U.S. Department of Health & Human Services
Health Information Privacy
I'm looking for...
HHS A-Z Index
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
Newsroom
HHS > HIPAA Home > For Professionals > Security > Security Rule Guidance Material
HIPAA for Professionals
Privacy
Security
Summary of the Security Rule
Text Resize A A A
Print
Share
Security Rule Guidance Material
In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).
Security Rule Educational Paper Series


INTERNATIONAL STANDARD
ISO 27799
Second edition
2016-07-01


Health informatics — Information security management in health using ISO/IEC 27002
Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002


NIST Special Publication 800-66 Revision 1
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
An Introductory Resource Guide for Implementing the Health Insurance Portability and Accou (HIPAA) S
Matthew Scholl,
Joan Hash, Paul
Carla Dancy Smi
INFORMATION
Computer Secu
Information Te
National Institu
Gaithersburg,
October 200
U.S. Departr
Carlos M. Gutier
National Ins
Patrick D. Gallag


HL7 INTERNATIONAL
ANSI
ANSI/HL7 PRIVECLASSSYS, R1-2014
8/8/2014
HL7 Healthcare Privacy and Security Classification System (HCS), Release 1
August 2014
Sponsored by:
Security Work Group
Community Based Collaborative Care Work Group
Security Work Group Co-chairs:
John "Mike" Davis, Bernd Blobel, John Moehrke, Trish Williams
Modeling and Vocabulary Facilitators:
John "Mike" Davis, Kathleen Connor, Duane Decouteau
Copyright © 2013 Health Level Seven International ® ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher. HL7 and Health Level Seven are registered trademarks of Health Level Seven International. Reg. U.S. Pat & TM Off.

标准化研究
Standardization Research
个人健康信息保护标准
Review of Personal Health Information Protection Standards
清华大学 [1] 中国电子技术标准化研究院 [2]
周梦颖 [1] 金 涛 [1] 何延哲 [2]
摘 要 通过分析国际标准化组织 (ISO)、欧盟标准化委员会 (CEN)、
准与规则，以及美国健康保险流通与责任法 (HIPAA) 的安全与隐私
术与安全审计四个维度上个人健康信息的要求，对制定符合我国特色
关键词 健康信息 保护 标准 大数据 安全管理 物理安全

意见处理（全部接受）

- 2018年10月2日工作组征求意见
  - IBM：2条
- 2018年10月18日九大医疗信息化微信群征求意见：CHIMA委员、OMAHA主群、HIMSS、北京卫生信息技术协会PHITA、蜜蜂会、健康医疗大数据应用、互联网医院专业群、互联网医疗协同创新群等
  - 8条主要意见
- 2018年10月19日WG1专家论证会
  - 9专家：40条
- 2018年10月24日工作组全会
  - 7条意见

征求意见处理

- 2018年12月26日开始公开征求意见，2019年2月11日截止
- 发送“征求意见稿”的单位数：向8个部门（工业和信息化部科技司、公安部十一局、国家保密局、国家密码管理局、国家认证认可监督管理委员会、中国信息安全测评中心、中央网信办网络安全协调局、卫健委法规司）发函并通过信安标委网站面向国内外进行了公开意见征集，征求意见范围具有广泛性和代表性。
- 收到“征求意见稿”后，回函并有建议或意见的单位数：3个部门，8个单位，5个个人。
- 收到意见总计88条，采纳49条，部分采纳14条，未采纳25条。

后续工作计划

- 2019.5：形成送审稿
- 宣贯，验证、完善

清华长庚医院数据安全管理体系

“标准”含义

- 标准是为在一定的范围内获得最佳秩序，对活动或其结果规定共同的重复使用的规则、导则或特性的文件。该文件经协商一致制定并经一个公认机构批准。
- 出发点：获得最佳秩序
- 限制条件：一定的范围
- 产生基础：协商一致
- 标准特征：共同使用和重复使用
- 权威性：公认机构批准
- 表现形式：规范性文件
- 内容：宜以科学、技术和经验的综合成果为基础，以促进最佳的共同效益为目的

标准支撑法律法规

标准偏向于技术细节，可随技术发展进行调整，而政策相对稳定

协商一致

- 使用披露要求
- 各相关方责任
- 数据分类分级和安全措施要点
- 场景分类和安全措施要点
- 开放分类和安全措施要点
- 典型场景重点安全措施

在确保健康医疗数据安全的前提下促进数据开发利用

谢谢！

敬请各位领导和专家批评指正！