ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39725—2020

信息安全技术
健康医疗数据安全指南

Information security technology—Guide for health data security

2020-12-14 发布　　2021-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:清华大学、北京清华长庚医院、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、山东国数爱健康大数据有限公司、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、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、奇安信科技集团股份有限公司、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、颐信科技有限公司、浙江蚂蚁小微金融服务集团股份有限公司、北京协和医院。

本标准主要起草人:金涛、刘海一、王建民、董家鸿、左晓栋、张剑、刘贤刚、屈劲、于广军、赵冉冉、袁耀文、傅兴良、杨浩、来子祺、苏凌云、叶晓俊、陶蓉、于惊涛、马诗诗、王枞、殷晋、付嵘、王龑、张毅、姚建伟、陈先来、谢安明、文天才、肖国荣、周亚超、郭颖、张勇、宋玲娓、闵京华、洪延青、程瑜琦、王昕、孟晓阳、罗妍。

引　言

健康医疗数据包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据。随着健康医疗数据应用、“互联网＋医疗健康”和智慧医疗的蓬勃发展，各种新业务、新应用不断出现，健康医疗数据在全生命周期各阶段均面临着越来越多的安全挑战，安全问题频发。由于健康医疗数据安全事关患者生命安全、个人信息安全、社会公共利益和国家安全，为了更好地保护健康医疗数据安全，规范和推动健康医疗数据的融合共享、开放应用，促进健康医疗事业发展，特制定健康医疗数据安全指南。

信息安全技术
健康医疗数据安全指南

1 范围

本标准给出了健康医疗数据控制者在保护健康医疗数据时可采取的安全措施。

本标准适用于指导健康医疗数据控制者对健康医疗数据进行安全保护，也可供健康医疗、网络安全相关主管部门以及第三方评估机构等组织开展健康医疗数据的安全监督管理与评估等工作时参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不标注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

GB/T 37964—2019 信息安全技术 个人信息去标识化指南

ISO 80001 整合医疗设备的网络风险管理的应用(Application of risk management for IT-networks incorporating medical devices)

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

个人健康医疗数据 personal health data

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电子数据。

注：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，参见附录A。

3.2

健康医疗数据 health data

个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关电子数据。

示例：经过对群体健康医疗数据处理后得到的群体总体分析结果、趋势预测、疾病防治统计数据等。

3.3

健康医疗专业人员 health service professional

经政府或行业组织授权有资格履行特定健康医疗工作职责的人员。