

奥邦检验认证集团有限公司企业标准

CTS_ABG 69725-2024

健康医疗数据安全管理体系 要求

Information technology - Security techniques -
Healthcare data security management systems - Requirements

2024-06-30 发布

2024-07-01 实施

奥邦检验认证集团有限公司 发布

目录

健康医疗数据安全管理体系 要求	1
1 范围	4
2 规范性引用文件	4
3 术语和定义	4
4 组织环境	4
5 领导作用	5
6 策划	6
7 支持	8
8 运行	10
9 绩效评价	11
10 改进	12
附录 A（资料性附录）：健康医疗数据分级安全措施	13
附录 B（资料性附录）：典型场景安全管理规范	13
附录 C（资料性附录）：数据安全文件模板	15

前言

本文件按照 GB/T1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件规定了健康医疗数据安全管理体系认证的要求，旨在指导医疗健康机构、科研单位、保险机构等建立健康医疗数据安全管理体系及相关认证活动，保障健康医疗数据的保密性、完整性和可用性。

本文件由奥邦检验认证集团有限公司技术部提出并起草。

本文件主要起草人：袁海、邵优良。

本文件奥邦检验认证集团有限公司 2024 年 06 月 30 日批准发布。

本文件自 2024 年 07 月 01 日发布之日起实施。

本文件由奥邦检验认证集团有限公司解释。

健康医疗数据安全管理体系 要求

1 范围

本文件规定了在组织范围内建立、实施、维护和持续改进健康医疗数据安全管理体系的要求。本文件包含针对健康医疗数据特性定制的风险评估、分级防护、场景化安全管控等专项要求。

本文件适用于所有涉及健康医疗数据处理的组织，包括但不限于医疗机构、公共卫生机构、医疗科研单位、健康管理公司、商业保险机构等，无论其规模和性质如何。

2 规范性引用文件

以下文件在正文中的引用方式使其部分或全部内容构成本文件的要求。对于注明日期的引用文件，仅引用的版本适用。对于未注明日期的引用文件，引用文件的最新版本（包括任何修订）适用。

GB/T 39725-2020 《信息安全技术 健康医疗数据安全指南》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

GB/T 37964-2019 《信息安全技术 个人信息去标识化指南》

ISO/IEC 27001:2022 《信息技术 安全技术 信息安全管理体系 要求》

ISO/IEC 27799:2016 《健康信息学 利用 ISO/IEC 27002 的健康信息安全管理》

3 术语和定义

在本文件中，GB/T 39725-2020、GB/T 35273-2020 及 ISO/IEC 27001:2022 中给出的术语和定义适用。

3.1 健康医疗数据 healthcare 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。

3.2 健康医疗数据控制者 healthcare data controller

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。

3.3 去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联到特定自然人的过程。

3.4 受限制数据集 limited data set

经过部分去标识化处理，但仍可识别相应个人并因此需要保护的个人信息数据集。

4 组织环境

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1) 通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2) 也可通过客服电话咨询 **025-85307007**。