|  |
| --- |
| 43 |

湖南省地方标准

DB 43/T XXXX—XXXX

数字化全病程健康管理：技术规范

Digital whole course health management：technical specification

XXXX - XX - XX发布

XXXX - XX - XX实施

湖南省市场监督管理局  发布

|  |  |
| --- | --- |
| ICS | 35.100.01 |
| CCS | L 79 |

目次

[前言 II](#_Toc133325596)

[1 范围 1](#_Toc133325597)

[2 规范性引用文件 1](#_Toc133325598)

[3 术语和定义 1](#_Toc133325599)

[4 设计原则 1](#_Toc133325600)

[5 总体要求 2](#_Toc133325601)

[6 技术要求 3](#_Toc133325602)

[7 安全要求 4](#_Toc133325603)

[参考文献 6](#_Toc133325604)

1. 前言

本文件按照GB/T 1.1—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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由湖南省工业和信息化厅提出。

本文件由湖南省信息技术标准化技术委员会归口。

本文件起草单位： XXX、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX。

数字化全病程健康管理：技术规范

* 1. 范围

本文件规定了数字化全病程健康管理系统的设计原则、总体要求、技术要求和安全要求。

本文件适用于数字化全病程健康管理系统的开发、设计和应用。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25000.51 系统与软件工程 系统与软件质量要求和评价）（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

WS 363（所有部分） 卫生信息数据元目录

WS 364（所有部分） 卫生信息数据元值域代码

* 1. 术语和定义

本文件没有需要界定的术语和定义。

* 1. 设计原则
     1. 规范性

数字化全病程健康管理系统应按照信息系统等级保护三级（或以上）的要求进行安全建设，安全设计应遵循已颁布的相关国家标准。

* + 1. 先进性和适用性

应采用先进的设计思想和方法，尽量采用国内外先进的技术。所采用的先进技术应符合实际情况，应合理设置平台功能、恰当进行数字化全病程健康管理系统配置和设备选型，保障其具有较高的性价比，满足业务管理的需要。

* + 1. 可扩展性

应考虑通用性、灵活性，以便利用现有资源及应用升级。

* + 1. 开放性和兼容性

对子系统的升级、扩充、更新以及功能变化应有较强的适应能力。即当这些因素发生变化时，子系

统可以不做修改或少量修改就能在新环境下运行。

* + 1. 可靠性

应确保数字化全病程健康管理系统的正常运行和数据传输的正确性，防止由内在因素和硬件环境

造成的错误和灾难性故障，确保互联网医院开发平台可靠性。在保证关键技术实现的前提下，尽可能

采用成熟产品和技术，保证数字化全病程健康管理系统的可用性、工程实施的简便快捷。

* + 1. 系统性

应综合考虑数字化全病程健康管理系统的整体性、相关性，目的性、实用性和适应性。另外，与业务系统的结合相对简单且独立。

* + 1. 技术和管理相结合

应遵循技术和管理相结合的原则进行设计和实施，数字化全病程健康管理系统采用的各种技术应与运行管理机制、人员思想教育与技术培训、规章制度建设相结合。从社会工程的角度综合考虑，最大限度发挥人、物、技相结合的作用。

* 1. 总体要求
     1. 数字化全病程健康管理系统架构包括：

1. 架构应采用互联网软件开发技术，兼容PC端、移动端、嵌入式终端等多终端入口，前后端分离模式，多语言全应用程序编程接口化开发；
2. 应具有消息路由功能，可具有业务流程管理（BPM）、可支持医院自动化业务流程编排和人工参与的工作流；
3. 架构应支持基于事件驱动（EDA）的消息传输机制，支持服务的发布与订阅。
   * 1. 数字化全病程健康管理系统管理功能包括：
   1. 应提供管理工具，能够管理所有业务系统集成节点，监控整个医院平台运行状态；
   2. 应支持对信息库访问内容的用户授权及认证，支持数据防篡改及隐私数据保密，支持业务流程的追踪与审计，支持日志的记录与查看，支持消息可靠性传递及消息追踪等；
   3. 应提供二次开发环境，提供基础公共业务组件的封装，并提供相应的维护管理工具。
      1. 数字化全病程健康管理系统交互信息应支持WS 363（所有部分）、WS 364（所有部分）等国家颁布的相关卫生数据标准，参考国际卫生行业相关数据标准。
      2. 数字化全病程健康管理系统集成能力应最大限度地复用现有应用系统的业务功能，在选择SOA技术标准规范时，平台应考虑现有业务功能封装对技术标准规范的支持能力，基本要求包括：
4. 以微服务技术作为SOA服务开发技术的首选技术；
5. 基于微服务的安全管理应遵循微服务服务规范中WS-Security规范，其他形式的服务也应提供安全保障；
6. 可支持主流的卫生信息交换国际标准和规范。
   * 1. 数字化全病程健康管理系统稳定性应满足年平均无故障时间应达到200 d以上。
   1. 技术要求
      1. 软硬件

应拥有至少2套开展业务的音视频通讯系统（含必要的软件系统和硬件设备），并满足：

1. 前置条件：支持注册并完成实名认证，可实现音视频套餐，创建应用并获取SDKAPPID和秘钥；
2. 集成音视频SDK；
3. 音视频存储。
   * 1. 最小接入系统数

接入系统指接入数字化全病程健康管理系统的独立应用系统，具体要求包括：

1. 对二级医院互联网医院开发平台，允许最小接入系统数大于或等于3个；
2. 对三级医院互联网医院开发平台，允许最小接入系统数大于或等于6个。
   * 1. 最小并发用户数

最小并发用户数要求包括：

1. 对二级医院基于互联网医院开发平台的应用系统，总的允许最小并发用户数大于200；
2. 对三级医院基于互联网医院拜发平台的应用系统，总的允许最小并发用户数大于600。
   * 1. 基础服务平均响应时间

基础服务平均响应时间要求包括：

1. 个人注册服务调用

单个患者注册平均响应时间小于1 s。

1. 个人基本信息查询

总记录50万以上，按患者唯一标识查询单个患者查询平均响应时间小于2 s；总记录100万以上，按患者唯一标识查询单个患者查询平均响应时间小于3 s。

1. 基于人口统计学信息的患者信息匹配（基于索引）

总记录50万以上，返回患者唯一标识数据，返回记录数小于10条时，平均响应时间小于10 s；总记录100万以上，返回记录数小10条时，平均响应时间小于15 s。

* + 1. 网络接入

应具备高速率高可靠的网络接入，业务使用的网络带宽不低于10 Mbps，且至少由两家宽带网络供应商提供服务，有条件的互联网医院接入互联网专线、虚拟专用网（VPN），保障医疗相关数据传输服务质量。

* + 1. CA认证

可实现在数字化全病程健康管理系统安全通信提供电子认证，应包括关键数据、身份认证、处方签章。

* + 1. 医保支付

可开发互联网医保支付通道，支持第三方支付接入。

* + 1. 云计算
       1. 应确保与云服务商签订保密协议，明确云服务商的责任与权限，并规定服务合约到期时，完整提供互联网医院客户数据，并承诺相关数据在云计算平台上清除。
       2. 应在数字化全病程健康管理系统的虚拟化网络边界部署访问控制机制，并设置访问控制规则。当远程管理云计算平台中设备时，管理终端与云计算平台之间应建立双向身份验证机制。
       3. 应确保互联网医院相关数据存储于公有云时，对医疗数据进行加密处理。
       4. 应确保互联网医院所在云计算平台支持部署密钥管理解决方案，保证互联网医院运营主体自行实现数据的加解密过程。
  1. 安全要求
     1. 数字化全病程健康管理系统的整体安全应符合GB/T 22239和GB/T 28452的规定，以安全技术、安全管理为要素进行并符合：

1. 应从网络安全（基础网络安全和边界安全）、主机安全（终端系统安全、服务端系统安全）、应用安全、数据安全等层面实现安全技术类要求；
2. 应从安全管理制度、安全管理机构、人员安全管理、平台建设管理和平台运维管理等层面实现安全管理类要求。
   * 1. 应能检测到数字化全病程健康管理系统管理数据、身份鉴别信息、电子病历、电子支付等重要业务数据在传输和存储过程中完整性受到破坏，并能够采取必要的恢复措施。
     2. 应对身份鉴别信息、电子病历、电子支付、电子处方等重要业务数据在传输和存储过程中对敏感信息字段进行加密，数字化全病程健康管理系统应支持基于标准的加密机制。宜采用PKI密码技术或采用具有相当安全性的其他安全机制实现。
     3. 应建立数据备份措施，建立备份管理制度，制定数据备份策略，对重要信息进行备份以及对依据备份记录进行数据恢复，包括：
3. 定期采取手工备份方式对重要文件及保存在数据库中的数据进行备份；
4. 定期采取自动备份系统进行应用数据备份，管理员应复核自动备份结果；
5. 关键存储部件宜采用冗余磁盘阵列技术并支持失效部件的在线更换；
6. 对重要设备应进行冗余配置，以实现双机热备或冷备；
7. 数据库服务器宜采用双机冗余热备方式，进行定期在线维护，以缩短恢复所需时间；
8. 用户可以通过备份记录进行数据恢复；
9. 在条件具备的情况下，应在异地建立和维护重要数据的备份存储系统，利用地理上的分离保障数字化全病程健康管理系统和数据对灾难性事件的抵御能力；
10. 故障恢复前应制定合理的恢复工作计划以及故障恢复方案，数据恢复完成后应检测数据的完整性。
    * 1. 客户端应用软件，如互联网医院APP、微信公众号或小程序等，应符合安全代码编写规范，使用代码安全防护手段（例如代码加壳、代码混淆、检测调试器等）对客户端应用软件进行安全保护，使之具备一定的抗攻击能力，防止重要信息泄露和非法获取使用。具体要求如下：
11. 程序安全
    1. 应在客户端应用软件安装、更新时对自身的完整性和合法性进行验证；
    2. 应具备身份认证控制和认证失败策略；
    3. 应采用两种或两种以上的要素对用户身份进行认证；
    4. 应具备会话超时后要求重新鉴权的机制；
    5. 应配合服务端提供密码复杂度校验功能；
    6. 应具备抵御动态调试、反编译、篡改、劫持、截屏、键盘窃听、重放等抗攻击能力；
    7. 应保证安装文件中不包含任何冗余文件和冗余说明；
    8. 应保证安装文件中不包含明文证书、密钥、网络配置等信息；
    9. 应避免使用存在已知漏洞的第三方组件；
    10. 应具备客户端应用软件运行环境检测能力。
12. 通信安全
    1. 应在客户端应用软件与服务器之间建立安全的信息传输通道，协议版本应及时更新至安全稳定版本；
    2. 客户端应用软件与服务器应进行双向认证。
13. 数据安全
    1. 应保证登录密码、支付密码及其他输入的敏感信息，不以明文显示；
    2. 应确保敏感数据在通过公共网络传输时的完整性和保密性；
    3. 应采用自定义权限保护组件访问；
    4. 应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问；
    5. 应保证在内存、临时文件、运行日志中不应以明文形式存储敏感数据；
    6. 应保证客户端应用软件进程被结束时、卸载后，不应残留敏感数据；
    7. 应支持页面返回、进入后台后，自动清除已输入的敏感信息；
    8. 应确保通过人机接或通信接自输入的数据格式或长度等信息符合系统设定要求。
       1. 客户端应用软件的运营机构，应接照《中华人民共和国网络安全法》及GB/T 25000.51的要求，加强客户端应用软件自身的安全开发工作，在客户端应用软件的版本更新过程中，始终遵循安全标准的要求，具体如下：
14. 应加强客户端应用软件的安全保障体系建设，建立客户端应用软件的事前检测、事中监测、事后追溯的全生命周期管理；
15. 针对APP、微信公众号、小程序、其它服务号等应进行主动、持续、动态的风险业务识别、侦测和分析，达到风险识别、预警、处置的风控闭环控制，保证应用在移动客户端运行的安全性和合规性，全面提升移动互联网业务风险防控水平；
16. 可对互联网医院所运行的移动应用做资产归集管理，明确资产所有人、使用人、开发人，移动应用资产所包含的软件版本、内嵌SDK和相关软件资产信息；
17. 应对在线运行的客户端应用软件进行应用合法性判别，防止盗版应用导致个人信息泄露等风险；
18. 应对在线运行的客户端应用软件进行不间断的安全漏洞分析、恶意程序分析等，持续对客户端应用软件在版本更新及运行过程中进行立体安全防护。

参考文献

[1] 《中华人民共和国网络安全法》 中华人民共和国主席令（第五十三号）

