

团 体 标 准

T/NDAS 7—2020

健康信息管理平台基本要求

General requirements for health information management platform

（征求意见稿）

（本稿完成日期：）

2020 – XX – XX 发布

2020 – XX – XX 实施

宁德市标准化协会 发 布

目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 建设原则.....	1
4.1 完整和实用性.....	1
4.2 松耦合和易扩展性.....	1
4.3 易操作和易维护性.....	2
4.4 安全和可靠性.....	2
5 功能框架.....	2
6 基本功能要求.....	2
6.1 用户注册、登录.....	2
6.2 健康信息采集.....	3
6.3 健康体检管理.....	3
6.4 健康指导.....	4
6.5 系统维护.....	4
7 接口要求.....	4
8 安全要求.....	5
8.1 身份鉴别.....	5
8.2 访问控制.....	5
8.3 安全审计.....	5
8.4 抗抵赖.....	5
8.5 软件容错.....	5
8.6 数据安全.....	5

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专利的责任。

本文件由上海冉煜健康管理咨询有限公司提出。

本文件由宁德市标准化协会归口。

本文件起草单位：上海冉煜健康管理咨询有限公司、上海安释信息咨询有限公司、上海知律信息科技有限公司、上海康茹节能环保科技有限公司、上海赢肯自动化科技有限公司、上海朴薪智能科技有限公司、上海舜玉机电科技有限公司。

本文件主要起草人：刘李烨、秦玉龙、胡智红、张宇、陈子展、张娟、姚王平、王青青。

健康信息管理平台基本要求

1 范围

本文件规定了健康信息管理平台的建设原则、功能框架、基本功能要求、接口要求及安全要求。本文件适用于健康信息管理平台的设计、开发、实施和维护。

2 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。

WS 365—2011 城乡居民健康档案基本数据集

3 术语和定义

下列术语和定义适用于本文件。

3.1

健康服务对象 health care consumer

通过健康信息平台获取和接受健康管理服务的个体。

注：本文件中的健康服务对象为个人。

3.2

个人健康信息 personal health information

关于健康服务对象健康状况的信息，该信息以计算机可处理的形式存在，且能够安全存储和传输。

3.3

健康指导 health guidance

对个体或群体的健康进行全面监测、分析、评估，提供健康咨询和指导以及对健康危险因素进行干预的全过程。

4 建设原则

4.1 完整和实用性

健康信息平台功能应覆盖个人健康信息采集、健康体检管理、健康风险评估与监测、健康指导等过程，并针对过程中每项业务的详细功能进行优化。

4.2 松耦合和易扩展性

健康信息平台应采用松耦合、模块化的平台设计思路，为各外接功能模块提供灵活、安全、稳定的接口服务，保证平台的模块较易扩展，易于平台升级。本文件规定的是健康信息平台的基本功能，在平台建设过程中可根据不同用户的需求和新出现的业务类型进行功能模块的扩展。

4.3 易操作和易维护性

健康信息管理平台建设应充分考虑行业特点及用户的操作习惯,同时提供针对平台的各个功能模块以及接口的可监控机制,便于及时发现运行错误并排除故障。

4.4 安全和可靠性

健康信息管理平台的建设和管理应完善的逻辑严密的安全管理机制,加强对敏感数据的管控,在保障可用性的基础上为业务数据提供完整性和保密性保护。在平台运行方面应保证系统无单一故障点,确保运行稳定。

5 功能框架

健康信息管理平台功能框架见图1。

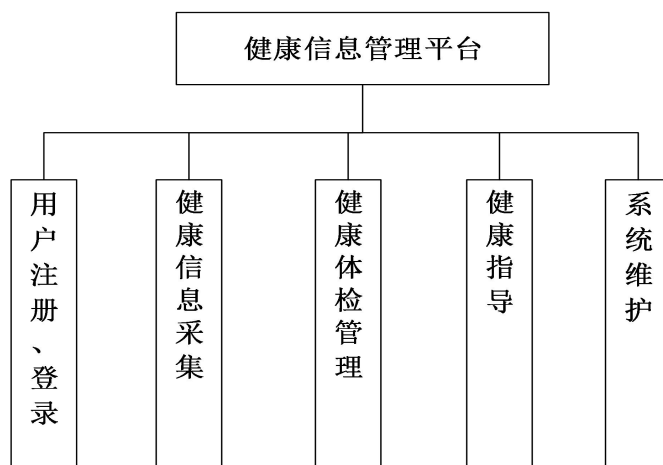


图1 平台功能框架

其中:

- 用户注册、登录的功能应包括用户注册和用户登录等;
- 健康信息采集的功能应包括个人基本信息采集、健康体检信息采集等;
- 健康体检管理的功能应包括体检机构管理、体检套餐和项目管理、体检服务管理等;
- 健康指导的功能应包括健康风险评估、健康干预等;
- 系统维护的功能应包括用户管理、权限管理、日志管理等。

6 基本功能要求

6.1 用户注册、登录

用户注册、登录功能要求如下:

- a) 应区分个人注册、医疗卫生人员和医疗机构注册;
- b) 应支持移动终端或邮箱等方式对注册信息进行验证;
- c) 应支持已注册用户以手机或邮箱加密码、验证码的方式登录,登录失败时应给予提示信息,并限制登录失败次数;

- d) 应支持用户密码找回;
- e) 应支持对密码加密存储, 防止密码外泄;
- f) 应支持所有注册用户的信息展现;
- g) 应支持对平台运营方进行单独管理, 包括用户信息的增加、修改、删除、设置角色权限、修改密码等;
- h) 应支持对医疗机构注册信息进行审核。

6.2 健康信息采集

6.2.1 个人基本信息

平台应支持对个人基本信息的采集。

个人基本信息的采集范围及数据类型、格式等, 应符合WS 365—2011中第5.2.1条的规定。

6.2.2 健康体检信息

平台应支持对健康体检信息的采集。

健康体检信息的采集范围及数据类型、格式等, 应符合WS 365—2011中第5.2.2条的规定。

6.2.3 重点人群健康信息

平台宜支持对以下重点人群的健康信息的采集:

- 老年人;
- 高血压患者;
- 糖尿病患者。

重点人群健康信息的采集范围及数据类型、格式等, 可参考WS 365—2011的有关规定。

6.3 健康体检管理

6.3.1 体检机构管理

体检机构管理功能要求包括:

- a) 体检机构准入: 对体检机构进行管理与维护, 对体检机构信息进行审核和确认;
- b) 服务类型管理: 对体检机构可接待的体检人员类型进行维护;
- c) 体检机构信息维护: 主要是对体检机构相关信息进行记录。主要包括医疗机构的基本信息、专业信息、专家信息、各个科室联系方式、体检办理负责人等基本信息的记录。

6.3.2 体检套餐和体检项目管理

体检套餐和体检项目管理功能要求包括:

- a) 体检项目维护: 支持对体检项目进行管理和维护;
- b) 体检套餐维护: 支持针对年龄、体质、疾病类型、健康要求等特点对体检项目进行组合制定体检套餐, 对体检套餐进行管理和维护;
- c) 个性化套餐设计: 支持根据用户的年龄、性别、家族多发病史、既往患病史、上次体检危险因素等情况进行个性化套餐设计。

6.3.3 体检服务管理

体检服务管理功能要求包括:

- a) 体检机构选择: 体检对象可自主选择体检机构进行体检;

- b) 体检项目选择：体检对象可自主选择体检项目、体检套餐或个性化套餐；
- c) 个人体检预约：体检对象可自主选择体检时间，通过平台进行预约，应支持对预约信息的查询及修改；
- d) 体检结果查询：体检对象可实时查询到体检报告和历次体检报告数据，可针对体检项目进行趋势分析，形成个人健康状况分析情况和注意事项提醒等。

6.4 健康指导

6.4.1 健康风险评估

健康风险评估功能要求包括：

- a) 健康状况评价：结合用户全身各部位信息记录的结果，对身体健康危险程度进行客观评定，对体质状况是否健康做出科学分析和提醒，并对整体健康水平进行评价
- b) 重要问题指导：针对用户的主要健康问题提出进行就诊或者检查方面的建议。

6.4.2 健康干预

健康干预功能要求包括：

- a) 制定健康干预计划：应能支持根据用户个人特点制定个性化健康干预计划，并涵盖营养干预、运动干预、不良生活习惯干预、心里干预、养生指导、疾病管理及环境干预等内容；
- b) 健康提醒：应能支持对用户的健康干预计划进行提醒；
- c) 效果评价：应能支持用户对干预周期前后效果进行对比。

6.5 系统维护

6.5.1 用户管理

应对使用健康信息管理平台的用户进行统一管理，其功能应包括但不限于：

- a) 提供对体检机构及健康服务对象的维护和管理；
- b) 支持对体检机构、体检机构工作人员相关信息的创建、修改、删除、查询。

6.5.2 权限管理

为实现用户使用平台功能的访问控制，保证有效用户正常使用的同时，防止非法用户和无权限用户对平台功能的使用及用户数据的访问，其功能应包括但不限于：

- a) 支持对用户的权限进行新增、修改、删除和查询等操作；
- b) 支持设置不同用户的访问和操作权限。

6.5.3 日志管理

为保证用户的行为防篡改、防抵赖，系统应支持对用户平台中的操作行为和操作的数据进行记录，其功能应包括但不限于：

- a) 支持对系统运行情况进行监控，并对时间、用户、角色、权限、行为等数据进行记录；
- b) 日志记录应为只读，不允许进行修改或删除；
- c) 可导出指定时间段的日志。

7 接口要求

接口要求包括：

- a) 健康信息管理平台应提供标准 API 接口，支持二次开发以及支持与第三方应用对接；
- b) 健康信息管理平台应支持与体检机构信息系统的对接，以便为健康服务对象提供各类个性化的健康信息管理服务；
- c) 健康信息管理平台宜支持与医疗终端和信息终端的对接，以便采集个人的生理指标信息和行为信息，获得健康教育信息、健康干预意见等。

8 安全要求

8.1 身份鉴别

身份鉴别的要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
- c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

8.2 访问控制

访问控制的要求包括：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

8.3 安全审计

安全审计的要求包括：

- a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
- b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

8.4 抗抵赖

抗抵赖的要求包括：

- a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

8.5 软件容错

软件容错的要求包括：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

8.6 数据安全

数据安全的要求包括：

- a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
 - b) 应对个人隐私数据、敏感数据进行加密存储；
 - c) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。
-