ICS：35.240.80
CCS：I6532

团　　体　　标　　准

T/GDIOT 009—2024

区域性医疗物联网平台技术规范

Regional Medical Internet of Things Platform Technical Specifications

2024-11-18发布　　2024-11-18实施

广东省物联网协会　发布

目 录

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。

本文件由广东省物联网协会提出并归口。

本文件起草单位：深圳市卫生健康发展研究和数据管理中心、广东省物联网协会、深圳市福田区妇幼保健院、中山大学附属第七医院（深圳）、深圳大学附属华南医院、深圳市中医院、深圳市人民医院、深圳市妇幼保健院、深圳市眼科医院、南方医科大学、广州医科大学附属第五医院、深圳市前海蛇口自贸区医院、深圳平乐骨伤科医院、深圳市龙岗区第四人民医院。

本文件主要起草人：和晓峰、吴旭生、曾明、段永恒、谭可欣、陈芮、张冬云、刘珺、庄锦湖、刘菲、郑子龙、欧阳杰、柳臻、钟晓茹、唐雄伟、邬俏璇、丘奂阳、黄莹、张毅俊、杨凯、郑霖、戴少锋、李斌、廖辰、吴俊、关晓印、乔怡茹、黎妍、赵成闻。

区域性医疗物联网平台技术规范

1 范围

本文件适用于建设区域性医疗物联网管理平台。本文件旨在推动深圳市优质医疗资源的扩容和区域均衡布局，提升医疗服务能力，促进医学科学发展。

本文件规定了深圳市区域性医疗物联网平台的技术规范要求。

2 规范性引用文件

GB/T 40684—2021 物联网 信息共享和交换平台通用要求

GB/T 39725—2020 信息安全技术 健康医疗数据安全指南

GB/T 25069 信息安全技术 术语

GB/T22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T35273 信息安全技术 个人信息安全规范

GB/T 34068—2017 物联网总体技术 智能传感器接口规范

GB/T 30269.807—2018 信息技术 传感器网络 第807部分：测试：网络传输安全

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

3 术语和定义

下列术语和定义适用于本文件

3.1 区域性医疗 Regional Medicine

是指在一定区域内，通过优化医疗资源配置，提升医疗服务能力，实现医疗服务均等化和便捷化的一种医疗服务模式。

3.2 医疗物联网 IoMT, Internet of Medical Things

是通信网络延伸到医疗场景中，通过感知和通信技术，将各类传感器、执行器、基础设施、医疗设备、各类智能化装备与医院信息系统联接在一起，支持医疗服务、医院运营过程中的数据采集、传输、处理、存储和分析应用，从而实现医疗场景中人与物通信、物与物通

信的网络。

3.3 电子病历 EMR, Electronic Medical Record

是指用于电子设备保存、管理、传输和重现的数字化病人医疗记录，它取代了传统的手写纸张病历。电子病历不仅包括病历信息，还涉及病人信息的采集、存储、传输、处理和利用的所有过程信息。

3.4 医疗设备 Medical equipment

医疗设备是指单独或组合使用于人体的仪器、设备、器具、材料或其他物品，包括所需的软件，其主要通过物理方法获得效用，而非药理学、免疫学或代谢方式获得，或者这些方式只起辅助作用。医疗设备的使用旨在达到预防、诊断、治疗、监护、缓解疾病，或对损伤、残疾进行诊断、治疗、监护、缓解、补偿等目的。

4 缩略语

下列缩略语适用于本文件

GPS：全球定位系统（Global Positioning System）

Wi-Fi：无线通信技术（Wireless Fidelity）

SIM：用户识别模块（Subscriber Identity Module）

NB-IoT：窄带物联网（Narrow Band Internet of Things）

LoRa：低功耗广域网（Long Range Radio）

MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）

CoAP：受限应用协议（Constrained Application Protocol）

HTTPS：基于安全套接字层的超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）

AI：人工智能（Artificial Intelligence）

SSL：安全套接层协议（Secure Socket Layer）

TLS：安全传输层协议（Transport Layer Security）

DDoS：分布式拒绝服务（Distributed Denial of Service）

5 区域性医疗物联网平台总体架构

5.1 概述

区域性医疗物联网平台需具备大容量用户管理与智能设备管理的服务能力。平台可应用于医疗服务与管理应用，如面向市（区）级-医院级分级应用，面向行政管理部门（卫健委）、医院/医生和患者管理等角色应用，对医院的人和物进行精细化管理，实现资源的智能化、信息共享和互联互通，提升智慧城市和智慧医院智能化水平。总体架构可划分为区域医疗物联平台和医院医疗物联平台，如图1所示。

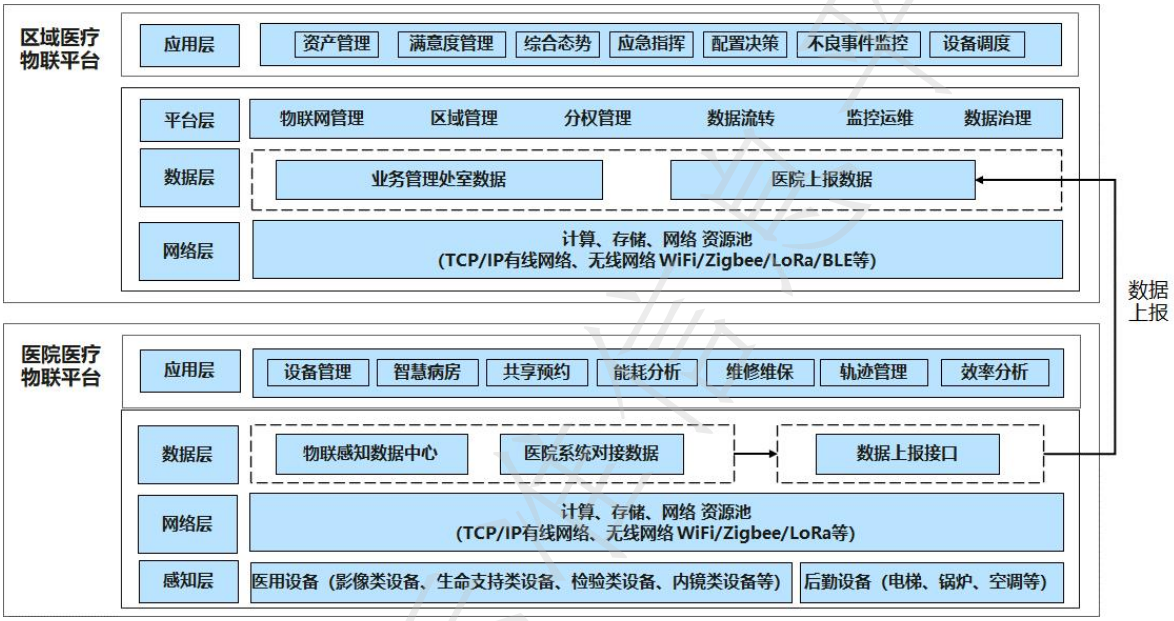

图1 平台总体架构图

5.2 医院医疗物联平台架构

医院医疗物联平台分为感知层、网络层、数据层和应用层。感知层通过将大量智能医疗设备进行接入和管理，实现对目标对象的感知与数据采集；网络层支持有线和无线多种协议，实现感知数据的灵活接入并通过网络层转发给数据层；数据层接收和汇聚各种感知数据和医疗数据，并对数据进行存储、分析和上报处理；应用层实现对医院的智慧化运营和管理。

5.3 区域医疗物联平台架构

区域医疗物联平台是一个区域性的物联数据汇聚平台，分为网络层、数据层、平台层和应用层。区域医疗物联平台通过以平台对接为主，感知设备补充的方式采集医院医用设备数据，整合全市各医疗机构分散独立、碎片化和烟囱式的物联感知资源。其中，数据层通过医院上报数据传输到平台层，平台层对感知数据进行数据解析并转发给应用层。通过区域数据流转机制，医院物联平台和区域物联平台能够协同工作，实现各种物联网应用业务服务，最终形成高度集成、协同运作的物联网网络体系。

5.4 平台协议要求

a）其他系统或设备与区域性医疗物联网平台的通信应进行身份认证；

b）应支持提供面向医疗行业设备端到云的数据通信统一协议包；

c）应考虑通信的可靠性和安全性，包括错误检测和校正机制以及加密措施；

d）不同的通信协议之间应基于协议网关达到互操作性和数据一致性的要求；

e）通信方式宜采用主流设备接口协议，如：MQTT、CoAP、HTTP/S等；

f）应支持接入区域性医疗物联网平台外部系统，如市、区级医院平台、市卫健委平台、全民健康信息平台、鸿蒙等；

g）应支持接入医疗场景下的第三方系统，如医院信息系统（HIS）、电子病历系统（EMR）、医学影像信息系统（PACS）、实验室信息系统（LIS）、医院资源规划（HRP）等。

6 功能要求

6.1 数据管理功能

数据管理功能应基于采集到的数据，对数据进行管理和服务，在保证数据权限与安全的前提下为多业务管理部门及综合业务管理提供数据支撑，通过数据安全风险分析结果，应对数据安全风险的各种技术措施。

a）平台应管理收集到的医疗和设备数据，宜参照GB/T 40684—2021的所述要求，进行平台数据管理；

b)应支持患者电子病历的交互与共享，实现电子病历数据的不可篡改、分级查阅和调阅可追溯；

c)支持采集的医疗设备数据流转到各个应用系统、大数据平台以及AI中台；通过规则引擎实现设备的智能联动以及对数据进行过滤；

d)应支持多维数据的接入，包括但不限于：环境数据、生命体征数据、体态数据、输液护理数据等多维度数据融合汇总；

e）应实现统一资源调度，便于跨部门、跨业务的融合数据分析。

6.2 资产管理功能

a）平台应支持设备等级、折旧、维修和报废管理，通过智能传感器实时监控医疗资产的使用和管理，提供决策依据；

b）利用RFID标签或条形码为医疗设备建立唯一标识,实现设备的实时跟踪定位和管理；

c）通过智能传感器和无线网络技术，远程监控医疗设备的运行状态，实时报警和故障

预警。

6.3 智慧医疗服务功能

智慧医疗服务包括患者服务、智慧医院服务和医疗管理单位服务，利用智能感知的信息为患者、医生及管理单位提供智慧服务与有效监管，包括但不限于以下功能：

a）平台应能实现在线预约功能，包括预约排队、设备调度优化等；

b）支持远程医疗咨询和健康监测，管理患者的健康档案和医疗记录；

c）支持医疗环境的安全监控和应急响应；

d）通过智能穿戴设备实时监测患者的生命体征，并将数据传输至平台；

e）允许医生和患者通过互联网远程访问数据，并在必要时远程控制或配置监测设备；

f）当患者的生命体征超出正常范围或预设阈值时，系统应能自动通知医生或紧急联系人；

g）应支持医疗机构之间检查检验结果的互认共享，减少重复检查。

7 性能要求

7.1 查询性能

a）简单查询：明确查询条件且检索记录较少的，查询响应时间<=1秒；

b）复杂查询：查询条件模糊且检索记录较多的，查询响应时间<=2秒；

c）批量查询：查询条件多个或复杂查询同时进行的，查询响应时间<=3秒。

7.2 安全性能

a）宜按照GB/T22239—2019、GB/T22240—2020所述要求,规划和设计符合国家网络安全法制度的相关要求。安全措施应包括但不限于身份验证、授权、敏感数据保密、强用户密码策略、持续监控登录用户、数据传输等方面保证系统安全运行；

b）可根据用户名获取用户授权的资源权限，实现对用户操作的资源进行控制；

c）系统对用户密码、数据库连接等敏感数据应采用国家认可的加密标准进行加密存储和处理；

d）采用单用户登录模式，监控登录用户使用系统，对于长时间未操作系统的用户采取登录认证强制失效。

7.3 网络性能

平台网络设备接入需兼容Wi-Fi、蓝牙、RFID、LoRa等多种物联网协议，以满足不同医疗设备的接入需求。平台需具备强大的并发处理能力，支持多个医疗单位并发使用，

保证系统响应时间与处理能力。平台网络应支持同时在线用户数、并发用户数以及设备联网接入满足区域医疗机构使用，并稳定在线。

7.4 数据性能

平台数据性能应能反映数据的传输能力指标：

a）应具备数据处理能力，包括数据读取速度、写入速度、查询速度和处理延迟；

b）应具备数据存储容量，包括可扩展性、数据冗余和数据压缩率。

8 接口要求

8.1 接口说明

接口主要用于实现数据的传输和交互，旨在确保数据的准确性、稳定性和安全性，以满足医疗行业的严格要求。接口传输要求应包含患者信息、资产信息、医疗设备信息等。

8.2 智能传感器接口要求

a）智能传感器的接口应支持有线或无线，有线接口包括RJ45、RS232、RS485、光纤接口等，无线接口包括Wi-Fi、蓝牙、ZigBee等；

b）智能传感器接口要求应遵循标准化和统一性，宜参照GB/T 34068—2017所述要求执行；

c）智能传感器传输安全要求宜参照GB/T 30269.807—2018所述要求执行；

d）应支持鸿蒙物联网网关接入认证功能。

8.3 设备接口要求

区域医疗物联平台应支持通过无线或有线方式与设备连接的能力，应具有接收采集数据和发送操作指令的能力。支持海量设备的接入，如鸿蒙直连设备、鸿蒙边缘子设备、射频识别设备、GPS、一维码、二维码、Wi-Fi设备、蓝牙设备、SIM卡设备、网关设备等。

8.4 安全认证要求

a）安全识别：通过安全可信识别医疗资产的风险；

b）安全保护：通过安全加固与防护设备保护医疗资产；

c）安全检测：使用安全分析平台检测安全防护的高级威胁与未知恶意文件分析，赋能防护设备阻断高级安全威胁事件；

d）安全响应：当发生安全事件，可通过安全设备告警迅速发现事件的威胁并通过调查取证和溯源找到原因，采取措施保护资产；

e）安全恢复：处理完毕安全事件，可恢复医疗平台的安全与正常运行。

9 安全性要求

9.1 物联网平台安全性要求

应包括但不限于以下安全性要求：

a）应对设备和平台之间的不同组件采用通信链路加密，如SSL/TLS协议加密传输数据，防止数据在网络传输中被窃取；

b）应能抵抗DDoS攻击，确保平台的服务不会因大量恶意请求而瘫痪。

9.2 设备安全性要求

应提供多维度的监控运维能力，包括但不限于消息跟踪、查看报表、告警管理以及设备异常检测等，提供安全检测能力，可持续检测设备的安全威胁。通过各种传感器和监测设备，实时收集数据，及时预警异常情况。

9.3 数据安全性要求

数据安全性要求应包括防止数据丢失、异常损坏、窃取及非法使用，应采取磁盘冗余保护、数据备份、数据加密、数据传输、隐私保护和严格的安全管理制度等手段，对数据进行安全保护。

a）宜按照GB/T22080—2016、GB/T22239—2019、GB/T31168和GB/T39725—2020等做好数据安全管理工作，并确保所有数据传输和处理符合医疗行业的安全和隐私保护标准；

b）账号管理：通过对大数据平台和数据仓库平台进行合理的账号管理，确保非法用户不能接入数据库；

c）敏感数据保护：利用数据脱敏和访问控制实现用户对系统和敏感数据的保护，确保敏感数据不会被非法用户看到；

d）存储安全：对数据进行多副本存储，单点故障不会导致数据丢失，对业务零影响；

e）安全审计：通过系统审计等功能实现对用户操作的全程记录，确保非法行为可追溯；

f）数据传输：应确保数据在传输过程中不被窃取、改变，保证数据的完整。基于鸿蒙物联网网关将数据转化标准模型数据上传到物联网平台，再通过鸿蒙网关达到统一协议与数据格式接入至医疗物联网平台；

g）数据共享与使用：支持医疗数据跨部门、跨业务共享和使用；

h）数据销毁：应参照网络安全法、密码法、数据安全法、个人信息保护法等法律法规

执行。

9.4 网络安全性要求

与区域医疗物联平台通信的所有系统或设备必须实施强制身份认证。应通过持续审查网络流量，实施精细化的访问控制策略，以确保及时检测、清除和阻断对网络资产的任何非法访问尝试。

9.5 兼容性

应提供数据接口标准符合DICOM 3.0国际通用标准及WS/T 500—2016、WS/T 482—2016卫生领域标准等。