ICS 35.080
L 77

T/ZJHIA

团体标准

T/ZJHIA XX-2025

医院智慧安防基本要求

General requirements for intelligent security in hospitals

2025-00-00 发布　　2025-00-00 实施

浙江省卫生信息学会　发布

目　次

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。

本文件由浙江省卫生信息学会提出并归口。

本文件起草单位：

本文件主要起草人：

医院智慧安防基本要求

1 范围

本文件规定了医院智慧安防的总体框架、基本要求与安全管理要求。

本文件适用于二级及以上医疗机构智慧安防的规划、设计、实施与管理。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 31458 医院安全技术防范系统要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB 50348 安全防范工程技术标准

GB 55029 安全防范工程通用规范

GA/T 1400 公安视频图像信息应用系统(所有部分)

3 术语和定义

GB 50348界定的以及下列术语和定义适用于本文件。

3.1

医院智慧安防 intelligent security in hospitals

基于物联网、大数据和人工智能技术，实现安全防范智能化管理。

4 总体框架

医院智慧安防总体框架由基础设施层、系统支撑层、大数据层、应用平台层和安全管理体系构成，各部分协同工作，共同完成数据的采集、处理、分析和应用支持。医院智慧安防总体框架如图1所示：

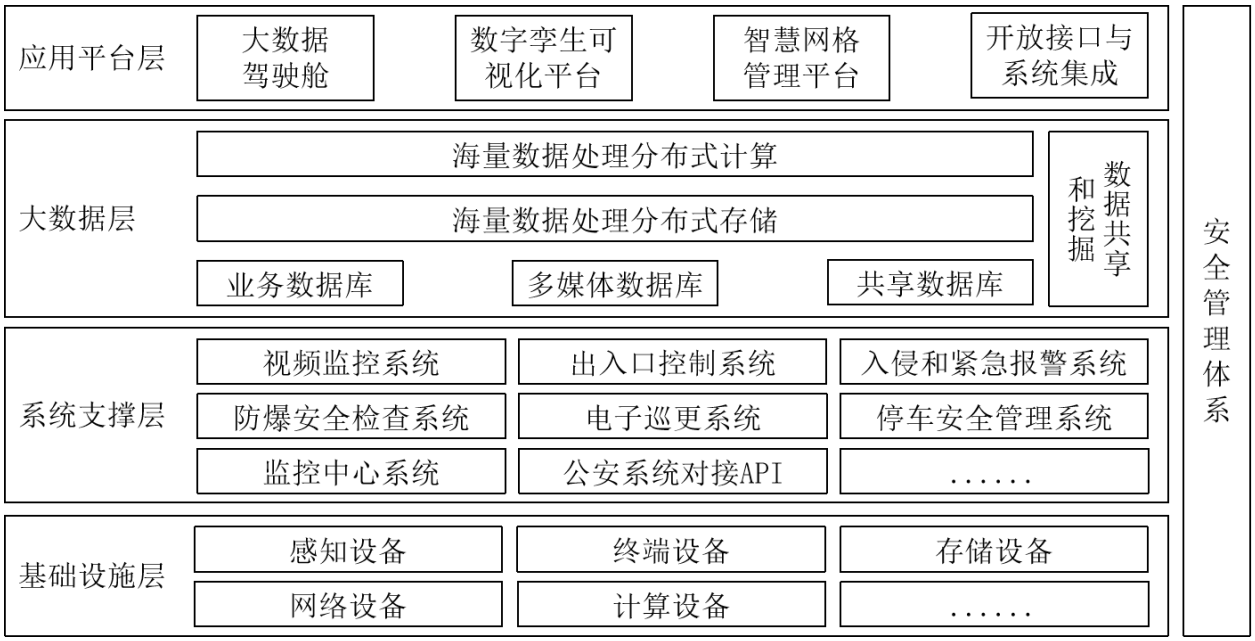

图1 医院智慧安防总体框架图

4.1 基础设施层

基础设施层为医院智慧安防提供坚实的基础设施保障，确保整个安防系统的物理基础和数据传输通畅。包含感知设备、终端设备、存储设备、网络设备和计算设备等。

4.2 系统支撑层

系统支撑层是医院智慧安防的核心操作层，通过有效的集成，提供对医院各类安全事件的实时监控和应急响应。包括视频监控系统、出入口控制系统、入侵和紧急报警系统、防爆安全检查系统、电子巡更系统、停车安全管理系统、监控中心系统以及公安系统对接API等。该层通过集成智能算法，提升安防系统的自动化与响应能力。

4.3 大数据层

大数据层负责多源数据的汇聚、融合与智能分析，利用AI技术为应用平台层提供实时数据支持，是智慧安防的核心枢纽。包括人员出入数据、医院管理数据、公共服务数据、视频数据、车辆出入数据、电子巡更数据、分析数据等相关数据等。在大数据的基础上以云计算的方式进行存储和计算，进行数据共享和数据挖掘，为医院智慧安防提供数据支撑。

4.4 应用平台层

应用平台层作为医院智慧安防的核心功能层，基于大数据层提供的数据支持，整合并呈现医院全域的安防态势，帮助管理者实时感知安全状况，并提供智能化的决策支持。该层包括大数据驾驶舱、数字孪生可视化平台和智慧网格管理等核心模块，并通过开放接口实现与其他系统的无缝对接。

4.5 安全管理体系

安全管理体系是医院智慧安防的保障层，负责制定并执行安全管理策略，确保整个系统的高效运行和数据安全。该体系通过对安防设备、数据、人员、操作等方面的全面监管，确保医院的安全工作可以按照预定目标和标准有序进行，提升整体安防管理水平。

5 基本要求

GB 50348界定的以及下列基本要求适用于本文件。

5.1 基础设施层

——实现全院范围内各类感知数据（如视频、环境、人员定位、门禁等）的实时采集，并支持数据的快速传输。
——感知设备应具备高清（4K）画质和高精度传感能力，人员定位精度达到厘米级。
——提供高性能终端设备，实现现场数据的采集与实时交互，支持多终端（PC、移动、大屏等）的远程监控与控制。
——配备大容量、高速存储设备，满足海量视频和事件记录数据至少90天的存储需求，并具备动态扩展至PB级的能力。
——配置高速、安全、稳定的网络设备，数据传输延迟不超过500毫秒，终端响应时间不超过1秒。支持网络冗余设计，防止因故障中断数据流。
——提供强大的计算资源，支持高并发数据处理，通过云计算与边缘计算相结合的分布式架构，高效完成视频流处理、行为分析和智能识别等任务。

5.2 系统支撑层

——支持海量数据的实时处理能力，能够同时处理大规模视频流和传感器数据，满足全院实时监控需求。
——实现对全院各类安全数据的统一采集、监控与分析，包括视频监控、出入口控制、报警及应急响应等关键功能。
——通过智能算法进行数据融合与行为分析，实现异常情况（如入侵、异常聚集、火灾预警等）的实时识别和自动报警。
——记录报警事件的人员、位置、时间等信息，存储时间不少于6个月。
——采用集中管理平台，实现各子系统间的数据共享与联动响应，确保安全事件得到快速、协调的处置。
——支持对关键事件（如安全警报、异常行为、紧急状况）的自动记录、存储和回溯查询，保障信息可追溯性与管理合规性。
——视频监控系统联网信息安全要求应符合 GB 35114 的相关规定。
——与公安系统和其他医院信息系统无缝对接，确保在紧急情况下能够实现实时数据共享和联动处理。
——智慧安防管理平台联网接口应符合 GB/T 28181 的相关规定，向公安机关推送视频图像数据应符合 GA/T 1400 的相关规定。

5.3 大数据层

——大数据层应整合视频监控、门禁记录、报警信号、人员定位等多源异构数据，打破信息孤岛，实现数据的统一存储与管理，为医院全域安防提供完整的数据视图。
——通过行为模式分析（如异常聚集、徘徊检测）、事件预测（如潜在安全风险评估），并支持实时预警，提升安防的主动性与精准性。
——通过加密存储和传输技术保护敏感数据（如患者信息、监控视频），实施数据脱敏和权限分级管理，确保合规性与隐私性。

——支持海量数据实时处理，视频数据处理能力不低于每秒1000帧，报警事件处理延迟不超过500毫秒。

5.4 应用平台层

——提供实时数据展示与决策支持功能，通过仪表盘形式呈现医院安全态势（如实时报警数量、重点区域监控状态），支持事件跟踪与管理。
——实时展示医院内部及周边安防态势，支持大屏、PC和移动端操作，实现全域监测、异常定位和预警推送。
——按照网格化管理模式，将医院区域划分为多个网格区域，且每个区域可根据实际需求设定具体的安全监控规则。
——根据大数据分析结果，自动生成安防策略建议（如人员调度方案），并支持多场景联动（如检测异常后自动调取视频并触发报警）。
——提供开放API，与医院信息系统及其他智慧系统无缝对接，兼容GB/T28181等主流安防协议。
——3D安防地图刷新频率不低于每秒1次，延迟不超过1秒。
——界面操作响应时间不超过3秒，API调用响应时间不超过200毫秒。
——系统应支持动态扩展，根据医院规模和需求进行功能升级，满足未来扩展需求。

6 安全管理要求

——医院智慧安防的安全应包括物理安全、网络安全、平台安全、系统安全、应用安全、数据安全，需制定详细的安全管理策略和操作规程，并遵循行业相关的规定。
——针对医院智慧安防建立安全审计制度，定期开展安全检查和风险评估，及时发现并整改安全隐患。
——实施严格的权限分级和身份认证，确保各级用户只能访问与其权限相符的数据和功能。
——制定完善的应急预案，明确在发生安全事件时的响应流程和责任分工。
——严格遵守国家和行业关于信息安全、数据保护和网络安全的相关标准和法规，定期接受第三方安全审计，确保系统持续满足合规要求。