

T/WEA

团 体 标 准

T/WEA XXXX—2026

医院智慧医疗核心功能配置应用指南

Guideline for configuration and application of core functions of
smart healthcare in hospitals

(征求意见稿)

2026 - XX - XX 发布

2026 - XX - XX 实施

中国智慧工程研究会 发布

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 总体原则与配置框架 4

5 配置总体要求 7

6 核心功能配置要求 10

7 配置实施与验收要点 15

8 运行维护与持续改进 18

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。

本文件由中国智慧工程研究会提出并归口。

本文件起草单位：

本文件主要起草人：

全国团体标准信息平台

引 言

随着新一代信息技术与医疗卫生服务体系的深度融合，医院信息化建设正由传统“业务系统分散建设、信息孤岛割裂”的阶段，迈向以数据要素为核心、以流程协同为主线、以智能应用为牵引的“智慧医疗”新阶段。智慧医疗的目标不局限于单点应用的上线，而在于围绕诊疗服务全链条，形成覆盖“诊前一诊中一诊后”、贯穿“医疗—护理—药事—医技—运营—后勤保障”的一体化能力体系，通过标准化的数据治理、集成互联与智能化决策支持，提升医疗质量安全、改善患者体验、增强医院运行效率与精细化管理水平。

当前医院在推进智慧医疗建设过程中，普遍面临以下共性问题：一是核心业务功能配置缺乏统一的结构化框架，不同医院在功能边界、模块粒度、数据口径方面差异较大，导致可复制性弱、建设成本高；二是系统建设重“上系统”、轻“用系统”，功能配置与临床路径、护理流程、药事管理、医技检验检查等关键业务流程耦合不足，影响落地效果；三是多系统并存、接口标准不统一，院内外数据共享受限，难以支撑区域协同、医联体协作与监管报送；四是智能应用引入缺乏分级分域的方法，临床决策支持、智能预警、智能随访等功能在安全可控、可解释性与持续评估方面存在短板；五是数据安全与隐私保护、合规审计、权限控制与安全运营等基础能力不均衡，给医院带来合规风险与运行风险。

为解决上述问题，本文件从“核心功能可配置、配置可落地、落地可评估、评估可迭代”的角度出发，提出医院智慧医疗核心功能的配置与应用指导思路，旨在为医院规划建设、系统选型、功能配置、集成实施、运行维护与持续改进提供统一参考。与强调单一系统建设的技术规范不同，本文件聚焦“核心功能配置与应用”这一关键抓手，强调以临床与管理需求为驱动、以流程为主线、以数据为底座、以安全合规为前提，促进医院智慧医疗能力体系的系统化构建与成熟度提升。

本文件所指“核心功能”，强调对医院智慧医疗建设具有基础支撑与广泛适用性的功能集合，通常包括但不限于：面向患者的智慧服务能力、面向医护的智慧诊疗与护理能力、面向医技与药事的协同能力、面向运营管理的精细化能力、面向支撑体系的集成互联与数据治理能力，以及贯穿全域的安全与合规能力。在此基础上，本文件强调“配置”不仅是软件功能开关或模块启用，更包含业务规则、流程节点、角色权限、数据字典、指标口径、接口策略与运行监控等可管理要素的系统配置。

通过本文件的实施，可期实现以下综合效果：统一智慧医疗核心功能配置的术语体系与功能框架，提升医院建设方案的可比性与可复制性；以流程与数据为抓手提升系统应用深度与协同效率；强化医疗质量安全控制与运营管理的精细化水平；在合规与安全可控前提下促进智能应用规范引入与持续评估，最终推动医院智慧医疗建设从“项目交付”向“能力运营”转型。

医院智慧医疗核心功能配置应用指南

1 范围

本文件规定了医院智慧医疗核心功能的总体原则与配置框架、配置总体要求、核心功能配置要求、配置实施与验收要点、运行维护与持续改进等要求。

本文件适用于各级各类医院（含综合医院、专科医院、中医医院及其他具备临床诊疗服务能力的医疗机构）开展智慧医疗相关信息系统与智能应用的核心功能配置与应用管理，也可作为医联体牵头医院对成员单位开展能力对标、协同建设与应用评估的参考依据。

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。

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

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧医疗 smart healthcare

综合运用信息技术与智能技术，对医院诊疗服务、护理服务、医技服务、药事服务及管理服务进行数字化、网络化与智能化改造，以实现流程协同、质量安全提升、资源优化配置和服务体验改善的能力体系。

3.2

智慧医院 smart hospital

以数据治理与互联互通为基础，以临床诊疗与管理决策为核心，形成覆盖医疗、服务、管理与保障全链条的数字化与智能化运行体系的医院建设形态与运行模式。

3.3

核心功能 core functions

对医院智慧医疗建设具有基础支撑作用、适用范围广、可复用性强，且能够显著影响诊疗质量安全与运营效率的一组关键功能集合，通常包括智慧服务、智慧诊疗、智慧护理、智慧医技、智慧药事、智慧管理与运营、集成互联与数据治理、安全与合规等功能域中的关键能力。

3.4

功能配置 function configuration

为实现目标业务流程与管理控制要求，对信息系统或平台的功能模块、业务规则、流程节点、数据字典、角色权限、接口策略、提醒与预警阈值、表单模板、指标口径等可参数化要素进行设定、组合与启用的活动。

3.5

业务流程 business process

在特定业务目标约束下，由多个角色按照既定规则完成的一组可重复的业务活动序列，包含触发条件、输入输出、关键节点控制、异常处理与闭环反馈等要素。

3.6

闭环管理 closed-loop management

围绕关键业务流程形成从“发起—执行—核对—记录—追溯—反馈—改进”的完整链路控制机制，确保各环节状态可识别、责任可定位、过程可追溯、结果可验证。

3.7

电子病历 electronic medical record

以患者就诊过程为主线，对诊疗活动及相关管理信息进行结构化与非结构化记录的电子化病历信息集合，支持医疗文书记录、医嘱执行、检查检验、用药管理、质量控制与追溯等业务应用。

3.8

结构化数据 structured data

按照预定义的数据模型、编码体系或数据元规范进行采集与存储的数据，具备明确的字段含义、取值范围与语义一致性，便于统计分析、互联互通与智能计算。

3.9

数据元 data element

用于描述信息交换或数据管理的最小数据单元，通常由名称、定义、数据类型、表示格式、取值范围、编码规则等属性构成。

3.10

主数据 master data

在医院多个业务系统间共享使用、相对稳定且需要统一管理的关键基础数据集合，通常包括患者、人员、机构科室、诊疗项目、药品、耗材、检验检查项目、设备资产等对象的基础信息及其编码映射关系。

3.11

身份认证 identity authentication

对用户、系统或设备的身份真实性进行验证的过程，可采用口令、证书、多因素认证等机制，为访问控制与审计追溯提供前置保障。

3.12

访问控制 access control

基于身份、角色、职责与授权策略，对信息资源访问范围、操作权限与数据可见性进行限制与管理的机制，通常包括最小权限、职责分离、授权审批与动态授权等要求。

3.13

审计日志 audit log

对系统访问、关键操作、配置变更、数据查询与导出等行为进行记录的日志信息集合，用于追溯责任、发现异常、满足合规与安全运营需要，并支持对日志完整性与不可抵赖性的保护。

3.14

数据分级分类 data classification and grading

依据数据对业务影响、敏感程度、合规要求与安全风险等因素，对数据进行类别划分与等级标识，并据此确定存储、传输、共享、脱敏、访问控制与审计等安全策略的过程。

3.15

脱敏处理 data masking

在不改变数据整体可用性的前提下，对个人身份信息或敏感信息进行遮蔽、替换、泛化或扰动，使非授权对象无法识别或还原敏感内容的处理方式。

3.16

互联互通 interoperability

不同信息系统、设备或平台之间按照约定的数据标准、接口规范与业务规则，实现信息交换、语义一致与流程协同的能力。

3.17

接口服务 interface service

用于实现系统间数据交换与业务协同的服务能力集合，通常包括数据查询与回写、消息通知、订单或任务下发、状态回传、统一编码映射与错误处理等能力，并应支持接口版本管理与调用监控。

3.18

临床决策支持 clinical decision support

基于临床知识库、指南路径、规则模型或算法模型，对诊疗过程提供提示、预警、建议或风险识别的功能集合，常用于用药安全、检验检查合理性、病情评估、感染防控与质控干预等场景。

3.19

预警机制 alerting mechanism

基于规则、阈值或模型结果，对异常状态、潜在风险或关键时限进行自动识别并触发提醒、告警与处置流程的机制，应包含触发条件、接收对象、处置责任、升级路径与关闭规则。

3.20

成熟度 maturity level

用于描述医院智慧医疗能力在制度流程、数据治理、系统协同、应用深度、智能化水平与安全合规等方面发展阶段与能力水平的分级评价概念，可用于对标建设目标、制定分期路线与持续改进计划。

4 总体原则与配置框架

4.1 总体原则

4.1.1 功能配置应围绕患者就医主旅程与医疗服务主流程展开，优先保障诊疗可及性、连续性与体验一致性。对门急诊、住院、日间手术、检查检验、药事服务、出入院管理、随访管理等关键环节，宜形成端到端的流程闭环与跨科室协同。

4.1.2 功能配置应以医疗质量与患者安全为底线要求，突出医嘱闭环、身份核验、关键节点双人核对、异常值预警、用药安全审查、抗菌药物管理、手术安全核查、护理风险评估与预警、院感防控等关键能力的可用性与可靠性，避免仅追求“智能化展示”而忽视风险控制。

4.1.3 核心功能配置应建立统一的数据标准体系与主数据管理机制，确保患者、人员、科室、诊疗项目、药品、耗材、检验检查项目、设备资产等关键对象的编码、口径与映射关系一致，支撑跨系统共享、统计分析、监管报送与智能计算。

4.1.4 医院智慧医疗能力宜通过统一集成架构实现跨系统业务协同与数据互通，避免点对点接口碎片化。对高频交互、关键闭环与跨域协作场景，宜采用标准化接口服务、消息通知与状态回传机制，并配套接口版本管理、调用监控与故障处置策略。

4.1.5 核心功能配置应根据医院规模、学科结构、信息化基础与管理成熟度，实施“先打底座、再强闭环、后上智能”的分期路线。上线后应建立运行监测、问题闭环与持续优化机制，形成“配置—应用—评价—改进”的持续迭代。

4.1.6 核心功能配置与应用应把网络安全、数据安全、个人信息保护、身份认证、访问控制、审计追溯、数据分级分类与脱敏、第三方接入管理等要求嵌入到系统设计与配置基线中，实现“最小权限、可审计、可追溯、可管控”。

4.1.7 医院智慧医疗核心功能可按“面向服务对象—面向业务链条—面向支撑体系”的逻辑进行划分，形成可配置、可评估、可迭代的能力框架。功能域划分宜至少覆盖以下内容：

- 智慧服务：面向患者与公众的服务触点与就医协同能力；
- 智慧诊疗：面向医生的诊疗记录、医嘱执行、路径与质控能力；

- 智慧护理：面向护士的评估、执行、交接与风险预警能力；
- 智慧医技：面向检验检查、影像、病理等医技环节的协同能力；
- 智慧药事：面向药品供应、处方审核、用药管理与临床药学能力；
- 智慧管理与运营：面向资源、成本、绩效、质量与运营监测能力；
- 集成互联与数据治理：面向数据标准、主数据、交换共享与数据服务能力；
- 安全与合规：贯穿全域的安全控制、审计追溯与合规保障能力。

为便于医院形成配置清单与实施路径，本文件将上述功能域进一步抽象为“能力要素”，每一能力要素应至少包含：业务对象、流程节点、角色职责、数据项与口径、接口交互、规则与阈值、异常处置与闭环、日志与审计、指标与监测等配置要素。

表1给出了核心功能域与典型能力要素示例，供配置建模与清单化管理使用。

表1 核心功能域与典型能力要素

功能域	典型能力要素	配置关注点
智慧服务	预约挂号、导诊分诊、移动支付、报告查询、线上宣教与随访	规则（号源/优先级）、身份核验、消息通知、渠道一致性
智慧诊疗	结构化病历、医嘱闭环、临床路径、质控规则、CDSS提示	表单模板、规则库、医嘱执行状态、预警阈值、可解释性
智慧护理	护理评估、医嘱执行、巡视记录、压疮/跌倒风险预警	评估量表、任务分派、交接班要素、预警升级路径
智慧医技	申请开立、预约排程、结果回传、危急值管理	检查适应证提示、排程规则、危急值闭环、报告结构化
智慧药事	处方审核、用药交互、药品追溯、抗菌药物管理	审核规则、权限策略、药品字典、追溯码、审计留痕
智慧管理与运营	资源排班、绩效核算、成本核算、运营看板	指标口径、数据来源、权限与脱敏、报表版本控制
集成互联与数据治理	主数据、数据标准、接口服务、数据服务目录	编码映射、接口规范、服务编排、数据质量规则
安全与合规	身份认证、访问控制、审计日志、数据分级分类	最小权限、职责分离、留痕不可抵赖、脱敏与共享审批

4.2 配置对象与配置边界

核心功能配置宜围绕四类对象建立统一的配置模型与边界控制：

4.3 人员与角色

包括岗位角色、职责边界、授权审批、临时授权、多点执业与外协人员管理等。应明确医生、护士、医技人员、药师、管理人员、运维人员、第三方服务人员等角色在不同场景的可见数据范围与可执行操作。

4.3.1 流程与节点

包括流程触发条件、节点顺序、必填要素、校验规则、异常分支、时限控制、升级路径与闭环条件。流程配置应与制度文件、临床路径、护理规范、药事规则、院感要求等保持一致，并确保关键节点具备可追溯性。

4.3.2 数据与口径

包括数据元、数据字典、编码体系、主数据、统计口径与指标定义。应明确结构化采集要求、数据质量规则、缺失值与异常值处理策略、跨系统字段映射关系、监管报送口径一致性等。

4.3.3 系统与接口

包括模块启用、参数策略、接口服务、消息机制、版本管理与容灾策略。应明确“核心系统—协同系统—外围系统”的交互边界，避免业务关键闭环依赖不稳定或不可控的外部接口。

4.4 分期建设与能力成熟度思路

4.4.1 底座能力夯实

以数据标准、主数据、统一身份认证与权限、审计日志、基础集成与互联互通为重点，形成可控、可用、可追溯的基础运行环境，为后续闭环与智能应用奠定条件。

4.4.2 关键流程闭环

围绕高风险与高频场景优先建设闭环能力，如医嘱闭环、危急值闭环、手术安全核查闭环、输血闭环、用药审核闭环、护理风险闭环、院感关键环节闭环等，确保质量安全收益可量化。

4.4.3 智能应用强化与运营提升

在闭环稳定运行基础上，引入临床决策支持、智能预警、智能随访与健康管理、运营预测与资源优化等能力，并建立持续评估机制，确保智能应用“可解释、可验证、可回退、可审计”。

4.4.4 协同联动与生态扩展

面向医联体、区域平台、互联网医院、医保与监管对接等场景，强化跨机构互联互通、数据共享审批与脱敏策略、统一身份与互信机制，形成更大范围的协同服务能力。

4.5 配置文档化、基线管理与变更控制

4.5.1 配置清单与配置说明

对核心功能域、模块启用、关键参数、规则库、阈值、表单模板、消息通知策略、接口清单与版本等形成结构化清单，并保持与制度流程的一致性说明。

4.5.2 配置审查与上线验收

对涉及质量安全、用药安全、隐私保护、权限控制、数据共享与外部对接的配置项，应实施上线前审查与验收，确保关键风险可控、回退方案明确。

4.5.3 变更管理与回退机制

对规则库调整、阈值调整、权限变更、接口变更、表单模板变更等应执行变更申请、影响评估、灰度发布与回退机制，确保业务连续性与审计可追溯。

4.5.4 运行监测与持续优化

应建立配置效果的运行监测指标，定期评估预警有效性、闭环完成率、超时率、误报漏报率、用户使用率与满意度等，并以问题闭环推动配置迭代。

5 配置总体要求

5.1 配置准备与现状评估

医院在开展智慧医疗核心功能配置前，应开展现状评估与差距分析，形成配置基线与分期实施路线。现状评估宜覆盖业务、数据、系统、组织与安全等维度，并输出可追溯的评估结论、问题清单与整改计划。

现状评估应至少满足以下要求：

- a) 明确评估范围，覆盖门诊、急诊、住院、手术麻醉、医技检验检查、药事、护理、病案、质控、运营管理等主流程；
- b) 识别高风险与高频场景，明确关键控制点（如身份核验、医嘱执行、危急值处置、输血、手术核查等）的现状完成率与主要断点；
- c) 梳理核心数据对象（患者、人员、科室、项目、药品、耗材、检验检查项目等）的编码一致性、映射关系与质量问题；
- d) 形成系统清单与交互链路图，识别接口碎片化、回传缺失、状态机不一致等影响闭环的问题；
- e) 评估身份认证、访问控制、审计日志、数据分级分类、脱敏与共享审批、第三方接入等安全能力，明确风险点与整改优先级。

现状评估维度与输出成果要求见表2。

表2 现状评估维度与输出成果要求

评估维度	评估重点	主要输出成果示例
业务	主流程梳理、关键控制点、闭环断点、高风险/高频场景	流程现状图；关键控制点清单；断点问题清单；优先级排序
数据	数据标准、数据元、主数据、口径一致性、质量规则	主数据对象清单与编码映射；数据质量问题清单；口径对齐方案
系统	系统边界、模块启用状态、接口方式、版本与运维能力	系统清单；系统交互链路图；接口清单；依赖与风险清单
组织	牵头部门、职责分工、治理机制、培训与考核	项目组织架构与RACI；会议机制；变更流程；培训计划
安全	身份认证、权限策略、审计留痕、分级分类、脱敏与对外共享	安全现状评估报告；整改计划；安全配置基线草案

医院智慧医疗核心功能配置应形成“评估—建模—配置—验证—运行—监测—改进”的闭环管理机制，以保障配置活动可管理、可验证、可追溯，并支撑持续优化。该闭环流程的结构应与图1相符合。

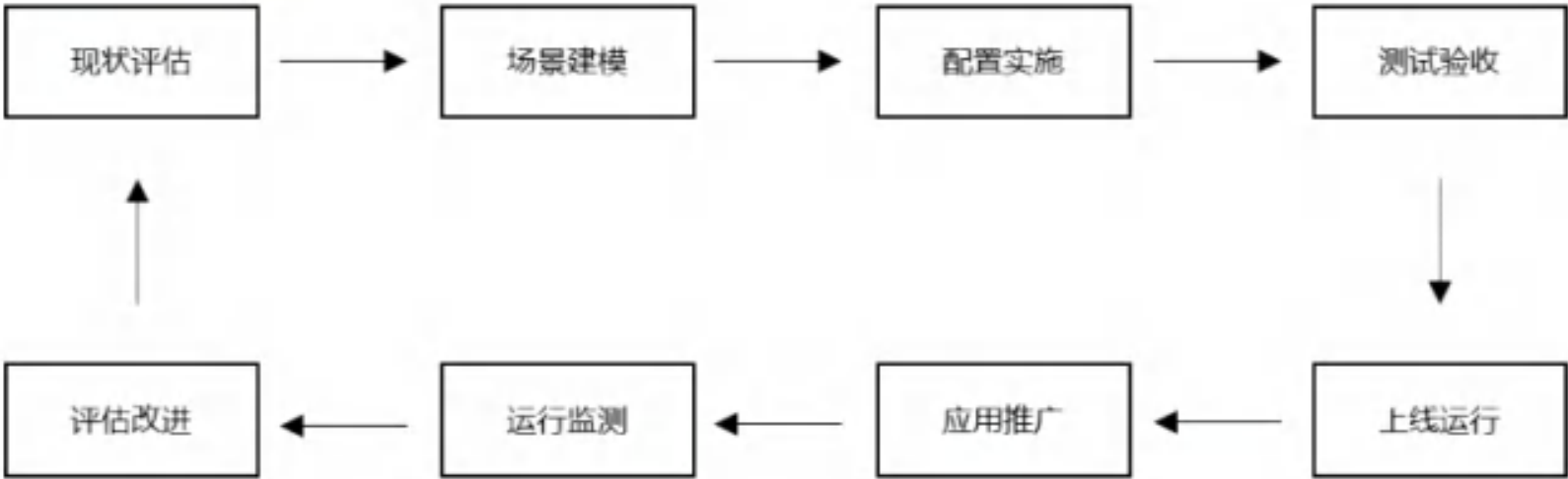


图1 医院智慧医疗核心功能配置与运营闭环流程示意图

5.2 需求管理与场景清单化

医院应采用“场景驱动”的方法形成需求清单，将核心功能配置落实到业务流程与可验收的场景闭环中，避免仅以系统功能菜单作为配置依据。

场景清单宜覆盖诊前、诊中、诊后全过程及院内外协同边界。每个场景应至少描述 触发条件、参与角色、输入输出数据、关键控制点、异常分支、闭环判定条件、时限与升级路径、审计点与指标口径等要素。

场景优先级宜综合考虑医疗质量安全影响、业务高频程度、患者体验影响、合规与监管要求、实施复杂度与依赖条件等因素。对涉及患者安全的高风险场景，应优先纳入近期建设并明确验收标准。

表3 场景需求清单模板

字段	内容要求
场景名称	采用“业务对象+关键动作”的命名方式，例如“危急值通知与处置闭环”
触发条件	明确触发事件与来源系统/岗位
涉及角色	至少列出责任角色、协同角色与审批角色
输入/输出数据	列出关键数据项、编码口径与必要字段
关键控制点	明确必须校验、必须记录、必须回传的节点
异常分支	包括超时、拒绝、撤销、重复、数据缺失等处理
闭环判定条件	明确“闭环完成”的状态机与完成条件
时限与升级	明确处置时限、提醒频次、升级路径与责任归属
审计与留痕	明确应记录的日志要素与不可抵赖要求
验收样例	提供可复核的测试样例、验收数据与判定方法

需求变更应纳入统一的变更管理流程。对规则库调整、阈值调整、权限策略变更、接口字段变更、模板变更等，应进行影响评估、验证测试、灰度发布与回退方案设计，确保业务连续性与审计可追溯。

5.3 数据元与主数据配置

核心功能配置应以统一的数据标准体系与主数据管理机制为前提。医院应建立数据字典与数据元管理机制，并将其与表单模板、接口字段、指标口径进行一致性绑定。

主数据应实施统一编码、统一维护、统一分发与统一变更控制。主数据对象宜至少包括 患者主索引、人员与资质、机构科室、诊疗项目、药品、耗材、检验项目、检查项目、设备资产等。主数据变更应具备审批、发布与回滚机制，避免因编码不一致导致闭环失败。

结构化采集应遵循“先口径、后模板、再质控”的路径。医院宜在关键病历文书、关键医嘱、关键护理评估与关键医技结果等环节优先推进结构化采集，并配置必填校验、逻辑校验、范围校验与编码校验等数据质量规则。

5.4 集成互联与接口协同配置

医院应建立统一的集成互联策略，优先采用平台化方式实现跨系统业务协同与数据交换。对关键闭环场景，应配置标准化的状态机与回传机制，确保闭环判定条件可计算、责任可定位、过程可追溯。

接口协同配置应至少满足以下要求：

- a) 明确关键闭环接口的最小数据集与必备状态字段（含状态码、时间戳、执行人、异常原因码等）；
- b) 建立接口版本管理与兼容策略，明确字段新增、枚举扩展、含义变更等变更规则；
- c) 配置接口调用监测与告警阈值，覆盖调用量、成功率、时延、错误码分布、重试策略等；
- d) 建立故障分级响应与应急处置流程，关键接口应具备降级与补偿机制；
- e) 对院外协同对接，应在最小必要、分级分类、共享审批与脱敏策略约束下配置交换范围与频率。

5.5 身份认证与角色权限

医院应建立覆盖“人员—角色—职责—权限—数据范围”的统一授权模型，并与组织架构、值班排班、临时授权与外协人员管理机制联动。权限配置应坚持最小权限与职责分离原则。

权限策略应重点控制以下高风险操作：

- a) 病历查询与批量导出；
- b) 医嘱与处方开立、撤销、修改；
- c) 检验检查结果更正、报告撤回与重发；
- d) 危急值确认、关闭与补录；
- e) 护理执行确认、交接班关键要素修改；
- f) 药品调拨、退药、盘点差异处理；
- g) 费用调整与退费；
- h) 规则库、阈值、字典、接口映射等关键配置变更。

身份认证应满足安全策略要求。对远程访问、运维管理、规则维护、批量导出等高风险场景，宜采用更高强度认证措施，并强化审计与告警。

5.6 规则库、阈值与知识内容配置

医院应建立规则库治理机制，确保规则来源可追溯、变更可控、效果可评估。规则与阈值应记录依据、版本、适用范围与维护责任。规则变更应经业务审核，必要时经相关管理委员会审议，并在上线前完成验证测试与灰度发布，保留回退版本。

对预警类规则，医院应定期评估触发量、处置完成率、超时率、误报率、漏报识别情况与采纳率，避免告警疲劳或规则失效。对决策支持类规则或模型输出，应提供必要的解释信息与证据链呈现方式，并明确可回退策略。

5.7 日志审计与配置留痕

医院应建立覆盖业务操作、数据访问、接口调用、配置变更与异常处置的全链路审计机制。审计日志应至少记录：操作者身份、时间、对象、操作类型、操作结果、来源终端或网络信息、关键字段变化摘要等，并满足完整性保护与防篡改要求。

对核心配置项应实施配置留痕与版本管理。对规则库、阈值、权限策略、模板、接口映射、主数据字典等关键配置，宜采用配置中心或版本库实现可对比与可回滚，并保留变更原因、审批记录与实施记录。

5.8 测试验证与回退

核心功能配置上线前应完成分层测试与业务验证，包括配置一致性核验、典型流程联调、异常分支与超时测试、接口容错与重试测试、权限边界测试、日志审计完整性测试，以及性能与并发测试等。

上线验收应以“场景闭环”为核心。对每个纳入范围的关键场景，应明确验收样例、验收数据、验收角色与判定条件，形成可复核的验收记录。对不能一次性全量切换的场景，宜采用灰度上线与分批切换策略，并设置明确的回退触发条件与回退流程。

5.9 运行监测与应用推广

医院应建立运行监测体系，将核心功能配置纳入常态化运营管理。运行监测指标宜覆盖闭环质量、预警有效性、系统与接口稳定性、数据质量、安全合规与用户体验等方面。

应用推广应与制度流程、培训考核与支持机制联动。医院宜按角色制定分层培训与复训计划，将关键闭环与安全合规要求纳入岗位培训与日常督导。

5.10 安全与合规配置基线要求

医院应建立安全与合规配置基线，将身份认证、访问控制、审计留痕、数据分级分类、脱敏与共享审批、终端与远程访问控制、第三方接入管理、接口安全、漏洞管理与安全事件响应等要求融入功能配置全过程。

对涉及个人信息处理的功能，应落实合法、正当、必要原则，配置告知与授权、最小化采集、访问控制与审计、去标识化或脱敏、对外提供审批与记录等措施，并将隐私风险评估与整改纳入上线验收与运行监测。

6 核心功能配置要求

6.1 智慧服务功能配置要求

6.1.1 功能范围与配置目标

智慧服务功能配置应面向患者就医全流程与多触点服务一致性，配置目标应覆盖 就医前信息获取与预约、就医中导诊分诊与支付结算、就医后报告查询与随访管理等关键环节，形成以患者为中心的“一次身份、全程服务、全链可追溯”的服务体验。

智慧服务配置应优先保障服务的可用性与一致性，避免出现“线上入口可用但线下流程无法承接”“多个渠道信息口径不一致”“支付结算与收费系统不同步”等影响体验与安全的情况。

6.1.2 就医身份管理与多渠道一致性

智慧服务应配置统一的患者身份管理与多渠道一致性策略，至少满足以下要求：

- a) 建立患者主索引与身份绑定机制，支持证件号、手机号、就诊卡号、医保凭证等多标识映射与一致性校验；
- b) 配置实名制与必要的身份核验策略，确保预约、支付、报告查询、线上问诊与随访等场景的身份可信；
- c) 配置线上线下渠道一致性要求，明确同一患者在窗口、自助机、移动端、网站端等渠道的基本信息、预约记录、缴费记录、检查检验结果查询口径保持一致；
- d) 配置异常身份处理机制，包括重复建档、证件变更、代办与监护人代管、儿童与特殊人群身份管理等，并确保审计留痕。

6.1.3 预约挂号与号源管理

预约挂号功能应配置面向门诊、检查、检验与治疗等资源的号源策略与规则体系，至少包括 号源池划分（科室/医生/时段/号别）、放号策略、预约时限与退改规则、爽约管理与黑名单策略、优先级策略（急诊/绿色通道/特需/复诊等）以及资源调整与补号机制。

预约流程应形成可追溯的闭环链路，至少实现从“预约申请—号源锁定—支付—签到—就诊—费用与结果关联—结束/取消”的状态记录与回传。预约状态机与处置规则应与院内实际接诊流程一致，并按场景需求条目方式进行配置与验收，场景描述格式宜符合表3。

6.1.4 导诊分诊与就诊导航

智慧导诊分诊应配置线上线下一体的就诊导航能力，至少包括 科室与专病专症导航、位置导航与候诊信息展示、患者排队叫号信息联动、分诊规则与人工干预机制。涉及急诊分级分诊或专科分诊的，应将分诊规则、风险提示与分流策略纳入可配置规则库，并记录规则依据与适用范围。

导诊分诊产生的关键提示、分诊建议、人工调整与最终去向应留痕可追溯，形成“提示—确认—执行—反馈”的服务闭环，闭环流程结构应与图1相符合。

6.1.5 支付结算与电子票据

智慧支付应与收费结算系统一致协同，配置目标应实现“费用生成可追溯、支付状态可回传、退费流程可闭环、票据开具可对账”。配置应至少包括：支付渠道策略（窗口/自助/移动端/第三方支付）、支付超时与撤销规则、退费触发条件与审批策略、对账周期与异常处理、电子票据开具与查询策略。

支付与退费操作应强化权限与审计，尤其是批量退费、异常冲正与人工更改支付状态等高风险操作，应按第5章权限控制与审计要求配置最小权限与强化留痕。

6.1.6 报告查询、健康宣教与随访

报告查询应配置检验检查结果的发布策略、延迟策略与异常值提示策略，明确哪些结果可对患者开放、开放时点、展示方式与必要的解释提示。对危急值等高风险信息的患者端展示，应配置合适的提示与引导机制，并与院内危急值处置闭环保持一致，避免患者端提前获知而院内尚未处置导致风险。

健康宣教与随访应配置随访计划、随访内容模板、触发条件、发送渠道、回收机制、异常反馈升级路径与闭环判定条件，并对涉及个人信息与健康信息的处理配置告知授权、权限控制与审计策略。

6.1.7 智慧服务运行监测与体验改进

智慧服务应建立以可用性与体验为导向的运行监测体系，指标宜纳入表4体系并结合服务场景补充，例如预约成功率、线上支付成功率、退费闭环时长、报告可达率、随访回收率、患者满意度与投诉等。监测结果应形成改进闭环，并与图1所示闭环流程一致。

6.2 智慧诊疗功能配置要求

6.2.1 功能范围与配置目标

智慧诊疗功能配置应围绕诊疗活动全过程，重点配置电子病历记录、医嘱闭环、临床路径、质控规则与临床决策支持等能力，目标是实现诊疗过程可记录、关键节点可控制、风险可预警、质量可追溯、数据可复用。

智慧诊疗配置应坚持“先闭环、后智能”的路径，优先确保医嘱执行、危急值处置、手术核查、用药安全等关键流程闭环稳定运行后，再引入更高影响的智能提示或模型输出。

6.2.2 电子病历与结构化记录配置

电子病历应配置统一的病历模板体系与结构化采集策略，至少包括 门急诊病历、入院记录、病程记录、出院记录、手术记录、麻醉记录、会诊记录等关键文书的模板与必填要素，并建立版本管理与变更控制。

结构化记录应优先覆盖关键诊疗要素（主诉、现病史、诊断、过敏史、用药史、体征、检验检查要点、评估结论、处置方案等），并将数据元口径与编码映射固化到模板配置中。模板结构与数据口径应与医院数据标准体系保持一致，并为后续质控与决策支持提供可计算数据。

6.2.3 医嘱闭环配置

医嘱闭环应配置从“开立—审核—执行—核对—记录—停止/撤销—追溯”的全链路状态机，明确各节点责任角色、时限与异常处理规则。医嘱闭环至少应覆盖：药品医嘱、检查医嘱、检验医嘱、治疗医嘱、护理医嘱等类型，并确保执行状态与结果能够回传到病历与质控体系。

医嘱闭环的配置应至少满足以下要求：

- a) 配置医嘱类型与字典映射规则，确保医嘱分类与项目编码一致；
- b) 配置审核规则与审核责任（药师审核、医技适应证提示等），并对审核结论留痕；
- c) 配置执行确认机制与双人核对要求（如高警示药品、输血等），并记录执行人、核对人、时间与异常原因；
- d) 配置撤销、暂停、重开等异常分支处理与补偿机制；
- e) 配置闭环完成判定条件与超时预警策略，预警处置应形成闭环，结构应与图1相符合。

6.2.4 临床路径与诊疗流程协同

临床路径应配置路径准入条件、关键节点与时限、必做项目清单、变异记录与原因分类、退出条件与再入路径规则。路径执行过程应与医嘱、检验检查、护理任务、费用与病历记录联动，避免“路径停留在纸面或看板”而无法驱动实际执行。

路径变异与质控干预应形成可追溯闭环，记录触发原因、干预措施、执行结果与后续改进建议，并纳入运行监测指标。

6.2.5 诊疗质控与临床决策支持

诊疗质控应配置关键质控规则与触发条件，规则依据应可追溯。对时间敏感类规则，应配置时限提醒、升级路径与关闭规则，并统计规则触发量与处置效果，避免告警疲劳。

临床决策支持应配置适用范围、提示方式、解释信息与可回退策略。决策支持输出宜提供触发依据与关键证据点，便于临床人员判断与追溯。对高影响提示（如禁忌用药、严重相互作用、危重风险等）应配置强提醒与确认机制，并强化审计。

6.2.6 智慧诊疗运行监测与持续改进

智慧诊疗运行监测宜纳入表4指标体系，并结合诊疗特点补充指标，例如病历结构化率、关键病历及时完成率、医嘱闭环完成率、超时率、撤销率、质控问题闭环率、决策支持采纳率等。监测结果应形成持续改进闭环，并与图1所示闭环流程一致。

6.3 智慧护理功能配置要求

6.3.1 功能范围与配置目标

智慧护理功能配置应面向护理评估、护理计划、医嘱执行、巡视与交接、护理风险预警与护理质量管理等环节，目标是实现护理任务可分派、执行可核验、风险可预警、交接可追溯、质量可监测。

6.3.2 护理评估与量表配置

护理评估应配置统一的评估量表库与评估频次策略，至少包括入院评估、跌倒/坠床风险、压疮风险、疼痛评估、营养风险等。量表字段应结构化，评分规则与阈值应可配置并记录依据与版本。

护理评估结果应与护理计划、护理医嘱与预警机制联动。

6.3.3 护理任务分派与执行核验

护理任务应支持基于医嘱、路径节点、评估结果与常规护理制度的自动生成与分派，并与排班系统联动。任务执行应配置执行确认、必要的双人核对、异常原因选择与补执行机制。对输血核对、管路管理、标本采集核验等操作应配置强制核验要素与审计留痕。

6.3.4 护理交接与巡视记录

护理交接应配置交接清单、交接必填要素、风险提示与责任确认机制，确保关键患者信息、关键医嘱状态、管路与皮肤情况、隔离与院感要求等可完整传递。巡视记录应支持标准化记录与异常触发预警，形成处置闭环。

6.3.5 护理风险预警与质量管理

护理风险预警应配置触发条件、阈值、接收对象、升级路径与关闭规则，并定期评估误报率与处置效果。护理质量管理应配置质控指标口径、抽查规则与整改闭环记录方式。

6.4 智慧医技功能配置要求

医技功能配置应覆盖检验、检查、影像、超声、病理等环节的申请开立、预约排程、采集与执行、结果生成、危急值管理、报告发布与回传等流程。医技闭环应重点配置申请适应证提示、预约排程规则、标本与患者身份核验、结果结构化与危急值处置闭环、报告版本控制与撤回重发机制等。

危急值管理应配置“识别—通知—确认—处置—关闭”的闭环状态机，明确通知渠道、接收对象、时限与升级路径，并强化审计留痕。危急值闭环的流程结构应与图1相符合，其运行监测指标宜纳入表4体系并补充危急值通知到达率、确认时长、处置完成率、超时率等指标。

6.5 智慧药事功能配置要求

药事功能配置应覆盖药品目录与字典、处方与医嘱审核、用药相互作用与禁忌提示、抗菌药物与特殊管理药品管理、药品采购与库存、调剂发药、退药与报损、追溯与召回等环节。处方审核应配置规则依据、适用范围、提示方式与强制拦截策略，并建立规则变更审查与评估机制。

用药安全闭环应实现“开立—审核—调剂—发药—用药执行—不良反应与干预—追溯”的可追溯链路，对高警示药品与特殊管理药品应配置更严格的权限、双人核对与审计。药事闭环结构应与图1相符合，监测指标宜纳入表4体系并补充处方审核通过率、拦截率、干预采纳率、不合理用药问题闭环率等。

6.6 智慧管理与运营功能配置要求

管理与运营功能配置应面向资源配置、运营监测、成本与绩效、质量与安全管理、后勤保障等场景，重点配置指标口径、数据来源、权限与脱敏策略、报表版本控制与看板发布策略。运营指标体系应确保口径一致、来源可追溯、更新频率可配置，并与质量管理、财务、人事等系统的数据治理一致。

运营监测与管理决策支持的配置应避免“单纯展示”，宜配置指标阈值、预警触发与处置闭环，形成“发现—分析—处置—复盘”的闭环管理方式，结构应与图1相符合。

6.7 集成互联与数据治理功能配置要求

集成互联与数据治理应作为各分域功能落地的共性支撑，重点配置主数据统一、数据标准、接口服务目录、数据质量规则、数据服务编排与调用监控。对关键闭环接口应配置最小数据集、状态机一致性、错误码规范与重试补偿机制，确保闭环可计算与可追溯。

数据治理应配置数据资产目录、数据生命周期管理策略、数据共享审批与脱敏规则，并建立数据质量监测与整改闭环，闭环结构应与图1相符合。

6.8 安全与合规功能配置要求

安全与合规应贯穿智慧医疗各功能域。应配置统一身份认证与权限体系、审计日志与安全运营、数据分级分类与脱敏、个人信息与健康信息处理的告知授权、对外提供审批与记录、第三方接入安全管理等。对批量查询导出、跨域访问、远程运维、规则库维护等高风险活动应配置更严格的认证与审计策略。

7 配置实施与验收要点

7.1 实施组织与职责分工

医院应建立覆盖业务、信息化、质量管理与安全合规的实施组织体系，明确项目治理结构、决策机制与责任边界，保障配置实施与应用推广同步推进。

实施组织宜至少包括以下角色与职责：

- 项目牵头部门：负责总体统筹、资源协调、计划管理与阶段评审；
- 业务责任部门：负责业务需求确认、流程规则审定、验收判定与应用推广；
- 信息化部门：负责配置实施、集成联调、技术验证、运行保障与配置基线管理；
- 质量与安全管理部门：负责质量安全控制点审查、风险评估与验收监督；
- 数据治理与安全合规责任人：负责数据标准、主数据、权限审查、审计策略与合规核验；
- 供应商或集成服务方：负责产品能力实现、接口联调、缺陷修复与技术支持。

医院应制定责任分工矩阵（例如RACI），将关键场景、关键配置项、关键接口、关键规则库与关键权限策略落实到责任人，确保出现问题时可快速定位与闭环处置。职责分工的设置宜与图1所示闭环流程中的各环节责任对应一致。

7.2 实施计划与分期推进

医院应编制实施计划，明确阶段目标、工作内容、里程碑、交付物、风险与依赖条件。实施计划宜按“先底座、后闭环、再智能、终协同”的依赖关系组织，避免关键基础能力未就绪即上线高影响功能。

实施分期宜至少满足以下要求：

- a) 第一批上线场景应优先覆盖高风险与高频场景，并明确闭环完成判定条件；
- b) 每批次上线应控制变更范围，避免同时变更规则库、权限策略、接口映射与模板结构等多个高风险要素；
- c) 对跨部门协同强、接口链路长的场景，宜采用“先单科室试点、后推广复制”的方式推进；
- d) 应明确与外部系统对接的时点与边界条件，涉及共享与对外提供的，应同步落实审批与脱敏策略。

7.3 配置基线管理与变更控制

医院应建立配置基线管理机制，将核心功能配置纳入可管理资产，保证配置可复现、可审计、可回退。配置基线宜至少包括：模块启用清单、参数策略、规则库与阈值、表单模板、主数据字典与映射、接口清单与字段定义、权限模型与授权策略、日志审计策略、运行监测指标定义与口径等。

配置变更应执行变更控制，至少包括：

- a) 变更申请与分类：明确变更内容、原因、影响范围与紧急程度；
- b) 影响评估：评估对业务流程闭环、数据口径、接口兼容、权限边界与合规要求的影响；
- c) 审批机制：涉及质量安全、用药安全、个人信息处理与对外共享的变更应按医院治理机制审查批准；
- d) 验证与发布：变更应在测试环境完成验证，宜采用灰度发布并保留回退版本；
- e) 留痕与审计：变更记录应可追溯，包含申请、审核、实施、验证与上线时间等要素。

7.4 联调测试与验证要求

核心功能配置上线前应开展联调测试与业务验证，确保配置正确性、闭环完整性与系统稳定性。测试应覆盖典型流程与异常分支，并对关键安全控制进行核验。

测试验证宜至少包括以下内容：

- a) 配置一致性核验：核验主数据映射、字典口径、模板版本与规则库版本一致性；
- b) 场景闭环联调：按表3条目组织场景测试，验证状态机、时限、升级路径与关闭规则；
- c) 异常分支测试：包括超时、撤销、重复、数据缺失、接口中断、回传延迟、权限不足等；

- d) 权限边界测试：验证最小权限、职责分离、临时授权与越权拦截；
 - e) 审计留痕测试：验证关键操作、数据访问、配置变更与接口调用的日志完整性与可追溯性；
 - f) 性能与并发测试：验证高峰期预约、支付、医嘱下达、结果回传等关键接口与模块的响应与稳定性；
 - g) 安全测试与合规核验：核验远程访问、第三方接入、数据脱敏与对外共享审批流程的有效性。
- 测试用例与测试记录应可复核，测试发现的问题应进入缺陷管理流程并闭环处置。

7.5 上线切换与风险控制

医院应制定上线切换方案，明确切换范围、切换窗口、回退策略、应急处置与现场支持安排，确保医疗业务连续性。

上线切换宜满足以下要求：

- a) 采用灰度上线或分批切换策略，优先在试点科室或低峰时段切换；
 - b) 对关键闭环场景设置上线后观察期，强化监测与人工兜底机制；
 - c) 明确回退触发条件，如闭环失败率超阈值、关键接口不可用、出现不可接受的安全或合规风险等；
 - d) 上线期间应保障业务、信息化与供应商联合值守，确保问题快速响应与处置。
- 上线切换过程中的监测与处置应形成闭环，闭环处置链路应与图1相符合。

7.6 验收原则、方法与证据要求

验收应以“场景闭环达标”为核心，不宜仅以“功能可点击、页面可展示”为验收标准。验收应同时关注业务效果、数据质量、接口稳定性与安全合规达标情况。

验收方法宜包括：文档审查、现场演示、抽样验证、日志追溯核验、接口监测核验、并发压力验证（必要时）与用户试运行反馈等。对涉及患者安全的关键场景，宜采用“抽样+追溯”的方式核验闭环完成与责任可追溯性。

验收证据应至少包括：

- a) 场景验收记录：按表3条目形成的验收用例、验收过程记录与判定结论；
- b) 配置清单与版本信息：关键配置项、规则库、阈值、模板与接口版本；
- c) 数据口径与主数据映射记录：编码映射表、口径说明与一致性核验记录；
- d) 接口联调与监测记录：关键接口成功率、时延、错误码与告警记录；
- e) 权限与审计核验记录：权限矩阵、越权拦截验证、审计日志抽样核验；
- f) 安全与合规核验记录：告知授权、脱敏策略、共享审批与第三方接入管理记录；
- g) 试运行报告：问题清单、处置记录、优化措施与复验记录。

7.7 交付资料与运维移交

配置实施完成后应形成可用于长期运行维护的交付资料，并完成运维移交。交付资料宜至少包括：

- a) 配置说明书与配置清单（含版本号）；
- b) 场景清单与验收记录（按表3条目归档）；
- c) 数据字典、主数据映射与口径说明；
- d) 接口清单、字段定义、错误码与联调说明；
- e) 权限模型、角色矩阵、审计策略与安全配置基线；
- f) 规则库与阈值依据、变更流程与回退方案；
- g) 运行监测指标定义、阈值与告警策略（与表4一致或可映射）；
- h) 运维手册、应急预案与值守机制说明。

交付资料应纳入档案化管理并可追溯。运维移交应包含关键场景的应急处置演练或桌面推演，确保医院运维团队具备独立处置常见故障与变更执行能力。

7.8 培训、推广与试运行管理

医院应制定分层培训与推广计划，培训对象宜覆盖临床、护理、医技、药事、管理与运维等角色。培训内容应突出关键闭环操作要点、异常处置方式、安全合规注意事项与常见问题处理。

试运行期间应建立问题收集、分级响应、修复验证与复盘改进机制，形成问题闭环记录。试运行问题闭环的组织方式应与图1所示持续改进流程一致，并为后续常态化运行监测与优化提供依据。

8 运行维护与持续改进

8.1 运维组织与服务保障

医院应建立与智慧医疗核心功能相适配的运维组织体系与服务保障机制，形成“业务+信息化+供应商”协同的运行保障模式，确保关键业务在系统异常、接口故障、数据异常等情况下能够快速响应与恢复。

运维组织应至少满足以下要求：

- a) 明确运维责任边界，区分应用运维、数据运维、接口运维、安全运维与终端运维职责；
- b) 建立值守与响应机制，对关键业务时段（门急诊高峰、手术高峰、日结/对账窗口等）设置保障人员与快速响应渠道；
- c) 建立运维分级响应与升级机制，明确响应时限、升级条件、处置责任人与跨部门协同路径；
- d) 对供应商支持范围、支持时段、远程接入方式与安全要求作出明确规定，并纳入第三方接入管理；
- e) 建立运维知识库与常见问题处置手册，形成可复用的处置经验与标准化操作。

运维服务保障应覆盖系统可用性、性能容量、接口稳定性、数据质量与安全合规等维度，保障体系的运行逻辑应与图1所示闭环流程一致。

8.2 运行监测与告警管理

医院应建立覆盖“业务闭环质量—系统与接口稳定—数据质量—安全合规—用户体验”的运行监测体系，对关键指标设置阈值与告警策略，并形成告警处置闭环。运行监测指标体系宜按表4设置，指标口径应统一、来源应可追溯、计算方法应可复核。

运行监测至少应包括：

- a) 业务闭环监测：关键闭环完成率、超时率、补录率、重复触发率等；
- b) 预警有效性监测：触发量、处置率、升级率、误报率与采纳率等；
- c) 接口与集成监测：成功率、时延、错误码分布、消息堆积与重试次数等；
- d) 数据质量监测：缺失率、一致性、及时性、编码匹配率与异常值比例等；
- e) 安全合规监测：异常访问、批量导出、越权拦截、敏感接口调用异常等；
- f) 体验与效率监测：关键功能使用率、任务完成时长、患者端关键路径转化率与满意度相关指标等。

告警管理应至少满足以下要求：

- a) 告警分级：按业务影响与风险等级设置告警级别，并与响应时限与升级路径关联；
- b) 告警降噪：对重复告警、链路级告警联动与误报较高的告警应优化规则，避免告警疲劳；
- c) 告警处置闭环：告警应关联工单或处置记录，记录原因、措施、恢复时间与验证结果；
- d) 告警复盘：对重大或频发告警应定期复盘，形成改进措施并固化到配置基线。

8.3 故障管理与应急处置

医院应建立故障管理与应急处置机制，确保在系统故障、接口中断、数据异常或安全事件情况下维持业务连续性，减少对医疗服务与患者安全的影响。

故障管理应至少包括：

- a) 故障分类分级：按影响范围（单科室/全院）、影响程度（一般/严重/重大）与故障类型（应用/接口/网络/数据/安全）分类；
- b) 故障定位与根因分析：明确定位路径，保留证据链（日志、监测曲线、接口报文、配置变更记录等）；
- c) 业务连续性保障：对关键场景设置降级策略与人工兜底流程，明确“可降级功能”和“不可降级功能”；
- d) 恢复验证：故障恢复后应验证关键闭环、关键接口与关键数据口径是否恢复正常；
- e) 复盘与预防：对严重及以上故障应形成复盘报告，明确整改措施、责任人、时限与验证方式，并纳入持续改进。

应急处置流程应覆盖“发现—分级—响应—处置—恢复—验证—复盘—改进”全链路。对涉及患者安全的关键闭环场景，应明确处置优先级与最短恢复目标，并在应急预案中体现。

8.4 配置项治理

医院应对核心配置项实施运行治理，确保配置在长期运行中保持一致性、有效性与可控性。治理对象包括但不限于：规则库、阈值、表单模板、主数据字典、接口映射、权限策略、消息通知策略与运行监测阈值等。

配置治理应至少满足以下要求：

- a) 版本管理：关键配置应具备版本号、适用范围、变更记录与回退点；
- b) 变更控制：配置变更应按第7章变更流程执行，尤其是涉及质量安全、用药安全与个人信息处理的配置项；
- c) 有效性评估：对预警规则、决策支持提示、时限阈值等应定期评估有效性，评估指标宜纳入表4体系；
- d) 告警疲劳治理：对高频提示、低采纳率提示应优化触发条件、分级策略或展示方式；
- e) 证据与依据维护：规则依据（指南、制度、共识等）变更时，应同步评估规则库适用性并更新版本记录。

8.5 数据质量治理

医院应建立数据质量治理机制，将数据质量监测、问题定位、整改处置与验证固化为常态化流程。数据质量治理应覆盖结构化采集数据、主数据、接口交换数据与分析指标数据，确保统计口径一致、数据可用可复核。

数据质量治理至少应包括：

- a) 质量规则库：建立缺失、重复、范围、逻辑一致性、编码匹配与及时性等规则；
- b) 质量监测：按表4数据质量类指标开展监测，并对关键对象设置阈值与告警；
- c) 问题闭环：对质量问题形成工单或整改记录，明确责任部门、时限与验证方式；
- d) 口径治理：对指标口径、统计周期、数据来源系统与计算规则进行统一管理，避免多版本报表导致管理决策偏差；
- e) 数据资产目录：建立数据资产目录与数据服务目录，明确数据责任人、更新频率、共享范围与使用约束。

8.6 安全运营

医院应建立面向智慧医疗核心功能的安全运营机制，覆盖身份认证、访问控制、审计追溯、数据分级分类与脱敏、第三方接入管理、漏洞管理与安全事件响应等内容，并与医院整体网络安全与数据安全管理体系协同。

安全运营至少应满足以下要求：

- a) 账号与权限运营：定期开展账号清理、权限复核与临时授权回收，重点关注离职、轮转、外协与第三方人员；

b) 审计与异常检测：对批量查询导出、跨域访问、敏感接口高频调用、越权访问拦截等开展监测与抽查，并形成处置闭环；

c) 数据分级分类与脱敏落实：对对外提供、共享交换、科研使用、运营分析等场景落实最小必要与脱敏策略，并保留审批与留痕；

d) 第三方接入控制：明确第三方接入范围、网络边界、认证方式、审计要求与应急处置机制；

e) 合规审计：按内部制度与外部监管要求开展合规检查，形成问题清单与整改计划，并验证整改有效性。

涉及个人信息与健康信息处理的，应持续核查告知授权、目的限定、最小化采集与访问控制等措施的有效性。

8.7 性能容量管理

医院应建立性能容量与可用性管理机制，确保核心功能在高峰期稳定运行。性能容量管理应覆盖应用层、数据库、中间件、接口平台、网络与终端等关键链路。

性能容量管理至少应包括：

a) 基线建立：建立关键业务链路的性能基线（响应时间、吞吐量、并发能力等）；

b) 容量评估：结合门急诊量、住院量、检查检验量、支付峰值与接口调用量进行容量评估与扩容计划；

c) 重点链路保障：对预约、支付、医嘱、结果回传、危急值等关键链路设置更严格的监测阈值；

d) 弹性与容灾：具备必要的冗余与容灾策略，并定期验证切换可用性；

e) 变更影响控制：重大版本升级或接口改造前应进行性能回归测试与容量评估。

8.8 用户支持

医院应建立用户支持与持续培训机制，保障不同角色对核心功能的正确使用与应用深度提升。用户支持与培训应纳入运行维护体系，并与制度流程与绩效考核联动。

用户支持至少应包括：

a) 支持渠道：热线、工单、现场支持与在线知识库等；

b) 问题分类：按“使用问题/配置问题/数据问题/接口问题/权限问题”分类处理；

c) 支持时限：对关键业务问题设置优先级与响应时限；

d) 复训机制：对关键闭环、关键安全合规要求与高风险操作开展定期复训；

e) 应用评估：定期评估功能使用率、关键环节依从性与满意度，作为优化依据。

8.9 定期评估

医院应建立定期评估与持续改进机制，至少按季度或半年组织一次核心功能运行评估，必要时开展专项评估（如用药安全、危急值、输血、手术核查、个人信息保护专项）。

定期评估应至少包括：

- a) 指标评估：按表4指标体系对关键指标进行趋势分析与达标评估；
- b) 风险评估：识别闭环断点、误报漏报、权限风险、数据质量风险与接口稳定性风险；
- c) 问题复盘：对重大问题、频发问题与跨部门问题开展复盘，明确根因；
- d) 改进计划：形成改进清单、责任分工、时限与验证方式；
- e) 固化与推广：验证有效的改进措施应固化为配置基线，并在全院推广复制。

全国团体标准信息平台