ICS 35.240.20
CCS L 07

T/CIAD

中国城乡发展国际交流协会团体标准

T/CIAD XXXX—2026

科室信息系统建设与管理规范

Specification for departmental information system construction and management

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2026－XX－XX 发布　　2026－XX－XX 实施

中国城乡发展国际交流协会　　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。

本文件由蚌埠医科大学第一附属人民医院提出。

本文件由中国城乡发展国际交流协会归口。

本文件主要起草单位：蚌埠医科大学第一附属人民医院、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX。

科室信息系统建设与管理规范

1 范围

本文件规定了科室信息系统建设与管理的建设原则、系统构成、系统功能、管理要求、安全与运行维护保障。

本文件适用于科室信息系统的建设与管理。

注：在不引起混淆的情况下，“科室信息系统”以下简称“系统”。

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 18894 电子文件归档与电子档案管理规范

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20988 网络安全技术 信息系统灾难恢复规范

GB/T 22080 网络安全技术 信息安全管理体系 要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 24405.1 信息技术 服务管理 第1部分：规范

GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 36092 信息技术 备份存储 备份技术应用要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

科室 administrative office

管理机构的直属单位，指机关组织系统中按业务划分的内设机构。

3.2

访问控制 access control

按确定的规则，对实体之间的访问活动进行控制的安全机制，能防止对资源的未授权使用。

4 建设原则

4.1 系统性原则

应强调系统建设的整体性和协调性，确保各组成部分之间无缝衔接，形成一个有机的整体。

4.2 先进性原则

系统应采用先进的硬件、软件和技术，确保系统的性能、稳定性和安全性。同时应注重技术的可更新性和可维护性，以便在后续发展中能够持续升级和优化。

4.3 安全性原则

系统应确保数据、信息的安全性、完整性和保密性。系统应具备多层次的安全防护机制，包括物理安全、网络安全、应用安全和数据安全等。

4.4 可扩展性原则

系统应具有一定的灵活性和扩展能力，以及具备良好的模块化设计，能够适应未来业务发展和数据增长的需求，方便在后续进行功能扩展和性能提升。

4.5 易用性原则

系统界面应友好、操作便捷，降低用户的学习成本和使用难度。系统应提供清晰的操作指南和培训，确保用户能够快速上手并高效使用系统。

4.6 合规性原则

系统建设和使用应符合国家相关法律法规、标准文件的规定。系统应具备数据备份、恢复和销毁等功能，确保档案管理的合规性。

4.7 稳定性原则

应保证系统的稳定、可靠、持续运行。

5 系统构成

5.1 概述

系统架构应运用互联网、大数据、云计算、人工智能等现代数字技术进行设计，包括基础设施层、数据层、业务支撑层、业务应用层、应用展现层、标准规范体系、安全与运行维护保障体系。

5.2 基础设施层

应依托云平台和互联网基础设施建设。

5.3 数据层

为系统提供数据存储、计算和相关软件环境的资源，保障上层对于数据的相关需求。

5.4 业务支撑层

应具备统一身份认证、日志管理、消息服务、安全监控、算法支撑、组件支撑等功能。

5.5 业务应用层

应建设便民服务、医疗服务、医疗管理、协同管理、运营管理、后勤管理、人力资源管理等内容。

5.6 应用展现层

应提供网站、移动端应用等应用入口。宜向第三方应用商提供接口服务。

5.7 标准规范体系

应建立完善的标准化体系，包括：数据标准、目录标准、评价标准、应用标准、信息安全规范、信息发布规范等。

5.8 安全与运行维护保障体系

系统建设应根据GB/T 22080和GB/T 28827.1的规定建立安全与运行维护保障体系。

6 系统功能

6.1 功能要求

系统应用应包括但不限于以下功能要求：

a) 便民服务；
b) 医疗服务；
c) 医疗管理；
d) 协同管理；
e) 运营管理；
f) 后勤管理；
g) 人力资源管理。

6.2 便民服务

具体内容和要求应包括：

a) 互联网服务：基于互联网为患者提供挂号、排队、缴费、信息查询、医患沟通等业务服务；
b) 预约服务：为患者提供实名制挂号、检查、检验、体检、处置、日间手术、住院等预约服务；
c) 就诊服务：实现号源统一管理，对内网预约平台和互联网预约平台的号源进行实时同步，支持网络、电话、窗口、诊间、社区等挂号方式，并提供门诊分诊、检验、检查、取药、治疗、体检等排队叫号服务；
d) 信用服务：对患者身份进行实名认证，具备对预约挂号后未就诊、诊疗后未付费等患者进行信息管理的能力；
e) 陪护服务：提供患者陪护预约服务，包括诊疗预约、检查、检验、处置等陪护服务；
f) 满意度评价：具备患者对预约、接诊、收费、药房、检查、陪护等过程进行评价功能；
g) 信息推送与公开：可将就诊相关信息通过多种方式通知患者或家属，根据医疗机构职能向社会公众公开就医需求相关信息。

6.3 医疗服务

具体内容和要求应包括：

a) 门急诊业务：支持门急诊电子病历规范书写，涵盖初诊、复诊、急诊等病历类型，具备病历录入、质控、模板管理等功能；实现门急诊处方、检查、检验、治疗、手术等处方和处置全流程管理，内置合理用药、医保控费等知识库，提供用药安全复核提醒；
b) 住院业务：按照规范开展住院病历书写，包含病案首页、入院记录、病程记录等完整内容，支持电子签名、三级阅改、痕迹保留等功能；实现住院用药、检查、手术、输血等医嘱全流程管理，具备临床路径管理功能，支持入出路径、变异管理及临床信息共享；

c) 护理业务：规范护理记录书写，包括体温单、危重症护理记录等，具备入院评估、出院随访、智能提醒等功能；实现非药品医嘱和药品医嘱的全过程闭环管理，支持输液全流程管理，具备患者身份确认、药品核对、智能提醒等功能；

d) 医技业务：实现手术信息全流程管理，涵盖手术申请、排班、术前访视、术中监控、术后护理等环节，支持手术室人员、物资精细化管理；开展麻醉信息管理，包括术前访视、麻醉记录、术中给药、术后随访等功能；实现临床检验、医学影像、病理、电生理等医技业务的信息管理，支持设备数据自动采集、报告审核、危急值管理等功能；

e) 移动业务：支持移动查房，具备患者信息查询、医嘱录入、影像调阅等功能；实现移动护理，涵盖患者身份识别、医嘱执行、体征采集、巡视管理等功能；提供移动药事、移动术前访视、移动物流等延伸服务；

f) 院外业务：开展患者随访管理，支持日常随访、专病随访等多种类型，具备随访计划制定、记录跟踪、数据整合等功能；提供健康宣教管理，通过多种传播方式推送疾病预防、康复、健康生活方式等信息。

6.4 医疗管理

具体内容和要求应包括：

a) 医务管理：开展电子病历质量管理，具备质控规则设置、实时监控、分析追溯等功能；实现临床路径与单病种管理，支持质控指标设置、监控及偏差分析；进行手术分级管理，基于手术分级目录授予医师相应手术权限；建立危急值管理机制，实现危急值自动筛查、提醒、干预及追溯；

b) 护理管理：对护理质量进行全流程控制，具备质控知识库设置、计划制定、考评分析、人员资质管理等功能；

c) 药事管理：支持药事信息综合管理，包括用药咨询、处方审核点评、药师查房、个体化给药方案制定等功能；开展处方点评，具备规则设置、样本抽取、统计分析、报告生成等功能；实现发药、抗菌药物、基本药物、药物物流、静脉药物配置等全流程管理，支持药品识别、追溯及安全审核；

d) 院感管理：开展院内感染监测预警，具备数据采集、自动筛查、上报审核、干预反馈、指标分析等功能，对重点区域进行综合监测；

e) 卫生应急管理：对突发急性传染病、公共卫生事件及紧急医学救援等信息进行管理，具备应急值守、监测预警、风险评估、信息报告等功能；具备应急资源管理、辅助决策、指挥调度、模拟演练等应急应对功能；

f) 数据上报管理：规范安全（不良）事件上报，包括登记、审批、反馈、分析等功能；实现传染病、重大非传染性疾病及死亡信息、预防接种信息、食源性疾病信息等的规范上报、审核、导出及数据交换。

6.5 医疗协同

具体内容和要求应包括：

a) 院内协同：开展多学科协作诊疗，具备科室管理、申请管理、协作结果管理、会诊级别管理等功能，支持患者基本信息、电子病历、检查检验等信息共享；

b) 区域协同：提供远程会诊服务，具备身份认证、病历采集、专家会诊、结果下传等功能；开展远程影像诊断，支持多种影像类型的远程诊断及影像数据标准化处理；实现分级诊疗，具备疾病分级管理、转诊申请、审核、病历协同传输、费用结算等功能；支持上下级机构的双

向转诊，涵盖专家门诊、检查检验、住院病床等预约服务及转诊全流程管理；开展区域病理共享和区域检验共享，支持标本物流跟踪、远程诊断、报告审核发布及质量控制。

6.6 运营管理

具体内容和要求应包括：

a) 财务管理：提供门急诊及住院患者费用结算与收费服务，支持多种支付途径、方式及医疗保险结算；开展财务信息管理，具备财务核算、审核、分析、监督、报表生成等功能，支持多类型财务数据采集及数据校正同步；实现审计信息管理，具备数据预警分析、审计管理、作业执行、法规管理、内控评价等模块；

b) 预算成本管理：开展全面预算管理，具备编制、审批、调整、控制、执行跟踪、统计分析等功能，支持多种预算编制方法；实现全成本核算管理，具备数据采集、收入成本分析、分摊管理、量本利分析等功能，支持多种成本核算模型；

c) 资产管理：对设备、后勤设备、固定资产等进行全生命周期管理，具备采购、入库、出库、领用、盘点、维修、报废、折旧、效益分析等功能，支持移动盘点及物联网技术应用；规范有线电视网络管理，具备监控、访问控制等功能；

d) 物资管理：建立临床试剂全流程管理，具备厂家管理、出入库、库存、有效期、报警等功能；实现高值耗材全流程追溯管理，支持供应商信息共享、采购、审批、登记、核销等功能；规范低值耗材及办公用品管理，具备请领、出入库、盘点、预警、审批等功能，支持多种识别方式及终端设备。

6.7 后勤管理

具体内容和要求应包括：

a) 楼宇智能管理：实现智能照明、环境温湿度、智能热水、智能电能、智能门禁等控制管理，具备自定义策略、远程控制、监测报警等功能，支持多种控制方式及覆盖多区域；

b) 辅助管理：开展科室洁净度管理，具备人员出入、智能发衣柜、更衣柜管理等功能，支持多种身份识别方式；对医疗废弃物进行全生命周期跟踪管理，具备分类、称重、标记、运输、回收、监管等功能，支持多种标识及定位方式；

c) 会议管理：实现视频会议管理，具备大型会议、远程会议、设备控制、会场配置等功能，支持多种音频处理及视频压缩传输方式；规范会议信息管理，具备预约、通知、签到、记录等功能，支持多种消息传递及会议记录方式。

6.8 人力资源管理

具体内容和要求应包括：

a) 战略规划：对人力资源供需进行规划，具备人力资源规划、岗位管理、人才招聘等功能，支持员工基本信息数据更新与同步共享；

b) 执行管理：开展人力资源日常管理，包括休假排班、员工培训、人员考勤、考核测评等功能，支持人力资源综合信息查询与展现；实现绩效与薪酬管理，具备绩效管理、薪酬核算功能，支持员工薪酬自动化算法模型；开展人事档案管理，涵盖人事档案、专业技术档案等管理功能。

7 管理要求

7.1 事件管理流程

7.1.1 分类管理

应对服务过程中的各类事件进行分类管理，并规定不同管理流程，至少应包括如下内容：

c) 识别需要管控的服务过程，并制定文件化的过程管理流程，至少应包括：
   1) 响应支持管理过程；
   2) 巡检管理过程；
   3) 需求管理过程；
   4) 事项管理过程。
d) 建立需求分类分级制度与流程，需求来源识别的流程与制度。建立事件优先度管理的制度与流程，优先处理影响就诊流程和患者隐私保护需求；
e) 与事件流程相关人员沟通并确认其管理职责。

7.1.2 接收管理

应制定信息技术服务需求管理制度与流程，至少应包括：

a) 不同种类事件应建立受理制度与流程，设立事件受理评审组织，应包括信息人员、业务操作与管理人员、医务管理人员、行政管理人员；
b) 设定专人负责事件请求的处理，应熟悉诊疗流程，熟悉诊疗相关法律，识别事件分类与定级；
c) 设置专门的沟通渠道作为与需方的联络方式，沟通渠道可以是电话、即时通信、网站、邮箱等多种方式。

7.1.3 分派管理

应采取有效手段和方法受理需方的运行维护服务请求，及时跟踪服务请求的处理进展，至少应包括：

a) 建立事件分派制度与流程，设立事件分派评审组织，应包括信息人员、业务操作与管理人员、医务管理人员、行政管理人员；
b) 建立事件的分派过程管理制度与流程，确保事件分派到责任人；
c) 建立事件分派过程跟踪和反馈等制度与流程，应有明确的通知记录，并对责任人的接收也有明确的记录，并反馈给事件提交人；
d) 建立事件接收的监督和考核制度与流程。

7.1.4 执行管理

a) 事件执行过程中，应及时对事件处理过程进行记录与反馈，对事件的影响变化做出及时记录，包括：对事件的处理要及时记录进展情况，同时应及时反馈给相关人员；
b) 事件的处理要有期限要求管理，至少应包括记录处理时间、结束时间；
c) 事件的处理过程变化应及时反馈给相关人员；
d) 及时对事件进行分析，可能引起重大医疗事故，严重泄密事件，规定上报时间限制；
e) 事件完成应有总结，包括自我评价、存在的问题，有完成审批流程。

7.1.5 评价管理

信息技术服务质量管理组织应制定专家与用户评价管理制度与流程，至少应包括：

a) 专家与用户评价流程；
b) 专家与用户评价的范围、内容、方式；
c) 专家与用户评价信息的采集、汇总、分析要求；
d) 专家与用户负面评价的核实、评估、处置、反馈、跟踪验证要求；

e) 专家与用户评价记录的保存要求。

7.1.6 评审管理

信息技术服务质量管理组织应制定服务评审与改进管理制度与流程，至少应包括：

a) 服务评审的范围、内容、频度、方式；
b) 服务过程的评审要求；
c) 对供应商服务评审的要求；
d) 服务改进需求识别；
e) 服务改进流程；
f) 服务改进跟踪验证要求。

7.1.7 日志与记录

事件管理流程中，应完善各个管理环节的日志与记录，便于后期评审与追溯，日志与记录至少包含以下内容：

a) 任务规划完成目标及定性、定量的衡量标准；
b) 完成事件规划和实际使用的技术、人员与资源；
c) 完成事件应遵循的流程与操作规范；
d) 评价日志，应包括多维度的；
e) 审计日志，应包括存在的问题与改进意见。

7.2 人员管理

7.2.1 科室应明确系统管理负责人，负责统筹系统建设与管理工作，协调解决系统建设和运行中的重大问题。

7.2.2 配备专职或兼职运维人员，运维人员应具备相应的技术能力，熟悉系统架构、功能和运维流程，能够熟练处理系统故障和日常运维工作，定期参加技术培训，提升专业能力。

7.2.3 系统用户应进行岗前培训，熟悉系统操作流程、使用规范和安全注意事项，考核合格后方可使用系统；定期开展用户培训，更新系统操作知识和安全意识。

7.2.4 建立人员岗位职责制度，明确系统管理负责人、运维人员、系统用户的岗位职责，落实岗位责任，做到分工明确、责任到人。

7.2.5 系统用户离职、调岗时，应及时注销或调整其系统账号权限，收回相关操作凭证，做好工作交接，防止数据泄露和误操作。

7.2.6 运维人员和系统用户应签订安全保密协议，明确保密责任，严禁泄露系统信息、用户信息和业务数据。

7.3 档案管理

应符合GB/T 18894的规定。

7.4 监控管理

7.4.1 应制定信息系统监控管理要求，至少应包括如下内容：

a) 监控范围与监控对象界定；
b) 监控参数设置及定期优化；
c) 定义告警信息的构成，至少应包括：
   1) 告警的系统；

2） 涉及的业务；
3） 影响的系统服务。
d） 制定监控告警处理制度与流程；
e） 定义告警信息的通知方式；
f） 定义监控日志及告警信息的保存期限；
g） 定义定期评价监控结果和告警处理结果的要求；
h） 定义定期评价及改进监控管理的要求。

7.4.2 应制定信息系统日常巡检管理制度与流程，至少应包括：
a） 巡检管理范围；
b） 巡检执行方式；
c） 巡检频率；
d） 巡检记录要求；
e） 巡检记录保存要求；
f） 巡检工作复核要求；
g） 巡检作业手册管理要求。

7.5 应急响应管理

7.5.1 应制定应急响应方案及其验证管理制度与流程，应急方案应以患者就诊流程、诊疗与运营活动正常开展为目标，至少应包括：
a） 明确应急方案执行响应后的目标和效果；
b） 应急与演练方案的范围、方法、频度；
c） 建立独立的演练工作组，演练测试环境；
d） 应急与演练方案的评价、评审要求；
e） 应急与演练改进跟踪验证要求。

7.5.2 围绕诊断诊疗与运营流程，梳理出关键环节，并配备冗余设备，保障故障发生时能及时补充。根据不同级别系统，至少配备以下设备：
a） 关键系统快速恢复使用设备，包括网络线路与设备、服务器、存储等；
b） 关键软件与服务，如操作系统、服务端软件、数据库的快速恢复使用。

7.5.3 针对业务的连续性要求，应有相应的人员应急响应与调度制度，至少应包括以下内容：
a） 明确值班方式与响应要求；
b） 有专门的排班制度、排班负责人，提前一定周期完成排班工作；
c） 对于排班过程中的请假、调班等有明确的变更流程；
d） 明确值班服务项目内容，有超出服务能力的升级流程；
e） 定期检查与考核人员对事件定级能力，包括患者诊疗应急性识别、保密性识别；
f） 对到岗、响应处理等行为有监督工具，同时定期检查与考核。

8 安全与运行维护保障

8.1 安全要求

8.1.1 应符合 GB/T 22080 和 GB/T 20269 的规定。
8.1.2 网络安全等级保护应不低于 GB/T 22240-2020 中第二级的规定。
8.1.3 应制定与执行信息安全管理制度和规范，以及相关的操作规程。

8.1.4　应设立信息安全管理机构并明确相关职责。

8.1.5　应制定与执行应急预案，并定期进行不同级别的演练。

8.1.6　涉及重要数据与信息安全的岗位，应与相关工作人员签订保密协议。

8.1.7　用于对实体和其所呈现身份之间绑定关系进行确认过程的专用设备。应支持口令认证、证书认证、智能卡认证、短信认证、第三方系统联动等身份鉴别方式。

8.1.8　数据中心服务器操作系统和数据库管理系统提供鉴别机制，保证用户身份安全可信，支持用户标识和用户鉴别。应支持受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

8.1.9　应制定信息安全区域划分管理制度与流程，至少应包括：

a)　可根据数据安全等级和应急等级、网络访问方式与风险程度划分不同的网络区域；

b)　信息安全区域访问控制准则与流程；

c)　应制定信息安全区域访问记录管理要求，涵盖患者诊疗记录、科室运营信息。

8.1.10　应制定信息安全管理制度与流程，至少应包括：

a)　信息安全管理范围；

b)　明确数据资产的安全管理要求，包括主体部门、管理制度、使用流程、数据授权管理；

c)　明确设施安全保护管理要求，包括主体部门、管理制度、作业规范管理；

d)　提供完善的患者信息脱敏制度，应有隐私保护、知识保护等措施；

e)　制定不同信息访问的授权部门；

f)　重点信息系统信息安全保障要求。

8.2　运行维护要求

8.2.1　运行管理

8.2.1.1　运维工作应符合 GB/T 28827.1 的规定，建立日常运维台账，记录系统运行状态、故障情况、处理过程、维护内容等信息，实现运维工作可追溯。制定与执行完善的管理制度和运维计划，进行不间断运行维护管理。

8.2.1.2　系统运行中发生故障或事故时，应严格按照相关处理流程处置。

8.2.1.3　对任何事故、故障及检测发现的安全点或漏洞，应做好相关情况记录，并由专人保管，定期进行分析。

8.2.1.4　建立操作人员维护活动日志并定期进行独立检查，确保日志内容完整性，发现故障时应做好记录并采取有效地纠正措施。

8.2.1.5　制定与执行网络、服务器、应用系统、数据库的访问控制制度，明确与合理设置用户的访问权限，对特权用户需制定策略审核，关键设备应选择高质量的口令，并经常更新。

8.2.1.6　对不同类型的第三方访问，如物理访问（办公室、计算机机房、档案室等）、逻辑访问（网络、服务器、数据库等）应给予必要访问控制，并进行风险评定，制定第三方对系统的访问制度。

8.2.1.7　机房及系统应实施分级权限管理，不同级别应设置不同的权限，相关工作人员按相应权限进出机房。

8.2.1.8　系统的全部或局部发生变更时，应得到批准并做好记录。对可能影响整个系统暂时无法工作、存在一定风险或不确定因素的重要变更，应严格按照变更控制流程操作，并在进行有效测试后实施。

8.2.1.9　建立与执行应用系统开发文档和源代码控制制度，对最新、最完整的源代码进行备份，并做好访问控制以保证其机密性。

8.2.1.10　具备日志记录、用户重要操作日志记录、日志查询、日志保护、日志备份、日志分析模型、日志审计报告等功能。

8.2.1.11　支持用户名称、操作日期和时间、操作类型、是否成功、合规审计等审计内容。
8.2.1.12　对重要业务应用应能进行应用恢复。

8.2.2　设备管理

8.2.2.1　建立完整的设备运行日志、操作记录，妥善保存与安全有关的资料，定期检查安全保障设备，确保其处于正常工作状态。
8.2.2.2　操作人员不得擅自增减硬件设备，发生硬件故障时应及时与管理员联系，由管理员进行维护，
8.2.2.3　制定与执行重要信息处理设施（如小型机、数据库、业务系统等）的操作规程。
8.2.2.4　建立与执行关键设备日志的定期审核制度，发现异常应追究其来源并做好记录，发现连续性错误警报或攻击事故，应按事故上报与处理流程处置。

8.2.3　数据库管理

8.2.3.1　制定与执行完善的数据备份方案，对所有业务数据进行定期备份，备份介质应由专人管理。
8.2.3.2　信息系统的灾难恢复与数据备份应符合 GB/T 20988 和 GB/T 36092 的规定。
8.2.3.3　数据库应适时进行更新，并具有详细的日志记录。
8.2.3.4　应制定信息系统与业务数据的备份与恢复管理流程，至少应包括：

a)　备份管理范围，应包括数据、操作系统、运行配置信息等；
b)　备份方式、备份频率；
c)　备份媒体定期测试要求；
d)　备份媒体、备份质量管理；
e)　定期进行系统恢复演练。

8.2.4　第三方服务管理

8.2.4.1　选择第三方时，应事先按 GB/T 24405.1 的规定评估第三方服务可能带来的风险并制定相应的控制措施。在签署合同时，应明确信息安全和保密要求、服务定义以及服务交付标准。
8.2.4.2　对第三方服务人员进行管理，根据第三方人员的岗位性质和重要程度，制定相应的物理访问和逻辑访问控制策略并实施。对涉及重要岗位和信息的第三方人员可与其单独签订保密协议。
8.2.4.3　对第三方服务项目进行管理，包括需求控制、进度控制、质量控制、审核验收、总结等，对于任何与合同不符合的变更应留下变更记录。