



# 中华人民共和国国家标准

GB/T 28827.8—2022

---

## 信息技术服务 运行维护 第 8 部分：医院信息管理系统管理要求

Information technology service—Operations and maintenance—  
Part 8: Hospital information system management requirements

2022-10-12 发布

2023-05-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 事件管理流程 .....	2
4.1 概述 .....	2
4.2 分类管理 .....	2
4.3 接收管理 .....	2
4.4 分派管理 .....	2
4.5 执行管理 .....	2
4.6 评价管理 .....	3
4.7 评审管理 .....	3
4.8 日志与记录 .....	3
5 服务规划 .....	3
5.1 业务影响度定级 .....	3
5.2 数据安全性定级 .....	4
5.3 组织与人员 .....	4
5.4 资源保障 .....	4
5.5 目录与质量 .....	5
6 供应商服务管理 .....	5
6.1 外包服务管理 .....	5
6.2 服务安全要求 .....	5
6.3 评估与验收 .....	5
7 沟通与协同管理 .....	6
7.1 概述 .....	6
7.2 协同管理 .....	6
7.3 沟通管理 .....	6
8 配置与监控管理 .....	6
8.1 配置管理 .....	6
8.2 监控管理 .....	7
8.3 日常巡检管理 .....	7
8.4 备份与恢复管理 .....	7

9 应急响应管理 .....	7
9.1 应急方案管理 .....	7
9.2 备用与保障 .....	8
9.3 应急人员管理 .....	8
10 安全运维管理 .....	8
10.1 网络安全区域划分 .....	8
10.2 信息安全管理 .....	8
参考文献 .....	9

## 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。

本文件为 GB/T 28827《信息技术服务 运行维护》的第8部分。GB/T 28827 已发布以下7个部分：

- 第1部分：通用要求；
- 第2部分：交付规范；
- 第3部分：应急响应规范；
- 第4部分：数据中心服务要求；
- 第6部分：应用系统服务要求；
- 第7部分：成本度量规范；
- 第8部分：医院信息系统管理要求。

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。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：安徽医科大学第一附属医院、合肥工业大学、卫宁健康科技集团股份有限公司、安徽省卫生健康委员会、解放军总医院、复旦大学附属华山医院、西安交通大学医学院第一附属医院、安徽中医药大学第一附属医院、中国科学技术大学附属第一医院、江苏省人民医院、云南省肿瘤医院、福建省立医院、复旦大学附属肿瘤医院、中国人民解放军空军军医大学第一附属医院、陆军军医大学第一附属医院(西南医院)、厦门大学附属翔安医院、芜湖市医院管理中心、江苏亚寰软件股份有限公司、广州赛宝认证中心服务有限公司、神州数码信息服务股份有限公司、上海溪盎科技有限公司北京分公司、北京赛迪认证中心有限公司、北京中科金财科技股份有限公司、金蝶医疗软件科技有限公司、南京海泰医疗信息系统有限公司、神州数码系统集成服务有限公司、四川久远银海软件股份有限公司、安徽省水恒科技有限公司、上海安翼保信息技术服务有限公司。

本文件主要起草人：周典、杨善林、徐红兵、陶敏、赵大平、邵东华、刘云、刘小茵、丁帅、刘敏超、黄虹、张琼瑶、王奕、陈韧、卫荣、路健、李振叶、蒋昆、汪鹏、刘春、徐冬、张文雅、蔡雨蒙、张勇、王飞、顾东晓、范春、田刚、陈艳、陈亚、潘伟强、郭刚、张翼、沈伟、黄健、白璐、马烈、张旭、凌志、彭戈、孙佩、张娜、黄健、张洁、张树梅、曹卫星。

## 引 言

GB/T 28827《信息技术服务 运行维护》分为 8 个部分：

- 第 1 部分：通用要求。目的在于提出信息系统运行维护的基本组成要素，以及提供运行维护服务的各类组织在这些要素方面应具备的条件和能力，指导供方改进和提升其运行维护服务能力，并为需方提供选择和评价供方的依据。
- 第 2 部分：交付规范。目的在于为运行维护服务交付过程中涉及的交付管理、交付内容、交付方式、交付成果提供指导，可作为需方选择供方的依据，也可作为供方改进运行维护服务交付能力的指南。
- 第 3 部分：应急响应规范。目的在于提出应急响应的基本过程，以及过程管理要求，提升组织的应急响应能力，提前发现隐患，及时解决问题，降低应急事件可能带来的不良影响。
- 第 4 部分：数据中心服务要求。目的在于规定数据中心运维服务的对象、服务策略、交付内容等要求，规范数据中心运维服务提供方行为，改进服务能力，提高数据中心运维服务的工作效率。
- 第 5 部分：桌面及外围设备规范。目的在于规范桌面及外围设备运行维护服务提供方服务行为，提高服务规范性和便利性，降低安全风险和运营成本。
- 第 6 部分：应用系统服务要求。目的在于提出应用系统运行维护服务模型，规定运行维护对应用系统设计、交付、运行、终止和评价的要求。
- 第 7 部分：成本度量规范。目的在于规定运维成本度量的方法及过程，包括运维成本的构成及运维成本度量过程。
- 第 8 部分：医院信息系统管理要求。目的在于指导医院信息系统服务组织改进和提升其信息系统管理能力。

本文件承接 GB/T 28827.1《信息技术服务 运行维护 第 1 部分：通用要求》的管理要求，结合医院信息系统管理需求，从信息系统服务规划、日常事务处理、供应商管理、沟通协同、信息安全等方面给出医院信息系统服务的基础组成部分，以及提供医院信息系统服务的各类组织在这些方面应具备的条件和能力。

本文件细化事件管理为多个环节，对配置管理等部分进行扩延、细化，同时根据行业特点重点强调了供应商管理、应急响应等方面的管理要求。对于 GB/T 28827 中已经提过的管理规范和要求，本文件不再重复。

本文件的第 4 章将事件管理过程细分为分类管理、接收管理、分派管理、执行管理、评价管理、评审管理，并规定了 6 个细分过程应该产生的日志与记录的内容。

本文件的第 5 章规定了需要医院领导、信息部门、业务部门共同参与的工作内容，确定信息化相关部门规定共同目标、内容、要求，确定职责与保障。

本文件的第 6 章规定了供应商服务作为信息部门对外提供服务的组成部分，信息部门对其做好管控的相关要求。

本文件的第 7 章明确了沟通与协同作为运维活动管理的重要组成部分，贯穿事件处理的各个环节，是形成部分记录的主要方法，该章规定了沟通与协同的相关管理要求。

本文件的第 8 章对配置管理细化与扩延，细化扩延了监控的运维要求。

本文件的第 9 章规定了医院应急管理需要的三个要素，应急预案、备用与保障、应急人员的相关管理内容与要求。

本文件的第 10 章规定了网络安全管理中医院应重点强调的相关管理内容与要求。

# 信息技术服务 运行维护

## 第8部分：医院信息系统管理要求

### 1 范围

本文件规定了医院自用信息系统在规划、建设、运行维护、持续改进、安全保障过程中的管理要求。本文件适用于医院临床、管理、后勤、行政等各方面的信息技术服务需求。

### 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 28827.1 信息技术服务 运行维护 第1部分：通用要求

GB/T 28827.2—2012 信息技术服务 运行维护 第2部分：交付规范

GB/T 28827.3—2012 信息技术服务 运行维护 第3部分：应急响应规范

GB/T 29264—2012 信息技术服务 分类与代码

SJ/T 11693.1—2017 信息技术服务 服务管理 第1部分：通用要求

### 3 术语和定义

GB/T 28827.1、GB/T 28827.2—2012、GB/T 28827.3—2012、GB/T 29264—2012、SJ/T 11693.1—2017 界定的以及下列术语和定义适用于本文件。

#### 3.1

**外包服务** **service outsourcing**

外部信息技术服务供应商为医院提供特定信息技术服务的过程。

#### 3.2

**医院信息系统** **hospital information system; HIS**

医院的管理、医疗等行为所依赖的计算机软硬件技术和网络通信等现代化技术与对象。

#### 3.3

**客观诊疗记录** **subjective medical record; SMR**

对患者的病史、症状、体征以及进行的各项检查、检验和治疗护理过程的客观记录。

#### 3.4

**主观诊疗记录** **objective medical record; OMR**

医务人员根据患者的病史、症状、体征、并结合各项检查、化验做出的诊断和治疗方案，并根据患者在治疗过程中病情变化调整治疗方案。

## 4 事件管理流程

### 4.1 概述

对事件进行分类,并对执行过程、执行结果、评价评审进行管理,确保事件过程的质量与效率持续改进。

### 4.2 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。

- a) 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。
- b) 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。
- c) 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。
- d) 与事件流程相关人员沟通并确认其管理职责。

### 4.3 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,应熟悉医院诊疗流程,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。

### 4.4 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。

### 4.5 执行管理

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:

- a) 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。

#### 4.6 评价管理

医院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。

#### 4.7 评审管理

医院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。

#### 4.8 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。

### 5 服务规划

#### 5.1 业务影响度定级

应根据信息系统对医院正常运营影响情况的重要性、紧急性等进行分级。医院信息系统分类分级应包括以下四级系统。

- a) 一级系统  
影响患者生命安全的系统:指涉及患者抢救,一旦出现故障会影响患者生命安全保障的信息系统。
- b) 二级系统  
影响医护诊疗流程的系统:指涉及医患诊疗业务,一旦出现故障会严重影响医患诊疗业务流程正常运转的信息系统。
- c) 三级系统  
影响医院运行流程的系统:指涉及医院诊疗活动,一旦出现故障会影响医院日常运行流程,但可以通过应急措施保障患者就医需求不受影响的信息系统。



d) 四级系统

影响医院管理流程的系统：指保障医院正常运营，不涉及医院诊疗活动的信息系统。

应针对不同分级的信息系统区分制定管理要求和目标，包括资源保障、组织与人员要求、服务过程要求、供应商要求等。

## 5.2 数据安全性定级

应根据信息系统对医院信息数据的安全性进行分级，涵盖患者隐私保护与医生知识产权保护，系统应支持设定维护权限，制定与外部交互时的管理规范与流程。定级应至少包括以下级别。

a) 一级系统

涉及医院核心运营数据，同时包括识别患者的信息、患者客观诊疗记录、医生主观诊疗记录。

b) 二级系统

涉及医院一般运营数据，同时包括识别患者的信息、患者客观诊疗记录。

c) 三级系统

同时包含识别患者信息，诊疗活动数据或客观诊疗信息。

## 5.3 组织与人员

医院应根据信息化深入程度、规模大小、稳定性要求、应急性要求，配备信息技术服务管理组织、信息技术服务执行人员与信息技术服务质量管理组织，以满足医院当前和未来的信息技术服务需求。

a) 信息技术服务管理组织

医院应设置专职的信息技术服务管理组织，负责医院信息服务的管理工作，最高机构为医院信息化委员会，涵盖医院领导、医疗护理管理机构主管、行政管理机构主管、外聘专家，其职责至少应包括：

- 1) 医院信息系统建设、运维的整体规划、设计；
- 2) 医院信息系统日常维护流程与制度的制定、执行监督、评估；
- 3) 对信息技术服务供应商评估、选择；
- 4) 对信息服务需求审议、评估、选择；
- 5) 对信息技术服务工作人员评价。

注：医院信息技术服务管理组织可以包括信息技术服务供应商的组织与成员。

b) 信息技术服务执行人员

医院应设立信息技术服务岗位，并配备专职工作人员，至少应包括：

- 1) 信息系统项目执行的规划及管理人员；
- 2) 信息系统服务需求分析人员；
- 3) 信息技术服务供应商管理人员；
- 4) 信息安全管理人员。

医院信息技术服务管理人员包含医院专职人员与信息技术服务供应商人员。

c) 质量管理组织

医院应设置质量管理组织，负责建立、实施、评价、改进医院信息技术服务质量管理制度与流程，针对医院的各项信息技术服务进行质量管控，确保高效高质量的服务交付。

## 5.4 资源保障

应对信息技术服务所需的资源，包括外部服务供应商所需的资源进行规划，并制定资源保障管理制度与流程，至少应包括如下内容。

- a) 建立资源的持续性投入的制度,包括人员、资金、工具、技术(包括安全技术)等,包含外包服务商提供运维的资源,以达到规划运营目标。应通过各类方式,制定长期的规划、培养机制,使得技术、人员、工具等达到管理需求。

注:人员包括外包运维人员,技术可以是购买或租用的服务、工具。

- b) 医院管理层应采取措施,保障医院信息系统管理所需资源的有效获取,至少应包括:
  - 1) 信息技术服务工具,包括硬件工具、过程管理软件工具、监控软件工具等;
  - 2) 场地:服务人员工位、机房、库房;
  - 3) 网络通信、计算资源、存储资源。

## 5.5 目录与质量

应建立并维护提供给医院各部门、医院服务对象的服务目录并明确服务质量评价方法,应通过医院信息管理组织审批,符合管理法规,符合患者隐私保护相关法规,并保存执行日志,确保服务质量检查的有效开展,发现服务流程中的问题,并提出改进意见。至少应包括:

- a) 服务对象与范围;
- b) 服务内容与定性、定量评价要求;
- c) 服务定级要求;
- d) 服务评价与评审规范。

## 6 供应商服务管理

### 6.1 外包服务管理

应制定外包服务管理制度与流程,至少应包括:

- a) 外包服务范围与内容;
- b) 应明确医院与供应商的职责与权力;
- c) 应明确服务范围、服务期限、服务人员能力要求;
- d) 外包服务人员的驻场要求,人员更换调整流程;
- e) 文件化的服务级别管理要求。

### 6.2 服务安全要求

应制定服务安全管理制度与流程,至少应包括:

- a) 应与服务供应商签订安全与保密协议,应涵盖患者隐私保护条例;
- b) 外部人员应熟悉医疗就诊服务相关法律,熟悉患者隐私保护要求,签订承诺书;
- c) 应制定外部服务人员的医院信息系统相关权限分配与回收管理流程。

### 6.3 评估与验收

医院对信息化的合约中,要明确验收、运行维护要求,至少应包含:

- a) 供应商选择、评价、考核管理要求;
- b) 外包人员的选择、评价、考核管理要求;
- c) 外包服务的服务级别管理要求;
- d) 应制定安装部署的定量、定性等验收指标;
- e) 应制定运行保障的验收的定量、定性要求;

- f) 外包服务商的绩效考核要求与合约中止条件约定。

## 7 沟通与协同管理

### 7.1 概述

建立与医院内部的临床、医技、行政、后勤部门和人员,与患者之间的信息服务平台,包含服务的宣传与介绍,服务过程中的协同、服务完成后的评价系统。

### 7.2 协同管理

应制定宣传、通知、沟通、协同管理制度与流程,至少应包括下列内容。

- a) 建立用于沟通交流的通讯录,同时具备隐私防护功能。
- b) 有多种主动推送渠道,包括电话、短信、即时通信等,建立信息服务专用门户。
- c) 建立不同级别的通知要求;建立通知反馈要求、不同级别通知要求应采用的沟通渠道与反馈要求。确保及时宣传信息系统变更、紧急情况处理等通知能及时、准确地被获得。
- d) 建立与医院各科室及外部供应商的协同管理制度与流程。
- e) 定期评价协同管理制度与流程。

### 7.3 沟通管理

沟通管理包括如下内容:

- a) 定期对自身工作内容、特点、服务目录等进行介绍和宣传;
- b) 有完善的通知体系,能够实现通知方式升级与职务升级,并能确认通知结果;
- c) 建立多种信息化网上调研方法和手段,快速了解各方的需求和想法;
- d) 建立与医院各科室及外部供应商的沟通管理制度与流程;
- e) 定期评价宣传沟通管理制度与流程。

## 8 配置与监控管理

### 8.1 配置管理

应对医院信息系统制定配置管理制度与流程并实施,至少应包括:

- a) 配置项分类分级原则;
- b) 配置管理对象范围及其完成率要求;
- c) 配置项的基本信息与定级信息;
- d) 按业务识别并管理配置项之间的关联关系;
- e) 建立配置管理与变更管理的关联关系;
- f) 定期进行配置审计,检查配置管理准确性、完整性;
- g) 关键配置项的安全管理措施、监控参数、本身攻击防范措施、应急方案;
- h) 配置项的业务关系、服务合约、应急操作、恢复、备份、安全防范、安装流程、常见故障处理等要求;
- i) 将设备基本信息、设备配置文件、系统软件安装包、系统备份文件及媒体纳入配置管理;
- j) 确保业务系统运行的所有运维对象,统一管理网络配置与数据传输接口需求,应包括诊疗设备的网络配置、数据接口配置;

k) 使用信息化工具进行配置管理。

## 8.2 监控管理

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。

## 8.3 日常巡检管理

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。

## 8.4 备份与恢复管理

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) 符合备份恢复的 RTO[恢复时间目标(Recovery Time Objective)]、RPO[恢复点目标(Recovery Point Objective)]要求;
- e) 备份媒体、备份质量管理;
- f) 定期进行系统恢复演练。

## 9 应急响应管理

### 9.1 应急方案管理

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、医院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。

## 9.2 备用与保障

围绕针对医院诊疗与运营流程，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) 终端设备保障，包括收款、药房、诊间等应配置备用终端，并拟定更换方案；
- b) 终端电源保障，手术室、ICU[重症加强护理病房(Intensive Care Unit)]等涉及生命安全的软件系统设备，应配备UPS[不间断电源(Uninterruptible Power Supply)]；
- c) 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；
- d) 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。

## 9.3 应急人员管理

针对医院业务连续性要求，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。

## 10 安全运维管理

### 10.1 网络安全区域划分

应制定信息安全区域划分管理制度与流程，至少应包括：

- a) 可根据医院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、医院运营信息。

### 10.2 信息安全管理

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) 明确医用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，如医务部门、科研部门、网络安全委员会等；
- f) 重点信息系统信息安全保障要求。

参 考 文 献

- [1] Information Technology Infrastructure Library(ITIL)Version 3
-