

T/EJCCCSE

团 体 标 准

T/EJCCCSE XXXX-XXXX

数字中医诊疗平台

Digital traditional chinese medicine (TCM) diagnosis and treatment platform

(征求意见稿)

20XX-XX-XX 发布

20XX-XX-XX 实施

中国商业股份制企业经济联合会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 总体要求 2

6 平台架构 2

7 性能要求 3

8 功能要求 4

9 安全要求 14

10 系统运行质量评价 17

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。

本文件由深圳问止中医健康科技有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：深圳问止中医健康科技有限公司。

本文件主要起草人：×××

数字中医诊疗平台

1 范围

本文件规定了数字中医诊疗平台的总体要求、平台架构以及功能、接口和安全等方面的技术要求。

本文件适用于开展中医互联网诊疗业务的实体医疗机构，也适用于作为实体医疗机构第二名称的中医互联网医院，以及依托实体医疗机构独立设置的中医互联网医院。

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 18336.2-2024 网络安全技术 信息技术安全评估准则 第2部分：安全功能组件

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

GB/T 25000.23-2019 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第23部分：系统与软件产品质量测量

GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GM/T 0028-2014 密码模块安全技术要求

XJ-D01《医疗保障信息平台电子凭证技术规范》

《中医医院信息与数字化建设规范（2024版）》

《互联网医院管理办法（试行）》

《中医病历书写基本规范》

《医疗机构病历管理规定》

《电子病历应用管理规范（试行）》

中华人民共和国卫生部令第53号《处方管理办法》

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网医院 internet hospital

经相关卫生行政部门审批，准许颁发或变更《医疗机构执业许可证》，提供互联网诊疗服务的医疗机构，包括作为实体医疗机构第二名称的互联网医院，以及依托实体医疗机构独立设置的互联网医院。

3.2

数字中医诊疗平台 digital traditional chinese medicine (TCM) diagnosis and treatment platform

互联网医院向患者提供中医诊疗及相关服务的系统平台。

3.3

电子处方 electronic prescription

采用信息技术，在诊疗活动中填写药物治疗信息，开具处方，并通过网络传输至药房，经药学专业技术人员审核、调配、核对，并作为药房或药店发药和医疗用药的医疗电子文书。

3.4

区块链 blockchain

一种分布式共享数据库账本，存储于其中的数据或信息具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。

4 缩略语

APP：应用程序（Application）

EMR：电子病历系统（Electronic Medical Record）

HIS：医院信息系统（Hospital Information System）

OCR：光学字符识别（Optical Character Recognition）

UTM：统一威胁管理（Unified Threat Management）

5 总体要求

5.1 数字中医诊疗平台应与医院信息系统、医保系统、药品物流系统、第三方支付系统及其他系统对接，整合各方服务能力，为面向居民的互联网管理和服务提供支撑。

5.2 应面向患者、医生、医院管理者提供针对性的服务功能；提供便捷的预约挂号、在线支付服务。

5.3 患者端应用宜采用多种入口，如微信公众号、小程序、支付宝、APP 等，构建医院线上互联网服务入口；医生端应用应包括移动端、PC 端等入口，支撑医生移动化办公；管理端应用应对互联网医院的业务质控管理、流程规范管理、资源分配以及数据分析等内容进行有效管控。

5.4 安全保障体系综合考虑系统可接受的风险程度，建立实现安全目标的安全模型和信息安全保护体系，达到风险、安全与投资的最佳平衡。

5.5 应同当地医疗服务与执业监管平台进行对接，满足当地互联网诊疗服务监管要求；数字中医诊疗平台应遵循国家标准和行业标准规范体系，严格遵守既定的技术路线，主动规避建设过程中的风险。

5.6 运营服务体系用于保障互联网医院的持续稳定运营，在运营过程中与各相关部门有效衔接，并对运营结果进行分析和监管。

6 平台架构

6.1 建设要求

6.1.1 平台建设应符合《中医医院信息与数字化建设规范（2024 版）》的规定。

- 6.1.2 根据国家卫健委明确规定，建设数字中医诊疗系统平台必须以实体的医疗机构为依托，政策要求数字中医诊疗系统平台建设必须是线上互联网云平台和线下实体医院信息系统相融合的平台架构，平台部署应是线上线下一体化的混合部署模式。
- 6.1.3 应按照 GB/T 18336.2-2024 等技术标准和安全要求进行建设，若在运行过程中被发现存在安全问题的应暂停使用直至整改完成。

6.2 平台架构

- 6.2.1 平台的开发应基于云计算、大数据、人工智能、互联网、物联网等技术。
- 6.2.2 平台宜采用 B/S 架构，功能实现应保障其应用可集成于 Web 环境，平台架构如图 1 所示。

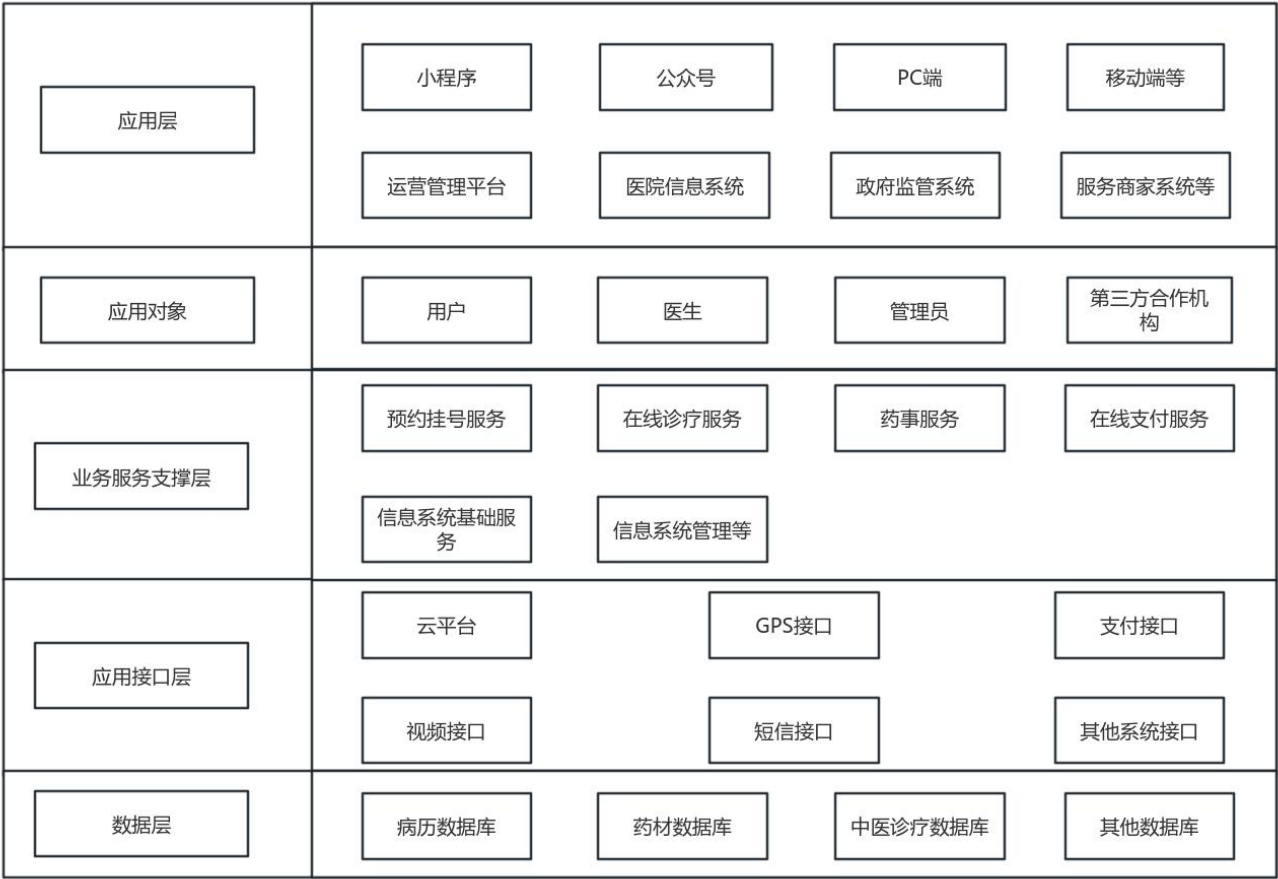


图 1 数字中医诊疗平台系统架构

7 性能要求

7.1 功能性

系统的功能性应符合 GB/T 25000.51-2016 中的规定。

7.2 可靠性

系统的可靠性应符合 GB/T 25000.51-2016 中的规定。

7.3 易用性

系统的易用性应符合 GB/T 25000.51-2016 中的规定。

7.4 效率

系统效率应符合 GB/T 25000.51-2016 中的规定。

7.5 维护性

系统的维护性应符合 GB/T 25000.51-2016 中的规定。

7.6 可移植性

系统的可移植性应符合 GB/T 25000.51-2016 中的规定。

7.7 使用质量

系统的使用质量应符合软件操作手册的规定。

8 功能要求

8.1 预约挂号服务

8.1.1 资源管理

8.1.1.1 在平台患者端的显著位置提供在线复诊的服务范围、准入条件公示，同时提供面向用户的预约挂号号源查询功能，应支持查询医院可挂号科室、科室医生、医生号源。

8.1.1.2 应支持设置出诊时间安排，排班后医生专门针对复诊患者进行线上复诊。

8.1.1.3 应支持多维度展示科室、医生信息，方便患者多维度了解医院。

8.1.1.4 在号源管理基础上按照资源的属性为用户提供查询功能，根据在线复诊预约或挂号的规则、价格、时间、是否有排班等信息进行查询。

8.1.1.5 可支持医生临时调班，并给患者推送通知提醒，医生可追加临时预约号源，供给有需要的患者进行在线预约。

8.1.2 复诊预判

8.1.2.1 中医互联网医院应严格执行对复诊条件的判断，需要对接医院 HIS、EMR 等系统进行自动判断，具体要求包括：

- a) 用户所提供复诊判断依据中指向的患者与就诊的患者必须为同一人；
- b) 在需要预约挂号的实体医疗机构线下就诊过，且为相同疾病诊断的患者作为复诊患者，具体时间范围应参照医院管理办法和国家政策；
- c) 开具处方时遇到小于 6 岁的儿童应有系统提示，支持医师对陪伴患儿的监护人和相关专业医师的身份加以辨识。

8.1.2.2 用于判断复诊的依据必须以电子化的方式留存，并明确与患者当次就诊的关联方式，以备查验。用于复诊判断的数据来源包括：

- a) 患者自行提供的历史病历（相关图文信息）；
- b) 医疗机构已有的电子病历；
- c) 通过各省市区级卫生平台或医联体调取的患者健康档案。

8.1.2.3 可根据诊断为通过复诊判断的患者设置当次预约、挂号的疾病标签，当且仅当用户所选号源的疾病属性与患者疾病标签一致时，才可为患者开放预约挂号功能。

8.1.2.4 可将患者历史病历（图文信息）和实体医疗机构已有链上该患者电子病历进行对比，并将调取患者健康档案行为动作过程数据通过应用区块链进行记录，如后续出现医疗纠纷时可作为司法取证依据。

8.1.3 在线预约

8.1.3.1 患者通过复诊判断之后，即可在线操作进行复诊预约。在线预约操作后应向居民发送通知或提醒，防止误操作。

8.1.3.2 在线预约成功后，根据患者信息、所预约资源信息生成预约订单，并以 APP 推送消息、微信或支付宝小程序推送消息或手机短信的方式报到。

8.1.3.3 医疗机构面向用户提供针对预约信息的查询与管理功能，用户可查看自己的预约信息，并在需要时对选定的未挂号就诊的订单进行取消。

8.1.3.4 医生端可帮助患者进行在线临时预约，方便老年患者在线就医。

8.1.3.5 有条件的医疗机构可将在线预约全流程数据记录到区块链上，数据由区块链上各个机构共享，方便对患者就诊记录进行追溯。

8.1.3.6 应支持通过复诊预判的患者进行在线挂号。在线挂号支付前，须对就诊患者本人的实名认证信息进行核对。在线挂号应以用户完成诊疗服务费支付为成功标志，并根据患者实名信息、所挂号资源信息生成挂号单。

8.1.3.7 挂号信息与对应医院智能信息系统应形成信息交互，以确保完成挂号后正常进入就诊等待序列。

8.1.3.8 系统应面向患者提供针对挂号信息的查询与管理功能，患者可查看自己的挂号信息，并在需要时对选定的尚未就诊的订单进行取消，取消后已支付的费用按照相关政策进行退回处理。

8.2 在线诊疗服务

8.2.1 提醒医生就诊

8.2.1.1 系统应为医生提供出诊提醒功能，当系统为医生分配订单后，应及时通知医生本人，通知的形式包括但不限于短信、APP 通知、网页通知、微信通知等。

8.2.1.2 医生登录系统后，可查看本人待接诊、接诊中、已完成的出诊列表。

8.2.1.3 医生可对挂号订单进行接诊操作，查看患者提交的病情信息、健康档案和相关图文信息等。

8.2.2 提醒患者就诊

当到达预约就诊时间时，系统应提醒患者进行线上就诊，通知的形式包括但不限于短信、APP 通知、网页通知、微信通知等。

8.2.3 在线复诊

8.2.3.1 应支持医生在接诊前预览患者病历，评估患者病情是否适合接受在线复诊，并做出在线接诊或中止复诊操作。

8.2.3.2 医生可通过图文、语音或者视频等在线交流的方式来了解就诊患者病情信息，图文、语音、视频交互记录应全程留痕、可追溯。

8.2.3.3 系统应提供中止线上复诊的功能，当医生在诊疗过程中发现患者不适宜接受在线诊疗服务的情况时，应中止复诊并如实记录中止原因及建议方案。

8.2.3.4 在诊疗服务过程中，应当有实时的消息提醒医患双方，提高医患交流的效率。

8.2.3.5 患者在实体医疗机构就诊，由接诊的医师通过数字中医互联网诊疗平台邀请其他医师进行会诊时，系统应支持会诊医师出具诊断意见并开具处方。

8.2.3.6 有条件的医疗机构，可支持医生为患者在线开具检验、检查、治疗等处方。

8.2.4 病历书写

系统应支持医生在线书写电子病历，电子病历基本内容应包括主诉、现病史、既往史等必要信息。系统应引导医生遵循《中医病历书写基本规范》《医疗机构病历管理规定》和《电子病历应用管理规范（试行）》的规定，为患者建立电子病历。

8.2.5 病历资料查询

8.2.5.1 数字中医诊疗平台应支持医生和患者在线查询检查检验结果和资料、诊断诊疗方案、处方和医嘱等病历资料。

8.2.5.2 数字中医诊疗平台应支持医生和患者下载检查检验结果和资料、诊断诊疗方案、处方和医嘱等病历资料。

8.2.6 在线处方

8.2.6.1 在线开方可包括续方、开方两种形式，出于用药安全考虑，系统应优先推荐医生针对患者既往明确诊断、用药安全的处方进行续方；在医疗机构能保障用药安全的前提下，可开展在线开方。

8.2.6.2 应引导医生遵守《处方管理办法》等相关规定，禁止医生在线开具麻醉药品、精神药品等特殊管理药品的处方。

8.2.6.3 医生在线诊断、提交处方时必须进行实名验证，获得电子签名及相应时间戳。

8.2.6.4 医生开方时，平台应支持查询医院药房、合作第三方药品供应商的药品库存信息，库存不足时，不支持开具电子处方。

8.2.6.5 医师、药师身份认证信息可应用区块链技术实现在多个医疗机构之间互认和共享，以区块链底层地址标识为基础，实现多码融合，即将多种医疗相关的标识信息在不改变原有系统业务流程的情况下，进行整合共享，方便应用扩展。

8.2.6.6 在医生提交处方进行实名验证时，可将电子签名及相应时间戳信息记录到区块链上作为存证数据多方保存。

8.3 药事服务

8.3.1 处方审核

8.3.1.1 应有专职药师在线进行处方审核工作，系统应具备在业务时间至少有1名药师签到功能。

8.3.1.2 医生电子签名完成后该处方提交至平台指定的药师进行在线审方，系统应引导药师遵守《处方管理办法》的有关规定进行审方。

8.3.1.3 药师审核合格的处方，应当在处方上附加电子签名与时间戳，才可生效。

8.3.1.4 系统可提供基于知识库的前置审方系统辅助药师进行审方，审方流程参照线下方式执行，审方提示有合理性问题但医生强制生效的处方需特别记录。

8.3.1.5 有条件的医疗机构可通过人脸识别等人体特征识别技术进行药师的身份识别认证。

8.3.2 合理用药

医生在开具在线处方时，系统可通过知识库对方药合理性进行自动判断，对不合理用药进行警示提醒，辅助医生进行开方，具体功能包括但不限于以下内容：

- a) 下达处方时能关联项目获得药物知识，如提供药物说明查询功能等；
- b) 处方下达时能获得的药品剂型、剂量或可供应药品提示；

- c) 具有针对患者诊断、适应人群、历史处方、过敏史等进行合理用药、配伍禁忌、给药途径等综合自动检查功能并给出提示；
- d) 对高危药品使用给予警示。

8.3.3 处方确认

8.3.3.1 完成审方的处方，系统应结合医保规则对其中自费、自付、共付的费用进行划分，生成在线的支付订单推送至患者端。

8.3.3.2 系统应提醒患者对药品清单、取药方式及配送地址进行确认，以确保药品订单正常配送。

8.3.3.3 处方订单经患者确认并支付之后，系统应提醒患者确认处方信息和用药的注意事项。

8.3.4 对接药品

8.3.4.1 系统应对接药品服务方（自有药房或第三方药品供应商），将支付完的处方信息推送给药品服务方，进行药品后续服务确保药品的准确配送。

8.3.4.2 有条件的医疗机构宜与配送公司对接，方便患者及互联网医院管理部门实时了解药品配送信息。

8.3.5 药品供应管理

8.3.5.1 平台应提供对申请入驻的药品库信息进行合规性审核管理功能。

8.3.5.2 应对合规性入驻中医互联网医院药房的药品 ID 进行重新编码以符合在线处方开具的监管需求。

8.3.5.3 平台应支持对药品库相关药品信息的日常管理维护，包括药品名称、剂型、规格、单位、包材、批准文号、生产企业以及是否属于重点监控的药品、禁用药品和药库的新增、位置等信息。

8.3.5.4 平台宜支持对第三方合作药店或生产商药品的认证审批功能和药品信息管理功能，包括药品名称、药品编码、药品简介等内容。

8.3.5.5 平台宜支持对入驻的合作药店、医药厂家、快递公司信息与药库的接口信息进行管理。

8.3.6 患者购药

8.3.6.1 完成审方后，系统应生成在线的支付订单推送至患者客户端，通过支付平台完成支付。

8.3.6.2 互联网医疗机构应提供一种或多种取药方式供患者选择，包括但不限于院内取药、配送到家（医院配送、药店配送）、药店取药。

8.3.6.3 系统应将配送地址、配送时间、药品清单等信息推送给患者进行确认，以确保支付的药品订单能正常配送。

8.3.6.4 有条件的医疗机构宜与药品物流公司对接，方便患者及互联网医院管理部门实时了解药品配送信息。

8.3.7 药品调剂

8.3.7.1 药品在完成收费后，应结合互联网医院药品管理的方式，将基于处方所形成的订单定向推送至指定药房进行药品调剂。

8.3.7.2 承接互联网医院在线电子处方调剂任务的实体医疗机构药房和第三方药品供应商的药师应对调剂的在线电子处方的用药适宜性进行审核。

8.3.8 药品配送

8.3.8.1 当患者选择配送作为取药方式，调剂好的药品由药品物流组织物流公司配送，配送形式采用配送上门等方式。

8.3.8.2 互联网医院宜与药品供应商、药品物流公司实现信息的互联互通，保证药品订单到配送订单之间信息的准确传递。

8.3.8.3 平台可提供针对药品配送完整环节的全流程管理，供卫生管理部门、药品配送机构和患者本人实时查询当前配送状态。

8.3.8.4 互联网医院宜提供对药品供应商和药品物流服务商公司的定期审核功能，以保证药品生产、储存和流通环节的安全和高效。

8.3.9 药品签收

8.3.9.1 药品配送信息应支持实时查询，以改善患者购药的用户体验。

8.3.9.2 药品的签收应以患者收到的提货码作为验证标识，实现药品配送到人，避免配送错误引起的医疗纠纷。

8.3.9.3 在完成配送后，应将配送签收信息反馈至互联网医院，形成针对药品服务的闭环。

8.3.9.4 互联网医院宜提供用药指导功能。在患者签收药品后，互联网医院宜关注患者用药情况，如药品信息浏览、加强用药依从性管理、提供用药不良反应的快速反馈通道、续方提醒等功能。

8.4 在线支付服务

8.4.1 在线支付

8.4.1.1 互联网医院应建设统一支付平台或将现有的在线支付平台融合进互联网医院的支付场景中，能够覆盖患者在互联网医院全流程中的所有支付环节，根据患者在互联网医院就诊过程中产生的不同类型账单，进行分别支付和统一对账管理。

8.4.1.2 患者在互联网医院就医过程中所产生的医疗费用账单通过支付宝、微信、银联等在线支付渠道进行实时付款，账单由医院智能信息系统汇总生成并推送到患者端，患者根据账单金额选择可用的支付渠道进行在线付款。

8.4.1.3 医院智能信息系统推送到患者端的账单长时间没有支付，系统应自动关闭该账单。自动关闭账单的等待时长由医院根据自身业务特性设定阈值，账单自动关闭后应向患者端推送相应提醒消息。

8.4.1.4 患者通过互联网医院就诊进行相关费用支付时，系统应自动推送缴费成功消息，消息包含费用概要信息和支付状态，用户通过消息入口可查询缴费明细；系统应在患者在线支付成功、退款成功、账单超时自动关闭等环节进行对应提醒消息的在线推送。

8.4.1.5 互联网医院应与当地医保对接为患者开通医保支付，结合医保规则对方中自费、自付、共付的费用进行划分。

8.4.1.6 支付平台宜支持多商户接入、多渠道支付、多方统一对账、多应用支持、多途径数据统计分析和导出。

8.4.1.7 互联网医院可在支付完成后为用户提供电子发票。

8.4.2 退费处理

8.4.2.1 平台应支持患者线上支付费用的退还操作，对于已经支付但是经双方确认取消的医疗服务按照患者支付途径原价退还。

8.4.2.2 在患者因故无法上线接受在线复诊医疗服务或院方医疗资源安排计划变更无法为患者提供在线复诊医疗服务时，系统应支持授权相关管理者进行患者在线复诊服务费用的退费操作安全要求。

8.4.2.3 用户完成电子处方支付后，在转交药品物流之前，经医院方沟通协调许可后，可以在线进行退费申请操作；在进入物流环节后如用户必须退费，则需要与医院、药品供应商及物流多方综合协调后进入特殊退费流程，协商过程需进行记录。

8.4.2.4 根据患者在线支付途径对于退款周期的不同要求，系统应在退费操作完成时推送消息提醒患者预计的退款到账周期。

8.4.2.5 对于接入在线医保结算的医疗机构，退还费用中医保支付部分可参照当地医保实行的在线医保结算退费流程进行退费操作。

8.4.2.6 对于开展线上预约检验检查业务的医疗机构，提供预约检验检查费用的在线退费功能。

8.4.3 财务对账

8.4.3.1 平台线上医疗服务开展过程中产生的账单与患者实际支付应逐一对应，并满足互联网医院财务管理部门的财务监管和对账操作。

8.4.3.2 平台应提供统一对账功能，为财务科室提供包含分类账单和汇总数据的对账工具，辅助财务管理人员方便快捷地完成财务对账工作。互联网医院的对账业务包括平台生成账单财务对账、平台生成账单财务对账、第三方药品供应链生成账单的财务对账。

8.4.3.3 按互联网医院的关账时间点汇总当日对账，对账单明细和支付订单进行逐一匹配核实，系统自动排列问题账单进行错账提醒，相应人员进行错账处理实现账款平衡。

8.4.3.4 对账结果应以邮件或者短信等方式每天推送给系统授权的财务人员，如果对账结果异常，应给出显著提示；实时记录坏账超过一定数量时应分别给开发人员和财务人员发送通知提醒。

8.4.3.5 平台应开放账单下载功能，对账工具应具备数据报表的筛选统计和数据导出功能。

8.4.3.6 对于多院区接入互联网医院的医疗机构能够支持分院区独立对账操作。对账平台对互联网医院业务的扩展化支撑功能可包括：

- a) 对账平台需要提供图文化的对账总览，对于平账总览能够下载打印，辅助院方财务交账；
- b) 对账平台需要提供差账明细清单，辅助院方快速准确定位差账原因；
- c) 差账清单能够下载打印，院方安排专员进行差账处理；
- d) 对账平台需要支持多级权限管理，并能按照人员分配不同的访问和操作权限；
- e) 对账平台需要支持对账记录和对账日志的长期存储和导出分析，协助医院方优化业务流程及互联网医院系统功能完善；
- f) 对账平台能够对接院方的短信平台，支持分权限发送每日财务对账单到指定人群；
- g) 对账平台须长期稳定运行，对账平台数据须精准可溯源。

8.5 信息系统基础服务

8.5.1 患者身份认证服务

8.5.1.1 应对患者进行实名认证，实名认证须对患者姓名、身份证号、手机号进行实名制校验。

8.5.1.2 应支持为患者提供必要的风险提示和个人隐私保护，可通过在线签署协议的方式获取患者的同意授权，协议中应包含互联网诊疗服务内容、流程、双方责任和权力以及可能出现的风险等；禁止对未签署《知情同意书》的患者提供互联网诊疗服务。

8.5.1.3 支持统一管理注册用户的信息。应支持通过权限管理及分配机制，设定各类型、人员账号的访问权限。应支持后台查询患者的基础信息、认证信息等。应支持后台查询患者的注册日志、安全日志、操作日志等。

8.5.1.4 可依托活体检测、人脸比对等生物识别技术进行实名校验。

8.5.1.5 通过应用区块链防篡改、可追溯的技术能力将病人注册信息以及过程信息同步记录到区块链中，并将相关图片、音频、视频数据的存证位置及文件摘要信息记录到区块链上作为存证，为后续如果出现医疗纠纷作为司法取证依据。

8.5.2 医生身份认证服务

8.5.2.1 应支持注册开通或后台批量创建医生账户。医生通过注册登录方式提交身份信息和执业资质进行注册，注册成功后通过账号密码完成登录。

8.5.2.2 应支持医生提交个人免冠证件照、《医疗机构执业许可证》照片至其执业医疗机构进行审核。审核合格的，予以账号登录医生端为患者提供诊疗服务；审核不合格的，将审核结果通过医生端消息通知申请人。在平台上提供诊疗服务的医师须在依托的实体医疗机构或其他医疗机构注册，且须具有3年以上独立临床工作经验。

8.5.2.3 应提供医生实名认证功能，能够管理医生个人基本信息、身份证、执业医师注册证、执业医师资格证等信息。医师信息应能在国家医师注册系统中查询。

8.5.2.4 应提供完整的后台管理功能，将线上提供服务的医生的个人信息、账号权限、处方权信息、服务定价、服务方式、服务开通与关闭等由医院管理部门统一管理。

8.5.2.5 应支持医生进行电子签名认证，数字证书应来自具有发布可信电子认证的机构。对开具处方过程中的处方审核管理提供证书签名，所有在线诊断、处方必须有医师电子签名，保证诊疗过程中传递信息的安全性、真实性、可靠性、完整性和不可抵赖性，有移动端开方功能的，须在移动端实现数字证书的应用。

8.5.3 药师身份认证服务

8.5.3.1 应支持注册开通或后台批量创建药师账户方式。药师通过注册登录方式提交身份信息和执业资质进行注册，注册成功后通过账号密码完成登录。

8.5.3.2 应支持对药师提交个人免冠证件照、相应资质证明和执业证书信息到实体医疗机构进行审核，审核通过后，予以账号登录药师端；审核不合格的，将审核结果通过药师端消息通知申请人。可与第三方机构药师建立合作关系，签署合作协议后方可开通账号。

8.5.3.3 药师在线审方时可使用电子签名，对开具处方过程中的处方审核管理提供电子签名，保证诊疗过程中传递信息的安全性、真实性、可靠性、完整性和不可抵赖性。

8.5.3.4 有条件的医疗机构，可通过人证比对与识别、证件OCR、静默活体和视频认证等技术，进行药师的身份识别认证。

8.5.4 医疗机构身份认证服务

8.5.4.1 互联网医院应根据当地互联网医院监管要求登记机构信息，机构信息包括机构编号、机构名称、机构类型、接入IP地址等。

8.5.4.2 应对接当地医疗服务与执业监管平台进行机构信息申请提交接入，管理机构审核通过后方可开展互联网医院诊疗业务。

8.5.4.3 管理机构应能够通过当地医疗服务与执业监管平台对机构信息进行查询。

8.5.4.4 医疗机构可对接医疗机构查询接口进行机构认证实时校验。

8.5.5 消息服务

8.5.5.1 互联网医院应当为业务系统提供短信、微信、站内信的消息服务，如业务办理通知、业务查询通知、问诊信息推送、健康信息推送等消息推送服务，须提供业务系统间的消息收发能力，可支持基础业务消息不限于以下内容：

- a) 业务办理通知;
- b) 就诊服务提醒;
- c) 处方消息通知;
- d) 处方订单消息通知。

8.5.5.2 根据医院系统平台建设情况构建消息推送,提供消息服务注册管理、消息类型管理、消息渠道配置、自定义消息模板等服务,满足新增业务相关通知推送需求,满足微信小程序、微信公众号、短信、APP应用消息等多渠道消息触达需求。

8.5.6 电子病历与健康档案共享服务

互联网医院应为参与互联网诊疗活动的患者建立并提供电子病历及健康档案管理服务,实现电子病历及健康档案内容的统一化管理,包括电子病历及健康档案的上传、调阅、归档,支持医生在接诊过程中查看患者的基础信息,并在相应服务流程中提供调阅功能。电子病历及健康档案内容包括但不限于患者的门诊记录、检查记录、检验记录、住院记录等,为医护人员提供完整的、实时的病人信息访问。数字中医诊疗平台应与实体医疗机构的线下信息系统对接,实现线上线下一体化管理。

8.5.7 即时通信交互组件服务

8.5.7.1 互联网医院应当提供即时通信服务相关各方的交互组件,包括图文互动组件和音视频互动组件。

8.5.7.2 应提供实时(聊天)和延时(留言)模式,支持文字、图形和语音;支持一对一互动场景。

8.5.7.3 应提供音视频功能软件,支持平台开播、观看和互动;满足视频问诊、远程医疗等多种应用场景。即时通信交互组件可直接调用,嵌入业务流程中,利用该组件的互动记录将保存在数据中心备查。

8.5.8 接口网关服务

8.5.8.1 在系统设计过程中,不可避免地需要对内或者对外以统一数据交互标准格式提供服务,因此应建立接口网关服务,聚合各个业务模块服务接口,提供统一的签名算法、加解密算法、流量控制、访问鉴权以及监控等能力,保障系统数据交互的安全性、可靠性和稳定性。

8.5.8.2 在数据传输过程中,采用国密算法对参数进行加密和签名,接收到数据的时候采用国密算法进行解密和签名验证,保障数据安全性。

8.5.8.3 依据评估的系统用户数和系统可承载量对接口按需进行流量控制,提供限流和熔断机制,防止访问量突增带来的系统不可用。

8.5.8.4 应具备完善的接口权限管理体系,对系统接入方做严格的身份认证及访问权限判定等,禁止非法访问。

8.5.8.5 应建立完善接口访问监控系统,实时监控服务访问状态,遇到非法访问、攻击或者系统崩溃情况应该及时对系统管理员发出警告并及时作出处理。

8.5.8.6 支持多种负载均衡规则,提高系统高并发和高可用。

8.5.9 医保电子凭证对接服务

开展线上医保结算的互联网医院需对接医保电子凭证,参照 XJ-D01《医疗保障信息平台电子凭证技术规范》开展线上医保结算业务。

8.6 信息系统管理

8.6.1 基础管理

基础管理包括但不限于以下内容:

- a) 医院信息管理：管理设置审核互联网医院业务的基本信息、账号密码等；
- b) 科室信息管理：对互联网医院的科室进行管理，包括创建科室，修改科室、禁用科室等。拟开展的互联网诊疗科目不应超出所依托实体医疗机构的诊疗科目范围；
- c) 资质信息管理：针对互联网医院坐诊医生人员资质进行管理，根据资质确定图文、电话、视频的收费标准；
- d) 人员信息管理：对机构的人员进行管理，包括新建医生，医生权限、修改医生信息和权限等；
- e) 业务权限管理：超级管理员对后台管理员以及医生进行权限管理，对不同的人分配其对应的权限；
- f) 非药品目录管理：针对患者编码、医嘱类型编码以及收费项目编码等信息数据进行统一编码管理，应参照相关医疗服务与执业监管平台中所采用的数据接口标准模式；
- g) 价格管理：管理互联网医院挂号、处方等价格；
- h) 排班管理：管理互联网医院的医生排班，支持批量导入、单个修改、网诊时段、号数的设置等；
- i) 消息管理：管理所有收到和发出的消息，需实现发送消息功能。

8.6.2 药品目录管理

8.6.2.1 对互联网医院的药品目录进行管理，供医生开电子处方使用，可对药品进行新增、禁用。规范维护药品数据字典，如药品代码、通用名、规格、价格等，统一命名口径，提高协作效率。

8.6.2.2 根据互联网医院开具处方的要求，麻醉药品、精神类药品及其他用药风险较高、有其他特殊管理规定的药品，确保不能列入药品目录，或加上管制分类标记按要求进行管理。

8.6.2.3 设置独立的账户权限，由互联网医院的药学团队负责在线药品目录的维护，在配送条件不能保证的情况下，某些对运输有特殊要求的药品不宜列入药品目录。药品目录的维护应做好人员权限控制，建议增加审核发布机制，当新增、删除或变更药品信息时，由更高级别的药师进行审核发布。药品信息的修改记录，应在信息系统中留痕。

8.6.3 信息公示

平台系统患者端应展示如下信息：

- a) 核发的执业许可证、卫生技术人员依法执业注册基本情况和卫生技术人员提供诊疗服务时的身份标识；
- b) 经卫生健康行政部门批准开展的诊疗科目；
- c) 提供的诊疗服务方式及出诊医师信息；
- d) 诊疗服务、常用药品和主要医用耗材的价格；
- e) 医疗纠纷处理程序、医疗服务投诉信箱和投诉咨询电话；
- f) 诊疗服务中的便民服务措施；
- g) 提供预约挂号开放规则、可提供预约挂号的号源情况以及相关停诊/替诊信息。
- h) 满意度评价公示；
- i) 健康宣教；
- j) 帮助中心。

8.6.4 医疗质量监控管理

8.6.4.1 系统支持业务流程闭环管理，保证诊疗行为的规范性和可追溯性，对在线复诊、电子处方进行监管。

8.6.4.2 支持在线复诊医生信息、患者信息、在线复诊记录信息等数据项进行监管。

8.6.4.3 支持采集互联网医院的电子处方与电子处方的流转信息，到处方的合理性、合规性、药品目录范围、医师合格性、药师审方等内容进行监管。监管数据项应包括：

- a) 在线处方医生信息；
- b) 患者信息；
- c) 处方信息等。

8.6.4.4 支持对互联网医院的各项协议进行管理，包括与医生的协议、与患者的协议，当发生医疗纠纷时可供参照。

8.6.4.5 支持对互联网医院的机构准入、诊疗科目范围、执业医师资格进行监管。支持对接执业医师库，验证和审核执业医师开展互联网医疗资格的合规性。对接医疗机构信息库，验证和审核互联网医院开展互联网医疗的诊疗科目范围的合规性。

8.6.5 数据统计分析

数据统计分析应包括但不限于：

- a) 预约挂号统计；
- b) 就诊记录统计；
- c) 专科门诊统计；
- d) 出诊记录统计；
- e) 服务评价统计；
- f) 财务数据统计；
- g) 业务数据统计；
- h) 医生数据统计；
- i) 患者数据统计；
- j) 病种数据统计。

8.6.6 监管数据上传

8.6.6.1 中医互联网医院应接入省级医疗服务与执业监管平台，并按照要求以中间表或服务的形式完成数据上传，接受管理机构的实时监管。

8.6.6.2 有区块链技术实现数据同步的医疗机构，可对监管数据的处理全部流程实现可追溯功能。

8.6.7 服务评价管理

服务评价管理功能包括但不限于：

- a) 患者评价：可支持患者在问诊结束后对医院、科室、医生进行满意度评价；
- b) 查看评价：患者端可显示当前发出的评价，医生端可显示所有可看的评价；
- c) 处理评价：可设置待处理显示、按时间排序等内容项，并提醒相关人员及时处理；对于没有证据否定其真实客观性的患者评价，互联网医院不得自行删除；
- d) 评价设置：可根据服务内容的差异，设置相关评论权限、规则，通过对患者所发出的评价予公开显示或隐藏操作，实现后台对服务评价进行统一管理；
- e) 投诉处理：可支持管理患者投诉的订单，并对相关投诉的服务内容进行反馈，以告知患者具体处理的结果。

8.6.8 黑名单管理

8.6.8.1 应支持在对违规使用或滥用在线医疗资源的情况进行筛查与识别的基础上，对特定的人群进行黑名单管理，按照医院确定的规则限制其线上的行为。记录达到一定次数以上爽约即进入黑名单，支持黑名单用户在一段时间内不允许互联网医院预约挂号。

8.6.8.2 应支持通过申诉或者人工客服方式针对意外操作或者网络原因等特殊情况进行黑名单的解封功能。

9 安全要求

9.1 基本要求

9.1.1 安全设计原则

9.1.1.1 根据各医疗机构的技术实现方式，数字中医诊疗平台在网络安全等级保护定级时，可作为独立的信息系统备案，也可作为医院信息系统的子系统进行备案。

9.1.1.2 数字中医诊疗平台的运营单位为网络与信息系统安全相关责任主体，应按照 GB/T 22239-2019 和 GB/T 28448-2019 等要求，根据第三级信息安全级安全保护等级选择基本安全措施，进行安全整体规划和方案设计，并依据风险分析的结果补充和调整安全措施。

9.1.1.3 数字中医诊疗平台的建设和运行维护单位应做好网络与信息系统安全工作，保障网络与信息系统安全可靠运营。

9.1.2 总体框架

互联网医院安全体系总体框架设计要求包括：

- a) 互联网医院安全体系从通用要求、扩展要求进行框架设计；
- b) 应从身份认证要求，访问控制要求，审计要求，数据完整性及保密性要求，备份要求几个层面实现安全基本要求；
- c) 应从云计算安全层面实现安全扩展要求；
- d) 针对信息系统的安全策略及安全计算环境、安全区域边界和安全通信网络三个部分的安全机制，形成一个统一的安全管理中心，实现统一管理、统一监控、统一审计、综合分析且协同防护。

9.1.3 安全物理环境

9.1.3.1 应保证基础设施位于中国境内，存储医疗数据的服务器不得存放在境外。

9.1.3.2 应划分数据库服务器和应用系统服务器，并保证应用服务器和数据库服务器放置于不同的区域。

9.1.3.3 存放服务器的机房应当具备双路供电或紧急发电设备。

9.1.4 安全通信网络

9.1.4.1 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

9.1.4.2 展互联网医院业务的音视频支持设备应有冗余（包括必要的软件系统和硬件设备）。

9.1.4.3 互联网医院应具备高速率高可靠的网络接入，业务使用的网络带宽不低于 10 Mbps，且至少由两家宽带网络供应商提供服务。有条件的互联网医院可接入互联网专线、虚拟专用网（VPN），保障医疗相关数据传输服务质量。

9.1.5 安全区域边界

- 9.1.5.1 应在数字中医诊疗平台网络边界设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。
- 9.1.5.2 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
- 9.1.5.3 应设置防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件，对恶意代码进行检测和清除并维护恶意代码防护机制的升级和更新。
- 9.1.5.4 应采取欺骗诱捕等技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
- 9.1.5.5 应对在线运行的 Web 系统进行不间断的安全漏洞分析、恶意程序分析、可用性分析等，持续对 Web 端进行安全监测。
- 9.1.5.6 应采取资产测绘技术措施，定期对互联网医院平台资产进行梳理、排查和更新。
- 9.1.5.7 应具备互联网医院内容监测措施，针对违法违规信息进行检测和拦截。

9.1.6 安全计算环境

- 9.1.6.1 应通过数据库审计系统等安全设备对数据库进行安全审计。
- 9.1.6.2 具有医学文书效力的资料，如病历、处方等，需要附加接诊医生的电子签名和可靠时间戳。
- 9.1.6.3 电子处方的修改，须以电子签名或采用密码等方式在信息系统中留痕，应包括调剂药师信息、调剂时间、药品信息等。
- 9.1.6.4 应采用加密或其他有效措施实现鉴别数据、重要业务数据和重要个人信息等的传输保密性及存储保密性。
- 9.1.6.5 采用符合 GM/T 0028-2014 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。
- 9.1.6.6 应对重要数据处理系统（包括应用服务器、Web 服务器、数据库服务器等）采用热冗余方式部署。

9.1.7 管理要求

- 9.1.7.1 应在管理制度中对《互联网医院管理办法（试行）》所涉及的关键事项均有明确规定。
- 9.1.7.2 应在管理制度中明确规定医疗数据存储、访问策略。
- 9.1.7.3 如果与第三方机构合作建立互联网医院，应当签署合作协议，明确各方在医疗服务、信息安全、隐私保护等方面的责任和权利。
- 9.1.7.4 应落实个人隐私信息保护措施，收集个人信息时的授权同意及制定的隐私政策应符合 GB/T 35273-2020 的规定。
- 9.1.7.5 应设置医疗质量管理部门、信息技术服务与管理部门、药学服务部门。
- 9.1.7.6 应有专人负责互联网医院的医疗质量、医疗安全和电子病历管理。
- 9.1.7.7 应有专人负责医院智能信息系统运维等技术服务，确保系统稳定运行。

9.2 云计算要求

- 9.2.1 应确保数字中医诊疗平台系统所在云计算平台的运维地点位于中国境内。
- 9.2.2 应确保与云服务商签订保密协议，明确云服务商的责任与权限，并规定服务合约到期时，完整提供互联网医院客户数据，并承诺相关数据在云计算平台上清除。
- 9.2.3 应在数字中医诊疗平台系统的虚拟化网络边界部署访问控制机制，并设置访问控制规则。
- 9.2.4 当远程管理云计算平台中设备时，管理终端与云计算平台之间应建立双向身份验证机制。
- 9.2.5 应确保互联网医院所在云计算平台支持部署密钥管理解决方案，保证互联网医院运营主体自行实现数据的加解密过程。

9.3 客户端应用软件安全要求

9.3.1 安全计算环境

9.3.1.1 一般要求

客户端应用软件，如互联网医院 APP、微信公众号或小程序等，应符合安全代码编写规范，使用代码安全防护手段（例如代码加壳、代码混淆、检测调试器等）对客户端应用软件进行安全保护，使之具备一定的抗攻击能力，防止重要信息泄露和非法获取使用。

9.3.1.2 程序安全

- 9.3.1.2.1 应在客户端应用软件安装、更新时对自身的完整性和合法性进行验证。
- 9.3.1.2.2 应具备身份认证控制和认证失败策略。
- 9.3.1.2.3 应采用两种或两种以上的要素对用户身份进行认证。
- 9.3.1.2.4 应具备会话超时后要求重新鉴权的机制。
- 9.3.1.2.5 应配合服务端提供密码复杂度校验功能。
- 9.3.1.2.6 应具备抵御动态调试、反编译、篡改、劫持、截屏、键盘窃听、重放等抗攻击能力。
- 9.3.1.2.7 应保证安装文件中不包含任何冗余文件和冗余说明。
- 9.3.1.2.8 应保证安装文件中不包含明文证书、密钥、网络配置等信息。
- 9.3.1.2.9 应避免使用存在已知漏洞的第三方组件。
- 9.3.1.2.10 应具备客户端应用软件运行环境检测能力。

9.3.1.3 通信安全

- 9.3.1.3.1 应在客户端应用软件与服务器之间建立安全的信息传输通道，协议版本应及时更新至安全稳定版本。
- 9.3.1.3.2 客户端应用软件与服务器应进行双向认证。

9.3.1.4 数据安全

- 9.3.1.4.1 应保证登录密码、支付密码及其他输入的敏感信息，不以明文显示。
- 9.3.1.4.2 应确保敏感数据在通过公共网络传输时的完整性和保密性。
- 9.3.1.4.3 应采用自定义权限保护组件访问。
- 9.3.1.4.4 应采取措施保护客户端应用软件数据仅能被授权用户或授权应用组件访问。
- 9.3.1.4.5 应保证在内存、临时文件、运行日志中不应以明文形式存储敏感数据。
- 9.3.1.4.6 应保证客户端应用软件进程被结束时、卸载后，不应残留敏感数据。
- 9.3.1.4.7 应支持页面返回、进入后台后，自动清除已输入的敏感信息。
- 9.3.1.4.8 应确保通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求。

9.3.2 安全建设管理

9.3.2.1 应用合法性监测

应对在线运行的客户端应用软件进行应用合法性判别，防止盗版应用导致个人信息泄露等风险。

9.3.2.2 安全风险监测

应对在线运行的客户端应用软件进行不间断的安全漏洞分析、恶意程序分析等，持续对客户端应用软件在版本更新及运行过程中进行立体安全防护。

10 系统运行质量评价

依据 GB/T 25000.10-2016、GB/T 25000.23-2019 和 GB/T 25000.51-2016 设计质量模型与评价准则，对软件进行测试与评价。
