北京市卫生健康大数据与政策研究中心

京卫数研中心〔2022〕12号

北京市卫生健康大数据与政策研究中心关于印发《北京地区互联网医院信息系统建设指南》的通知

各医疗机构:

为指导北京市各医疗机构互联网医院信息系统建设，现将《北京地区互联网医院信息系统建设指南》印发给你们，请各医疗机构结合实际情况，参考执行。

附件:《北京地区互联网医院信息系统建设指南》

北京市卫生健康大数据与政策研究中心

2022年5月18日

北京地区互联网医院信息系统建设指南

北京市卫生健康大数据与政策研究中心

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。

本文件由北京市卫生健康大数据与政策研究中心提出。

本文件由北京市卫生健康大数据与政策研究中心组织实施。

本文件起草单位：北京市卫生健康大数据与政策研究中心、中国软件评测中心、东华医为科技有限公司、上海联空网络科技有限公司、北京京东健康有限公司、厦门市易联众易惠科技有限公司、国新健康保障集团服务有限公司、北京知道创宇信息技术股份有限公司等。

本文件主要起草人：琚文胜、张世红、衡爽、孟晓、杨令宣、白玲、杨小冉、惠轩、周泽均、王宇、林家彬、王凯、馬列、周梦琪等。

引　言

为贯彻落实《国务院办公厅关于促进“互联网+医疗健康”发展的意见》有关要求，依据国家卫生健康委员会发布的《互联网诊疗管理办法（试行）》和《互联网医院管理办法（试行）》，以及北京市卫生健康委员会发布的《北京市互联网医院审核细则（试行）》等文件，规范和推进北京地区互联网医院健康发展，发挥远程医疗服务的积极作用，提高医疗服务效率，保证医疗质量和医疗安全，制定本文件。

本文件从功能、安全、质量等方面指导和规范互联网医院信息系统建设。

对文件中的具体事项，法律法规另有规定的，需遵照其规定执行。

北京地区互联网医院信息系统建设指南

1 范围

本文件规定了互联网医院信息系统总体框架以及功能、安全、质量等方面的技术要求。

本文件适用于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，也适用于开展互联网诊疗业务的实体医疗机构。

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 18336.2-2015 信息技术 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 信息系统安全等级保护基本要求

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

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

GM/T 0028 密码模块安全技术要求

GM/T 0054-2018 信息系统密码应用基本要求

YB XJ-D01-2019 医疗保障信息平台电子凭证技术规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

互联网医院 internet hospital

经本市各级卫生健康行政部门审批，取得《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。

3.1.2

互联网医院信息系统 internet hospital information system

互联网医院向患者提供互联网诊疗服务的信息系统。

3.1.3

实名认证 identity verification

以直接或间接的方式，经身份证件签发机构提供的相关验证渠道，对用户身份真实性进行验证。

3.1.4

复诊 subsequent visit

在《医疗机构执业许可证》登记的执业范围内，患者在一定时间内同类专业科室已被确诊的疾病（主要包括常见病和慢性病），再次进行相同诊断疾病的就诊活动。

3.1.5

电子处方 electronic prescription

是指由注册的执业医师和执业助理医师采用信息技术，在诊疗活动中为患者开具的，由取得药学专业技术职务任职资格的药学专业技术人员审核，并作为患者用药凭证、药房或药店发药的电子医疗文书。

3.1.6

区块链 blockchain

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

3.2 缩略语

AI：人工智能（Artificial Intelligence）
APP：应用程序（Application）
CPU：中央处理器（Central Processing Unit）
EMR：电子病历（Electronic Medical Record）
HIS：医院信息系统（Hospital Information System）
LIS：检验信息系统（Lab Information System）
OCR：光学字符识别（Optical Character Recognition）
PACS：图像归档和通信系统（Picture Achieving and Communication System）
PC：个人计算机（Personal Computer）
RIS：放射信息系统（Radiology Information System）
SDK：软件开发工具包（Software Development Kit）
UTM：统一威胁管理（Unified Threat Management）

4 互联网医院技术总体架构

互联网医院信息系统总体架构如图 4.1 所示。

总体架构适用于一家医疗机构通过自主或合作的模式建设符合本文件的互联网医院信息系统，向患者提供互联网诊疗服务，也适用于区卫生健康委员会通过自主或合作的模式建立符合本文件要求的互联网医院信息系统，支持区域内一家或多家互联网医院的入驻与运营，同时与北京市医疗服务与执业监管平台对接，满足互联网医疗业务的监管要求。

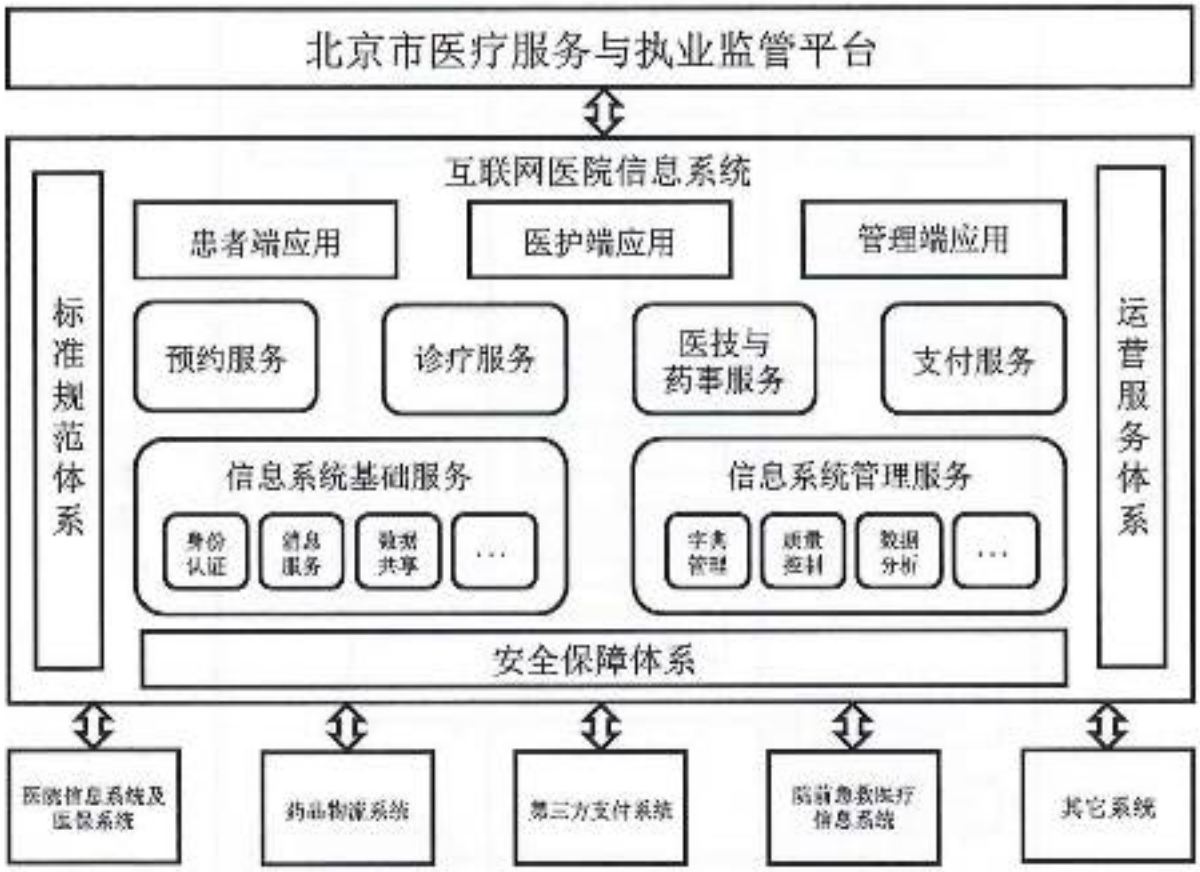

图 4.1 互联网医院信息系统总体架构

互联网医院信息系统应与医院信息系统（包括LIS、HIS、PACS、RIS、EMR等）、医保系统、药品物流系统、第三方支付系统、院前急救医疗信息系统及其它系统进行对接，整合各方服务能力，为面向居民的互联网医疗服务提供支撑。

互联网医院信息系统应面向患者、医生、医院管理者提供针对性的服务功能。业务应用围绕患者的就医流程，提供便捷的预约服务、在线支付服务；围绕患者的复诊、用药需求提供在线诊疗服务、医技与药事服务。患者端应用宜采用多种入口，如公众号、小程序、APP等，构建医院线上互联网服务入口；医护端应用应包括移动端、PC端等入口，支撑医护人员移动化办公的同时，也支持和医院线下工作站进行充分融合，丰富医护应用场景；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。

安全保障体系应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。

互联网医院信息系统应对接北京市医疗服务与执业监管平台，满足北京市互联网诊疗服务监管要求。

互联网医院信息系统应遵循国家标准和行业标准规范体系，遵守成熟、可靠、稳定的技术路线，主动规避建设过程中的风险。

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

互联网诊疗服务基本流程如图4.2所示。

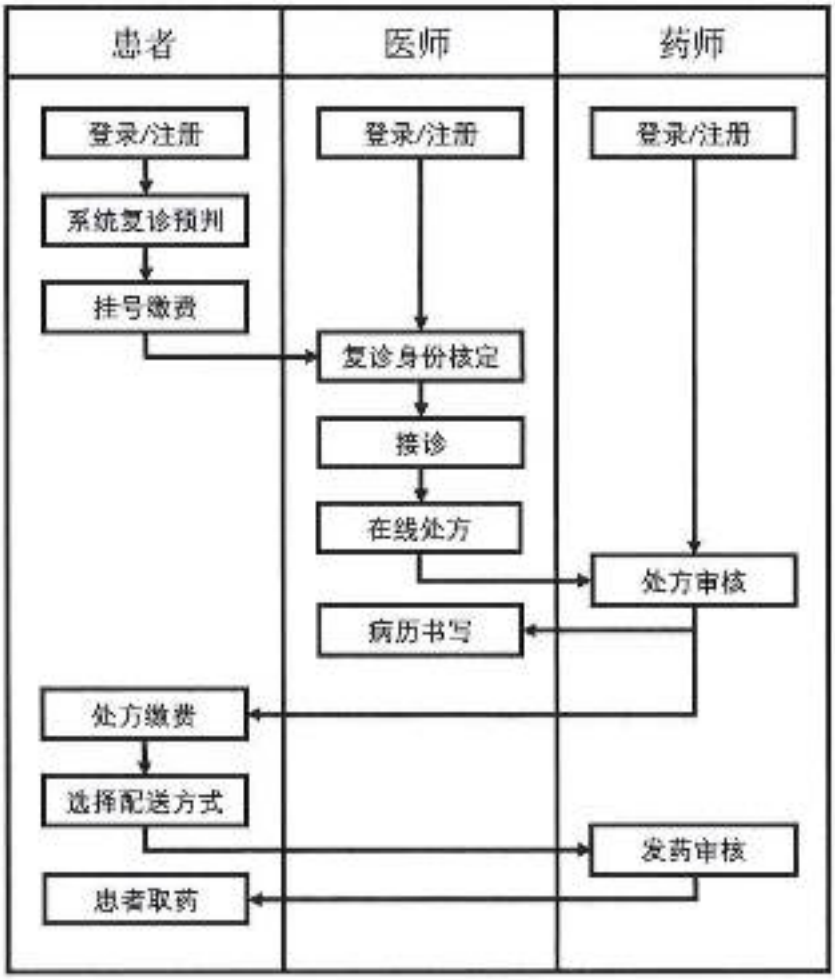

图 4.2 互联网诊疗服务基本流程

5 功能规范

5.1 预约服务

5.1.1 资源管理

5.1.1.1 基本要求

号源查询：应在互联网医院信息系统患者端的显著位置展示在线复诊的服务范围，提供预约挂号号源查询功能，支持查询医院可挂号科室、科室医生、医生号源（含多院区号源）。

出诊安排：互联网医院应支持设置出诊时间安排，排班后医师针对复诊患者进行线上复诊。

多维度展示：系统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，如在科室主页展示科室概况、诊疗范围、优势和特色，在医生主页展示医生职称、执业资质、擅长或其它自定义维度说明。

5.1.1.2 扩展要求

按资源属性查询：系统宜在号源管理基础上按照资源的属性为患者提供查询功能，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。

医师临时调班：系统可支持医师临时调班，并给患者推送通知提醒，医师可追加临时预约号源，提供给有需要的患者进行在线预约。

5.1.2 复诊预判

5.1.2.1 基本要求

复诊预判：互联网医院应严格执行对复诊条件的判断，仅对患者既往在实体医疗机构确诊的常见病/慢性病进行在线复诊，需要对接医院HIS、EMR等系统进行自动判断，具体要点包括：

（1）患者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；

（2）在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，具体时间范围应按照国家政策要求并根据实体医疗机构规定执行。

（3）开具处方时遇低龄儿童（<6岁）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。

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可包括：

（1）患者自行提供的历史病历（相关图文信息）；

（2）本实体医疗机构已有的电子病历；

（3）通过北京市、区级区域卫生信息平台或医联体信息系统调取的患者电子健康档案。

5.1.2.2 扩展要求

多维度管理：有条件的医疗机构，可通过疾病多维度数据结构的形式形成对患者慢性病、常见病的规范化管理。

智能预判：系统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，当且仅当患者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。

数据上链：系统可将患者历史病历（图文信息）和该患者历史就诊病历或电子健康档案的上链数据进行对比，核查是否存在差异，并通过区块链技术将调取患者健康档案的行为动作过程数据进行记录。

5.1.3 复诊预约挂号

5.1.3.1 基本要求

在线挂号：系统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，应对就诊患者本人的实名认证信息进行核对。在线预约挂号操作后，应向患者发送通知或提醒，防止误操作。在线预约挂号应以患者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。

挂号成功提醒：在线挂号成功后，以推送消息或手机短信的方式对患者进行提醒。

就诊等待：挂号信息与对应互联网医院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。

挂号信息管理：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。

5.1.3.2 扩展要求

临时预约挂号：医护端可帮助患者进行在线临时预约挂号，方便老年患者在线就医。

数据上链：有条件的医疗机构可将在线预约挂号和就诊的全流程数据记录到区块链上，链数据可在患者授权下在区块链上各个医疗机构间互通共享，方便对患者就诊记录进行追溯。

5.2 诊疗服务

5.2.1 提醒医师出诊

5.2.1.1 基本要求

医师出诊提醒：系统应为医师提供出诊提醒功能，当系统为医师分配出诊后，应及时以推送消息或手机短信的方式通知到医师本人。

查看出诊列表：医师登录系统后，可查看本人待接诊、接诊中、已完成的出诊列表。

5.2.2 提醒患者就诊

5.2.2.1 基本要求

患者就诊提醒：系统应在约定的接诊时间前以推送消息或手机短信的方式通知提醒患者进行线上就诊。

5.2.3 在线复诊

5.2.3.1 基本要求

复诊身份核定：系统应支持医师在接诊前预览患者历史病历，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。

医师接诊：系统应支持医师对待接诊患者进行接诊操作，查看患者提交的病情信息、健康档案和相关图文信息等。

医患交流：系统应支持医师通过图文、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，记录保存时间应遵照国家有关规定。

中止复诊：系统应提供中止线上复诊的功能，当医师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。

消息提醒：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。

5.2.3.2 扩展要求

在线会诊：患者在实体医疗机构就诊，由接诊的医师通过互联网医院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。

治疗类处方开具：有条件的医疗机构，可支持医师为患者在线开具检验、检查、治疗等处方。

多学科会诊：根据患者病情，可提供远程多学科联合诊疗服务。

5.2.4 在线处方

5.2.4.1 基本要求

在线处方：系统应支持医师针对患者既往明确诊断、用药等情况，在保障用药安全的前提下，在线开具处方。

处方引导：系统应引导医师遵守《处方管理办法》等相关规定，禁止医师在线开具麻醉药品、精神药品等特殊管理药品的处方。

电子签名及时间戳：系统应在医师在线诊断、提交处方时执行电子签名，加盖可靠时间戳。

开处方查库存：医师开方时，系统应支持通过接口等方式实现查询医院药房、合作第三方药品供应商的药品库存信息。

5.2.4.2 扩展要求

医师、药师身份认证信息整合：可应用区块链技术实现医师、药师身份认证信息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，即在不改变原有系统业务流程的情况下，将多种医疗相关的标识信息进行整合共享，方便应用扩展。

数据上链：在医师、药师进行电子签名时，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。

5.2.5 病历书写

5.2.5.1 基本要求

病历书写：系统应支持医师在线书写电子病历，电子病历基本内容应包括主诉、现病史、既往史、诊断、治疗意见等必要信息。系统应引导医师遵循《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。

5.2.6 病历资料查询

5.2.6.1 基本要求

病历资料在线查询：互联网医院信息系统应支持患者在线查询本人检查检验结果和资料、诊断治疗方案、处方和医嘱等病历资料。互联网医院信息系统应支持医师查阅患者既往电子病历和电子健康档案资料。

5.2.6.2 扩展要求

病历资料下载：互联网医院信息系统宜支持患者下载检查检验结果和资料、诊断治疗方案、处方和医嘱等病历资料。

5.3 医技与药事服务

5.3.1 医技服务

5.3.1.1 扩展要求

医技系统对接：系统宜与院内医技系统对接，支持医师在线开具检查检验申请，支持检查检验预约。

5.3.2 处方审核

5.3.2.1 基本要求

审方药师签到：互联网医院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。

审方规则：医师电子签名完成后，将处方提交至互联网医院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。

审方确认：系统应支持药师进行处方审核，审核处方时验证处方无篡改后，必须执行电子签名，加盖可靠时间戳。

5.3.2.2 扩展要求

系统辅助审方：系统可提供基于规则库、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师强制生效的处方需特别记录。

5.3.3 合理用药

5.3.3.1 扩展要求

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

（1）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；

（2）处方下达时能获得的药品剂型、剂量或可供应药品提示；

（3）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；

（4）对麻醉药品、精神类药品处方以及其他用药风险较高、有其他特殊管理规定的药品处方给予警示。

5.3.4 处方确认

5.3.4.1 基本要求

支付订单生成：系统应对已审核处方的费用进行合理划分，生成在线的支付订单推送至患者端。

患者确认：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。

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

5.3.5 对接药品

5.3.5.1 基本要求

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

5.3.6 药品供应管理

5.3.6.1 基本要求

入库审批：系统应提供对申请入库的药品信息进行合规性审核管理的功能。

药品编码：系统应对合规性入库的药品进行重新编码以符合在线处方开具的监管需求。

药品库管理：系统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、批次、效期、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。

5.3.6.2 扩展要求

供应商药品管理：系统宜提供对第三方合作药品供应商的药品信息管理功能，包括药品名称、药品编码、药品简介等内容。

接口管理：系统宜支持对合作的药品供应商、药品物流公司信息与互联网医院药库的接口信息进行管理。

5.3.7 患者购药

5.3.7.1 基本要求

订单支付：系统应支持患者通过支付平台完成订单支付。

取药方式选择：系统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。

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

5.3.7.2 扩展要求

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

5.3.8 药品调剂

5.3.8.1 基本要求

药品调剂信息推送：药品在完成收费后，系统应结合互联网医院药品管理方式，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。

药品调剂审核：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。

5.3.9 药品配送

5.3.9.1 基本要求

药品配送：当患者选择配送作为取药方式时，实体医疗机构药房和第三方药品供应商应及时将调剂好的药品交由药品配送机构进行配送，配送形式可包括配送上门、定点“自助药柜”存放、附近药店及站点取药等。

5.3.9.2 扩展要求

供应商与物流信息联通：互联网医院宜与药品供应商、药品配送机构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。

配送全流程管理：系统宜提供针对药品配送完整环节的全流程管理，设置药品打包环节的监管措施，如高清摄像等，并保留与第三方物流公司交接的系统化记录，将药品信息、药品配送信息上传至互联网医院信息系统，供药品配送机构和患者本人实时查询当前配送状态。

服务定期审核：互联网医院可提供对药品供应商和药品配送机构的定期审核功能，以保证药品生产、储存和流通环节的安全和高效。

5.3.10 药品签收

5.3.10.1 基本要求

药品签收验证：药品的签收应有签收人验证，如提货码、医保卡、身份证等作为验证标识，实现药品的配送到人，避免配送错误引起的医疗纠纷。

签收信息反馈：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。

5.3.10.2 扩展要求

用药指导：互联网医院信息系统宜提供用药指导功能。

患者用药关注：在患者签收药品后，互联网医院宜关注患者用药情况，如提供用药依从性管理、用药不良反应的快速反馈通道、续方提醒等功能。

5.4 支付服务

5.4.1 在线支付

5.4.1.1 基本要求

统一支付：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至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。

在线付款：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、数字人民币、银行卡等在线支付渠道进行实时付款，账单由互联网医院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。

账单关闭：互联网医院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。

消息推送：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，消息内容包含费用概要信息和支付状态，患者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。

5.4.1.2 扩展要求

医保支付：互联网医院宜与北京市医保对接为患者开通医保支付，结合医保规则对处方中自费、自付、共付的费用进行划分。

多方支付：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。

账单分类管理：互联网医院宜面向患者提供对各类账单的分类管理。

电子发票：有条件的互联网医院可在支付完成后为患者提供电子发票。

5.4.2 退费处理

5.4.2.1 基本要求

在线复诊服务退费：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，系统应支持在线复诊服务费用的退费操作。

药品退费：患者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，非药品质量原因不得办理退费，如患者必须退费，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，协商情况需进行记录。

退费进度查询：互联网医院信息系统应支持患者查询退费进度，并通过推送消息或手机短信的方式对患者进行提醒。

5.4.2.2 扩展要求

医保退费：对于有能力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北京市医保实行的在线医保结算退费流程进行退费操作。

检验检查退费：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。

退费到账周期提醒：根据患者在线支付途径对于退费周期的不同要求，系统宜在退费操作完成时推送消息提醒患者预计的退费到账周期。

5.4.3 财务对账

5.4.3.1 基本要求

统一对账平台：互联网医院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要求。互联网医院信息系统应提供统一对账平台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互联网医院信息系统生成账单财务对账、医院信息系统生成账单财务对账、第三方药品供应链生成账单的财务对账。按照医院财务对账时间要求，对账方式包括：

（1）当日对账：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，针对问题账单进行错账提醒，并通过相应角色进行错账处理实现账款平衡；

（2）隔日对账：在互联网医院关账时间的隔日进行财务对账，系统根据前一个财务日所产生的全部账单信息和支付订单进行账款匹配核实，账款不符时应定位到问题账单，并提供问题账单的错账处理操作功能。

监控预警：对账结果应以邮件或者短信等方式每日推送至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管理人员和财务人员发送通知提醒。

账单下载：系统应提供图文化的对账总览和账单下载功能，对账工具应具备数据报表的筛选统计和数据导出功能。

5.4.3.2 扩展要求

自动对账：系统宜具备无差错账单自动对账功能。

差账定位：系统宜具备账款不平场景下的可追溯过程定位差异根源等功能，如提供差账明细清单，辅助院方快速准确定位差账原因；差账清单能够下载打印，院方安排专员进行差账处理。

分院区独立对账：对于多院区接入互联网医院的医疗机构，系统宜支持分院区独立对账操作。

财务数据分析：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，对账平台数据应精准可溯源，协助院方优化财务管理。

5.5 信息系统基础服务

5.5.1 患者身份认证服务

5.5.1.1 基本要求

注册登录：患者首次使用互联网医院信息系统，应通过手机号码发送验证码进行注册，同时设置登录口令。已注册患者可通过手机验证码或账号口令登录。

实名认证：系统应对患者进行实名认证，通过患者姓名、身份证号、手机号进行实名制校验。

风险提示和知情同意：系统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。

账户管理：系统应支持统一管理注册患者的信息。应支持通过权限管理及分配机制，设定各类型、角色账号的访问权限。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。

5.5.1.2 扩展要求

生物识别：系统可依托活体检测、人脸比对等生物识别技术进行实名校验。

家庭成员实名认证：具备条件的医疗机构可在患者实名认证后，提供家庭成员管理功能。通过家庭成员实名认证信息，绑定其常用就医凭证（就诊卡、社保卡、电子健康卡等），代家庭成员完成部分线上操作。

区块链存证：可通过应用区块链防篡改、可追溯的特性将患者注册信息以及过程数据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、目录信息等关键数据记录到区块链上进行存证。

5.5.2 医护身份认证服务

5.5.2.1 基本要求

账户开通：系统应支持注册开通或后台批量创建医护账户。医护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口令完成登录。

注册审核：系统应支持医护人员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，予以账号登录医护端为患者提供诊疗服务；审核不合格的，将审核结果通过医护端消息通知申请人。在互联网医院信息系统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。应确保互联网医院所开设的临床科室，其对应的实体医疗机构临床科室至少有注册在本机构的正高级和副高级职称执业医师各1人。

实名认证：系统应提供医护实名认证功能，能够管理医护个人基本信息、身份证、执业医师注册证、执业医师资格证、护士执业证书等信息。医师/护士信息应能在国家医师/护士注册系统中查询。

账户管理：系统应提供完整的后台管理功能，将线上提供服务的医护人员的个人信息、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。系统应支持将医护信息接入北京市医疗服务与执业监管平台。

电子签名：互联网医院信息系统应支持医护人员进行电子签名，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电子签名，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，应在移动端实现数字证书的应用。

5.5.2.2 扩展要求

扩展认证功能：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，进行医护人员的身份识别认证。

5.5.3 药师身份认证服务

5.5.3.1 基本要求

账户开通：系统应支持注册开通或后台批量创建药师账户。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口令完成登录。

注册审核：系统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；审核不合格的，将审核结果通知至申请人。

电子签名：药师在线审方时应使用电子签名，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。

5.5.3.2 扩展要求

第三方机构药师合作：互联网医院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进行处方审核。

扩展认证功能：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。

5.5.4 机构身份认证服务

5.5.4.1 基本要求

信息登记：互联网医院应根据北京市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。

机构接入：系统应对接北京市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。

5.5.5 消息服务

5.5.5.1 基本要求

基础业务消息服务：互联网医院信息系统应提供基础业务消息提醒服务，包括但不限于通过手机短信、公众号、小程序、APP等方式进行提醒，基础业务消息不限于以下内容：

（1）业务办理通知：如预约挂号、缴费、退款、退药等办理消息通知。

（2）就诊服务提醒：如就诊提醒、接诊提醒、取消通知、停诊通知、入出院消息提醒等。

（3）处方消息通知：如处方审核通知、处方异常通知、处方查询、处方购药提醒等。

（4）处方订单消息通知：如订单提醒、配药提醒、发药提醒、取药提醒、签收通知等。

5.5.5.2 扩展要求

扩展业务消息服务：可根据互联网医院信息系统建设情况构建消息推送平台，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。

5.5.6 电子病历与健康档案共享服务

5.5.6.1 基本要求

电子病历及健康档案管理服务：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，支持医师接诊过程中查看患者的基础信息，如姓名、性别、年龄等，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。互联网医院信息系统应与实体医疗机构的线下信息系统对接，如HIS、PACS、RIS、LIS、EMR、集成平台或临床数据中心，实现线上、线下一体化管理。

5.5.6.2 扩展要求

信息互通共享：有条件的医疗机构可通过北京市、区级区域卫生信息平台或医联体信息系统，在互联网诊疗过程中申请调阅患者的历史电子病历与健康档案等数据信息，经患者授权同意后，可调阅查看患者在其他医疗机构的电子病历或健康档案信息，并对患者病历及健康档案的调阅使用过程进行多方记录和存证。

5.5.7 即时通信交互组件服务

5.5.7.1 基本要求

图文交互组件服务：互联网医院信息系统应提供实时（如，聊天）和延时（如，留言）模式，支持文字、图形，支持一对一互动场景；互动记录应保存在数据中心备查。

音视频互动软件服务：互联网医院信息系统应提供音视频功能软件，支持主流平台开播、观看及互动；支持一对一的互动直播，满足视频问诊、远程医疗等多种应用场景；互动记录应保存在数据中心备查。

5.5.7.2 扩展要求

扩展图文交互组件服务：互联网医院信息系统宜支持一对多、多对多的互动场景。

扩展音视频软件服务：互联网医院信息系统宜支持一对多、多对多的互动场景，支持高清视频，支持全屏及选定区域的桌面分享，支持云端录制，支持存储、转码、分发等功能，支持旁路直播。

5.5.8 接口网关服务

5.5.8.1 扩展要求

统一接口：宜使用统一的数据交互标准格式提供对内或者对外的数据交互过程服务，可通过建立接口网关服务，聚合各个业务模块服务接口，实现线上线下数据一体化，并保障系统数据交互的安全性、可靠性和稳定性。

签名和加解密算法：数据传输过程中，宜采用国密算法对参数进行加密、解密和签名验证，以保障数据安全性。

流量控制：宜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。

访问鉴权：应建立和完善接口权限管理体系，对系统接入方进行严格的身份认证及访问权限判定等，拒绝非法访问。

监控：宜建立和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时发出声光类警告并提醒相关人员及时做出处理。

负载均衡：可支持多种负载均衡规则，提高系统高并发和高可用。

5.5.9 医保电子凭证对接服务

5.5.9.1 扩展要求

医保电子凭证：有条件开展线上医保结算的医院需对接医保电子凭证，参照XJ-D01-2019《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。

5.6 信息系统管理服务

5.6.1 基础字典管理

5.6.1.1 基本要求

医院信息管理：应对互联网医院的基本信息、账户信息等进行管理。

科室信息管理：应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。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。

职称信息管理：应对互联网医院的医师及药师的职称进行管理，根据职称确定图文、电话、视频的收费标准。

人员信息管理：应对机构的人员进行管理，包括新建医师及药师、设置医师及药师权限、修改医师及药师信息和权限等。

业务权限管理：应支持业务管理员对医师及药师进行权限管理，对不同的角色分配其对应的权限。

非药品目录管理：应针对患者编码、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。

5.6.1.2 扩展要求

价格管理：宜对互联网医院普通号、专家号、处方等价格进行管理。

排班管理：宜对互联网医院的医师排班，支持网诊时段、号数设置等进行管理，支持批量导入、单个修改等。

5.6.2 医疗项目管理

5.6.2.1 基本要求

医疗项目基础管理：对于在线开具检验检查的互联网医院，应支持对检验检查等项目进行管理，提供包括但不限于：新增、删除、编辑以及统计等功能，以便医师能帮助患者开具检验检查单。

5.6.2.2 扩展要求

项目组合及快速开具：可将若干检验检查项目做自定义组合，可支持医师对患有常见疾病的患者快速开具检验检查单。

设置关联词：可自定义设置检验检查项目关键字，提高医师开具检验检查单效率。

5.6.3 药品目录管理

5.6.3.1 基本要求

药品目录管理：应对互联网医院的药品目录进行管理，对药品进行新增、禁用等操作，供医师开电子处方使用。应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。

特殊药品管理：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，应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。

药品维护：应设置独立的账户权限，由专职业务人员负责在线药品目录的维护。药品信息的修改记录，应在信息系统中留痕。

5.6.3.2 扩展要求

药品目录审核：宜提供药品目录维护人员的权限分级管理，设置审核发布机制，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。

5.6.4 信息公示

5.6.4.1 基本要求

信息公示：互联网医院信息系统患者端应展示如下信息：

（1）卫生健康行政管理部门提供的医师信息查询渠道；

（2）经卫生健康行政部门批准开展的诊疗科目；

（3）提供的诊疗服务项目、内容、流程情况；

（4）提供的诊疗服务方式及出诊医师信息；

（5）诊疗服务、常用药品和主要医用耗材的价格；

（6）医疗纠纷处理程序、医疗服务投诉信箱和投诉咨询电话；

（7）诊疗服务中的便民服务措施；

（8）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。

5.6.4.2 扩展要求

满意度评价公示：可对患者提供查看对医院、科室、医师的满意度评价等统计信息。

健康宣教：宜提供针对互联网医院首诊咨询以及复诊患者问诊相关服务科目内容，如健康信息、新闻资讯、医疗资讯、紧急通知、医院公告等进行精准推送。

帮助中心：宜提供用户使用手册，针对用户在应用使用中的问题进行解答展示，支持对患者端展示的内容进行管理，支持帮助文档类型设置，发布位置设置，显示排序设置等。

5.6.5 医疗质量监控管理

系统应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。

5.6.5.1 基本要求

在线复诊监管：应支持对在线复诊医师信息、患者信息、在线复诊记录信息等数据项进行监管。

电子处方监管：应支持采集互联网医院的电子处方与电子处方的流转信息，对处方的合理性、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：在线处方医师信息、患者信息、处方信息等。

5.6.5.2 扩展要求

协议监管：宜支持对互联网医院的各协议进行管理，包括与医师的协议、与患者的协议，当发生医疗纠纷时可供参照。

违规事件预警：宜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。宜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。宜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。监管指标项可包括：机构准入监管指标、诊疗科目准入监管指标、执业医师准入监管指标等。

5.6.6 数据统计分析

5.6.6.1 基本要求

预约挂号统计：应支持根据普通号、专家号等类型，根据科室、时间段等进行预约挂号统计分析。

就诊记录统计：应支持根据普通号、专家号等类型，根据科室、时间段等进行就诊统计。

专科门诊统计：应支持根据科室、就诊状态（未就诊、就诊中、历史未就诊、患者取消、已申请退款）、时间段和患者姓名等进行专科门诊统计。

医师出诊记录统计：应支持根据科室、医师统计出诊次数，包括总出诊次数、本月出诊次数和停诊次数等。

财务数据统计：应统计互联网医院医师服务订单包括预约挂号以及医嘱诊断等订单的收入情况，便于线上与线下医疗收支情况分析以及医师的绩效考核。

5.6.6.2 扩展要求

业务数据分析：宜支持互联网医院所涉及的业务数据汇总分析。

医师/药师数据分析：宜支持医师/药师互联网医院服务数据分析。

患者数据分析：宜支持互联网医院患者的数据统计分析。

病种数据分析：宜支持根据病种进行患者数据统计分析。

服务评价分析：宜支持针对互联网医院科室、医师等的满意度评价进行统计分析。

5.6.7 监管数据上传

5.6.7.1 基本要求

监管数据上传：互联网医院应接入北京市医疗服务与执业监管平台，并按照要求完成数据上传，接受管理机构的实时监管。

5.6.7.2 扩展要求

数据质量监控：系统宜支持对上传数据的有效性、完整性、一致性进行校验，并对其数据质量进行实时监控。

区块链数据同步：有条件的机构可应用区块链技术实现患者诊疗数据、医院运营数据等关键监管数据信息的上链并同步，实现穿透式全流程智慧监管及全过程追溯。

5.6.8 服务评价管理

5.6.8.1 扩展要求

患者评价：宜支持患者在问诊结束后对医院、科室、医师进行满意度评价。

查看评价：患者端宜支持显示当前发出的评价，医护端宜支持显示所有可看的评价。

处理评价：宜设置待处理显示、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。

评价设置：宜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的统一管理。

投诉处理：宜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。

5.6.9 黑名单管理

5.6.9.1 扩展要求

黑名单管理：系统宜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。爽约记录达到一定次数以上，或有异常预约挂号行为的，可进入黑名单，宜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。

人工解封：系统宜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。

6 安全规范

6.1 基本要求

6.1.1 安全设计原则

根据各医疗机构的技术实现方式，互联网医院信息系统在网络安全等级保护定级时，可作为独立的信息系统进行备案，也可作为医院信息系统的子系统进行备案。

互联网医院信息系统的运营、使用单位为网络与信息系统安全相关责任主体，应根据第三级信息安全保护等级选择基本安全措施，进行安全整体规划和安全方案设计，并依据风险分析的结果补充和调整安全措施。

互联网医院信息系统的建设和运行维护单位应做好网络与信息系统安全工作，制定应急预案并进行培训和演练，保障网络与信息系统安全可靠运营。

6.1.2 总体框架

互联网医院安全体系总体框架设计要求包括：

（1）互联网医院安全体系从通用要求、扩展要求进行框架设计；

（2）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；

（3）应从云计算安全层面实现安全扩展要求；

（4）应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。

6.1.3 安全物理环境

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。

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

存放服务器的机房应当具备双路供电或紧急发电设备。

6.1.4 安全通信网络

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。

开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）。

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10Mbps，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。

6.1.5 安全区域边界

应在互联网医院信息系统网络边界设置访问控制规则，默认情况下除允许通信受控接口外拒绝所有通信。

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。

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。

应采取欺骗诱捕技术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。

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。

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。

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。

6.1.6 安全计算环境

应对互联网医院信息系统的运行和操作日志进行监控管理，通过数据库审计系统等安全设备对数据库进行安全审计。

具有医学文书效力的资料，如病历、处方等，需要附加接诊医师的电子签名和可靠时间戳。

电子处方的修改，应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。

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。

宜采用符合GM/T 0028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。

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。

6.1.7 管理要求

应对互联网医院运营过程中的各类管理内容建立安全管理制度，应包括互联网医疗服务管理制度、互联网医院信息系统使用管理制度、互联网医疗质量控制和评价制度、在线处方管理制度、患者知情同意与登记制度、在线医疗文书管理制度、在线复诊患者风险评估与突发状况预防处置制度、人员培训考核制度，停电、断网、设备故障、网络信息安全等突发事件的应急预案。

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。包括但不限于：患者未在实体医疗机构就诊时，医师通过互联网医院只能为部分常见病、慢性病患者提供复诊服务；不得开具麻醉药品、精神药品等特殊管理药品处方；为低龄儿童(6岁以下)开具儿童用药处方时，应确认患儿有监护人和相关专业医师陪伴；在线诊断、处方必须有电子签名；不良事件上报；相关人员培训等。

应在管理制度中明确规定医疗数据存储、访问策略、操作留痕等。

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、权利和义务。

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《信息安全技术个人信息安全规范》的规定。

宜在医护端接诊界面设置医护人员姓名及工作编码的水印，在患者端设置患者姓名的水印，并在截屏时进行个人隐私保护相关提示。

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；临床科室应与所依托的实体医疗机构临床科室保持一致。

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。

应有专人负责互联网医院信息系统运维等技术服务，确保系统稳定运行。

6.2 云计算要求

应确保互联网医院信息系统所在云计算平台的运维地点位于中国境内。

应确保与云服务商签订保密协议，明确云服务商的责任、权利和义务，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。

应在互联网医院信息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。

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。

应确保互联网医院相关数据存储于公有云时，对医疗数据进行加密处理。

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。

6.3 客户端应用软件安全要求

6.3.1 安全计算环境

客户端应用软件，如互联网医院APP、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。

6.3.1.1 程序安全

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。

应具备身份认证控制和认证失败策略。
应采用两种或两种以上的要素对用户身份进行认证。
应具备会话超时后要求重新鉴权的机制。
应配合服务端提供口令复杂度校验功能。
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。
应保证安装文件中不包含任何冗余文件和冗余说明。
应保证安装文件中不包含明文证书、密钥、网络配置等信息。
应避免使用存在已知漏洞的第三方组件。
应具备客户端应用软件运行环境检测能力。

6.3.1.2 通信安全

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。
客户端应用软件与服务器应进行双向认证。

6.3.1.3 数据安全

应保证登录口令、支付密码及其他输入的敏感信息，不以明文显示。
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。
应采用自定义权限保护组件访问。
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。
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。
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。
应支持页面返回、进入后台后，自动清除已输入的敏感信息。
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。

6.3.2 安全建设管理

客户端应用软件的运营机构，应按照《中华人民共和国网络安全法》及GB/T 25000.51-2016的要求，加强客户端应用软件自身的安全开发工作，在客户端应用软件的版本更新过程中，始终遵循安全标准的要求。应加强客户端应用软件的安全保障体系建设，建立客户端应用软件的事前检测、事中监测、事后追溯的全生命周期管理。针对各种类型互联网医院如APP、公众号、小程序等应进行主动、持续、动态的风险业务识别、侦测和分析，达到风险识别、预警、处置的风控闭环控制，保证应用在移动客户端运行的安全性和合规性，全面提升移动互联网业务风险防控水平。

可对互联网医院所运行的移动应用做资产归集管理，明确资产所有人、使用人、开发人，移动应用资产所包含的软件版本、内嵌SDK和相关软件资产信息。

6.3.2.1 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。

6.3.2.2 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。

7 质量要求

7.1 功能要求

互联网医院信息系统应满足第5章功能规范中所列出的全部基本要求，适用范围可依据互联网医院业务开展情况而定。

建议互联网医院达到第5章功能规范中所列出的扩展要求。

互联网医院应与北京市医疗服务与执业监管平台对接，并满足北京市医疗服务与执业监管平台数据接口要求。

互联网医院信息系统软件产品应在功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性等方面满足GB/T 25000.51-2016的要求。

7.2 安全要求

互联网医院信息系统应按照GB/T 22239-2019、GB／T 28448-2019等要求定期进行第三级网络安全等级保护测评和安全测评，并满足第6章互联网医院安全规范要求。

互联网医院信息系统应按照GB/T 18336.2-2015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。

客户端应用软件应满足6.3中所列出的安全要求。

7.3 性能要求

互联网医院信息系统应具有支撑处理高峰期业务多用户并发压力的能力，如典型业务、复杂业务流程、频繁的用户操作等业务场景。

互联网医院信息系统应满足业务运行的性能需求，保障业务的交易成功率和系统可用性，并发成功率为100%，交易成功率大于99%。

互联网医院信息系统在运行过程中CPU平均利用率不大于85%。

互联网医院信息系统应具有压力解除后的自恢复能力。

参 考 文 献

[1] 国卫办医发〔2017〕8号 电子病历应用管理规范（试行）
[2] 国卫医发〔2018〕25号 关于印发互联网诊疗管理办法（试行）等3个文件的通知
[3] 卫医管发〔2010〕28号 医院处方点评管理规范（试行）
[4] 卫医发〔2002〕193号 医疗机构病历管理规定
[5] 北京市互联网医院审核细则（试行）