|  |  |
| --- | --- |
| ICS  | 11.020 |
| CCS  | C 07 |

|  |
| --- |
| WS |

中华人民共和国卫生行业标准

WS/T XXXXX—XXXX

互联网医疗健康信息安全管理规范

Internet Health and Medical Information Security Management Guideline

（征求意见稿）

XXXX - XX - XX发布

XXXX - XX - XX实施

中华人民共和国国家卫生健康委员会  发布

目次

[前言 II](#_Toc71299066)

[1 范围 1](#_Toc71299067)

[2 规范性引用文件 1](#_Toc71299068)

[3 术语和定义 1](#_Toc71299069)

[4 总则 2](#_Toc71299078)

[5 互联网医疗健康信息安全管理总体框架 2](#_Toc71299079)

[6 互联网医疗健康信息安全相关方职责 3](#_Toc71299080)

[6.1 建设方职责 3](#_Toc71299081)

[6.2 服务方职责 3](#_Toc71299082)

[6.3 运营方职责 3](#_Toc71299083)

[6.4 监管方职责 3](#_Toc71299084)

[7 互联网医疗健康信息安全过程管理 4](#_Toc71299085)

[7.1 建设过程管理 4](#_Toc71299086)

[7.2 服务过程管理 4](#_Toc71299087)

[7.3 运营过程管理 4](#_Toc71299088)

[7.4 监管过程管理 4](#_Toc71299089)

[8 互联网医疗健康信息安全数据管理 5](#_Toc71299090)

[8.1 采集数据管理 5](#_Toc71299091)

[8.2 存储数据管理 5](#_Toc71299092)

[8.3 传输数据管理 5](#_Toc71299093)

[8.4 应用数据管理 5](#_Toc71299094)

[8.5 销毁数据管理 5](#_Toc71299095)

[9 互联网医疗健康信息安全技术管理 6](#_Toc71299096)

[9.1 8.1 信息系统安全管理 6](#_Toc71299097)

[9.2 第三方接入安全管理 6](#_Toc71299098)

[9.3 个人信息安全管理 6](#_Toc71299099)

[10 互联网医疗健康信息安全组织管理 6](#_Toc71299100)

[10.1 制度管理 6](#_Toc71299101)

[10.2 人员管理 7](#_Toc71299102)

[10.3 应急管理 7](#_Toc71299103)

[参考文献 8](#_Toc71299104)

1. 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。

本文件起草单位：

本文件主要起草人：

互联网医疗健康信息安全管理规范

* 1. 范围

本文件规定了互联网医疗健康信息安全管理总体框架、信息安全相关方管理、信息安全过程管理、信息安全数据管理、信息安全技术管理和信息安全组织管理的规范和安全要求。

本文件适用于组织、个人在中华人民共和国境内开展互联网医疗健康活动所遵循信息安全管理。

* 1. 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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448 信息安全技术 网络安全等级保护测评要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 370448 信息安全技术 物联网安全参考模型及通用要求

GB/T 37973 信息安全技术 大数据安全管理指南

* 1. 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

* + 1.

互联网医疗健康服务 internet medical and health services

应用互联网及相关信息技术提供的互联网医疗服务、互联网公共卫生服务、互联网家庭医生签约服务、互联网药品供应保障服务、互联网医疗保障结算服务、互联网医学教育和科普服务、互联网人工智能应用服务等。

* + 1.

互联网医疗健康信息系统internet medical and health information system

应用信息化技术，支撑互联网医疗健康服务、运营与监管业务开展，产生互联网医疗健康信息，为互联网医疗健康服务过程以及管理和决策提供支持的信息系统。为服务过程、完成后实际交付使用的、对外提供互联网医疗健康服务的整套系统，包括计算机硬件、软件、网络等总称。

* + 1.

互联网医疗健康信息安全管理 internet medical and health information security management

国家和地方网信部门、卫生健康主管部门、医疗卫生机构及其他相关企业和机构，在互联网医疗健康服务开展过程，在应用建设、运营管理和信息管理等阶段，应用合理的技术与管理手段，保障信息安全的管理过程。

* + 1.

建设方 construction organization

建设方是指互联网医疗健康信息系统的建设责任主体。建设方可自行负责或委托第三方开展互联网医疗健康信息系统的建设、互联网医疗健康服务运营。

* + 1.

服务方 server organization

服务方是指互联网医疗健康服务的提供主体和责任承担主体。服务方负责保障互联网医疗健康信息安全。

* + 1.

运营方 operation organization

运营方是指互联网医疗健康服务的运营责任承担主体。运营方负责互联网医疗健康信息系统维护和互联网医疗健康服务运营等，维护系统稳定运行，保障服务稳定开展、推动服务合法合规有序发展的工作内容。

* + 1.

监管方 regulator

监管方是指县级以上卫生健康行政部门。监管方负责对本行政区域内互联网医疗健康信息安全管理监管。

* + 1.

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息。

* 1. 总则

互联网医疗健康的信息安全管理是互联网医疗健康信息系统建设、服务、运营与监管活动过程中的信息安全管理。

互联网医疗健康信息安全管理应确保互联网医疗健康信息系统的合规性、可用性和安全性；确保互联网医疗健康信息采集、存储、传输、应用、销毁等全生命周期的信息处理合法、正当、必要的原则，不得过度处理，保障信息完整、保密，保护个人信息安全、公众利益和国家安全。

互联网医疗健康信息安全管理应坚持与现有法律法规与政策标准一致性。对于民法典、网络安全法、网络安全等级保护条例，及其他信息安全相关法律法规与政策标准要求已覆盖内容，本文件不再作规定。

* 1. 互联网医疗健康信息安全管理总体框架

互联网医疗健康信息安全管理总体框架图如图1所示。



1. 互联网医疗健康信息安全管理总体框架图
2. 互联网医疗健康信息安全相关方管理：互联网医疗健康信息安全管理明确建设方、服务方、运营方和监管方主体责任；
3. 互联网医疗健康信息安全过程管理：互联网医疗健康信息安全管理保障建设、服务、运营和监管全过程的信息安全；
4. 互联网医疗健康信息安全数据管理：互联网医疗健康信息安全管理明确数据在采集、存储、传输、应用和销毁等过程的信息安全要求；
5. 互联网医疗健康信息安全技术管理：互联网医疗健康信息安全管理明确互联网医疗健康信息系统在应用安全、第三方接入安全和个人信息安全等方面需要遵从的安全规范；
6. 互联网医疗健康信息安全组织管理：遵照国家相关安全标准规范体系要求，明确组织要求安全事件管理要求。
	1. 互联网医疗健康信息安全相关方职责
		1. 建设方职责

建设方是互联网医疗健康信息系统建设和管理的责任主体，是信息安全管理的第一责任方。建设方应当履行下列互联网医疗健康信息安全保护义务：

1. 制定互联网医疗健康信息安全工作的总体方针和安全策略，阐明安全工作的总体目标、范围、原则和安全框架等，确定互联网医疗健康信息安全责任人，落实互联网医疗健康信息安全保护责任；
2. 在自行承担或引入第三方机构开展建设、服务与运营时，负责指导与管理服务方与运营方遵照安全管理要求开展相关工作；
3. 建立互联网医疗健康信息安全应急体系，制定应急预案，组建应急队伍、开展应急演练；
4. 接受上级业务主管、信息安全监管部门的安全审查和监管。
	* 1. 服务方职责

服务方是互联网医疗健康服务提供的责任主体，是互联网医疗健康信息的主要产生方，是服务过程相关信息安全责任方。服务方应当履行下列互联网医疗健康信息安全保护义务：

1. 按照相关规范要求开展互联网医疗健康信息服务，包括服务机构与服务人员的执业资质规范、服务过程安全规范、服务结果可追溯；
2. 服务人员开展互联网医疗健康服务过程中，应遵循信息安全管理要求，有义务保障服务对象个人隐私；
3. 配合建设方，完成网络安全事件、突发信息安全事件的管理与处置；
4. 接受上级业务主管、信息安全监管部门的安全审查和监管。
	* 1. 运营方职责

运营方是互联网医疗健康服务运营和信息系统维护责任主体，是运营过程相关信息安全责任方。运营方应当履行下列互联网医疗健康信息安全保护义务：

1. 应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障互联网医疗健康信息系统及网络安全、稳定运行；
2. 有效应对信息安全事件，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，防范信息安全违法犯罪活动，维护互联网医疗健康信息数据的完整性、保密性和可用性；
3. 接受上级业务主管、信息安全监管部门的安全审查和监管。
	* 1. 监管方职责

监管方是对本行政区域内互联网医疗健康服务开展的监管主体，是监管过程相关信息安全责任方。监管方应当履行下列互联网医疗健康信息安全保护义务：

1. 对互联网医疗健康服务准入信息安全监管，包括机构执业资格、服务人员执业资格、互联网医疗健康服务范围的执业资格等信息的真实性、完整性；
2. 对互联网医疗健康服务过程信息进行监管，包括服务过程中形成的文字、视频、音频等内容信息的真实性、完整性、不可否认性；
3. 对个人信息保护进行监管，包括信息采集知情告知与授权许可，信息传输与存储加密，以及信息脱敏使用、信息授权公开等；
4. 对互联网医疗健康服务质量进行监管，包括投诉、举报的公正性、及时性，以及处理结果告知投诉、举报人等。
	1. 互联网医疗健康信息安全过程管理
		1. 建设过程管理

建设方开展互联网医疗健康信息系统建设和管理活动时，应满足以下要求：

1. 建立健全互联网医疗健康信息安全管理体系和相关管理制度。明确互联网医疗健康信息安全管理相关岗位设置、工作要求与责任义务。包括但不限于安全管理制度、安全审核检查制度、安全岗位、人员管理制度，组织相关方完成突发事件的应急预案制定并落实应急演练。
2. 互联网医疗健康信息系统应通过网络安全等级保护三级测评和定期复评。互联网医疗健康信息系统集成第三方服务应用时，第三方服务也需要达到相关安全防护水平。
3. 互联网医疗健康服务过程与运营过程中收集和产生的个人信息和重要数据应当在境内存储。
4. 因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估，法律、行政法规另有规定的，依照相关规定管理。
5. 建设方有义务配合公安机关、网安部门和相关机构提供技术支持和协助，并按照规定向有关主管部门报告。
6. 对各项操作行为进行审计，审计范围应覆盖到每个用户，并对业务审批人员、监管人员等重要用户行为和重要安全事件进行审计，并对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
	* 1. 服务过程管理

服务方开展互联网医疗健康服务活动时，应满足以下要求：

1. 对服务对象与服务人员的个人隐私信息进行保护；
2. 建立信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关信息安全的投诉和举报；
3. 医务人员开展互联网医疗健康服务过程中，应根据相关管理要求使用数字证书和电子签名技术。
	* 1. 运营过程管理

运营方开展互联网医疗健康运营活动时，应满足以下要求：

1. 运营方及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。第三方运营方应签署信息隐私保密协议。
2. 第三方机构依托实体医疗机构开展互联网医疗健康业务的，必须通过协议、合同等方式明确各方在医疗服务、信息安全、隐私保护等方面的职责权利。
	* 1. 监管过程管理

监管方开展互联网医疗健康服务监管活动时，应至少包含以下工作内容：

1. 互联网医疗健康信息系统是否开展网络安全等级保护三级测评工作；
2. 监管方及其工作人员，必须对在履行职责中知悉的互联网医疗健康信息严格保密，不得泄露、出售或者非法向他人提供；
3. 应对互联网医疗健康服务相关建设方、服务方与运营方的互联网医疗健康信息安全执行效果开展监督管理。监督方式可包括信息及网络安全审计、互联网医疗健康信息系统安全漏洞扫描、系统与网络安全测试和信息安全事件处理监督等。监督工作可根据实际条件建立巡查抽查机制和行业监测预警机制；
4. 对互联网医疗健康服务相关方不满足信息安全管理要求，可根据情节严重程度，采取警告、通告批评、停服整顿、停止互联网医疗健康服务资格等处罚措施。
	1. 互联网医疗健康信息安全数据管理
		1. 采集数据管理

互联网医疗健康服务过程中，采集数据时应满足以下要求：

1. 应符合GB/T 35273的相关要求；
2. 个人信息收集、使用应遵循合法、正当、必要的原则；
3. 应公开收集、使用规则，明示收集、使用信息的目的、方式和范围；
4. 采集数据需经被收集者、监护人或授权人同意。采集个人图像、个人身份特征信息等敏感个人信息，需要告知个人必要性以及对个人影响，经过被收集者、监护人或授权人单独授权同意；
5. 不得收集与提供服务无关的个人信息。
	* 1. 存储数据管理

互联网医疗健康服务过程中，存储数据时应满足以下要求：

1. 应符合GB/T 35273的相关要求，以及GB/T 22239第三级安全要求；
2. 应依照法律、行政法规的规定，使用管理、物理和技术措施来保护互联网医疗健康信息免遭未经授权的访问、泄露或破坏。
3. 应确保存储数据的保密性、完整性，采用密码技术和校验技术保证存储过程中敏感信息或整个数据集的保密性、完整性，确保不被窃取、不被篡改。
4. 对互联网医疗健康服务过程的电子病历资料，遵循电子病历应用管理相关要求。
5. 应保留系统安全日志、访问日志、操作日志等，保证相关日志保存不少于六个月。
	* 1. 传输数据管理

互联网医疗健康服务过程中，传输数据的要求：

1. 应符合GB/T 35273的相关要求，以及GB/T 22239第三级安全要求；
2. 应确保信息传输的保密性、完整性，采用密码技术和校验技术保证传输过程中敏感信息或整个数据集的保密性、完整性，确保不被窃取、不被篡改。
3. 应满足图像、声音、文字以及诊疗所需信息的安全，图像清晰、数据准确。
4. 应满足临床诊疗要求，符合相关技术标准和规范要求。
	* 1. 应用数据管理

互联网医疗健康服务过程中，应用数据的要求：

1. 应符合GB/T 35273的相关要求，以及GB/T 22239第三级安全要求；
2. 不得违反法律、行政法规的规定和双方的约定收集、使用个人信息；
3. 未经相关部门许可，所采集的互联网医疗健康服务相关个人信息不得公开或向他人提供；
4. 应使用权限控制和访问日志记录等适宜的安全技术方式，对系统信息的访问、输入、修改、删除进行管理，防止内部非授权人员及其他人员未经授权获取个人信息；
5. 应对信息发布内容进行监管，发现法律法规禁止发布或者传播的信息，应当立即停止传播该信息，采取警示、限制功能、暂停更新、关闭账号等必要处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告；
6. 应支持敏感信息在第三方对接的授权使用，包括电子处方流转平台、医疗商用保险公司、电子处方配送企业及相关互联网医疗健康合作方，无本人或监护人、委托代理人授权许可，不得开放个人敏感信息使用。
	* 1. 销毁数据管理

互联网医疗健康服务过程中，销毁数据的要求：

1. 应符合GB/T 35273的相关要求；
2. 服务方停止互联网医疗健康服务时，应及时停止继续收集个人信息，对其持有的个人信息进行删除或删除处理；
3. 第三方运营承接方在停止运营服务时，有义务将历史服务数据以安全可利用的方式向建设方提供；
4. 因建设方、运营方违反法律法规规定，或违反与个人信息主体的约定，收集、使用、公开披露或向第三方共享、转让个人信息的，个人信息主体要求删除的，应及时删除、停止公开披露、停止向第三方共享、转让的行为，并要求第三方及时删除；
5. 个人信息主体申请注销账户时，经身份核验后，按信息存储相关规定期限后，删除或匿名化处理历史互联网医疗健康相关个人信息。
	1. 互联网医疗健康信息安全技术管理
		1. 8.1 信息系统安全管理

互联网医疗健康信息系统应满足以下安全要求：

1. 应符合GB/T 35273的相关要求，以及GB/T 22239第三级安全要求；
2. 应具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护数据的保密性、完整性、可用性；
3. 应具备基于数字证书的身份认证功能。在面向患者提供实名认证功能时，应符合国家相关规范要求，保护个人身份信息、生物识别信息等，防止泄露；
4. 应支持“最小授权”、“职责分离”、“角色分离”、“默认拒绝”等原则构建系统敏感数据的访问控制、权限控制以及授权控制策略；
5. 应保障患者互联网医疗健康服务的权益，确保服务记录、服务流程可追溯；
6. 互联网医疗健康相关移动端应用，应在可靠的应用渠道发布。建设方需要定期对移动应用进行监控，对于仿冒、钓鱼类应用的出现及时通知应用渠道管理方进行下架处理；
7. 互联网医疗健康相关移动端应用，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序。
	* 1. 第三方接入安全管理

互联网医疗健康信息系统与第三方信息系统对接应满足以下要求：

1. 根据业务开展需要，互联网医疗健康信息系统与包括医疗、医保、医药、商保、物流、公安等第三方信息系统对接时，应遵循国家法律法规及行业相关第三方产品或服务接入管理机制进行接入管理和信息安全管理。
2. 对第三方应用互联网医疗健康信息时，应通过相关部门审核同意，遵循最小原则，控制信息使用范围。建设方应与第三方签署隐私保护协议和数据使用协议，确保信息使用安全合规。
3. 对接全程应遵循相关信息安全管理要求。
	* 1. 个人信息安全管理

互联网医疗健康信息系统应满足以下个人信息安全管理要求：

1. 应遵循网络安全保护法、民法典等法律法规，以及GB/T 35273的相关要求；
2. 开发具有处理个人信息功能的服务时，宜在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，保证在系统建设时对个人信息保护措施同步规划、同步建设和同步使用；
3. 应具备个人信息隐私保护能力，包括但不限于：数据权限控制、个人信息去标识化、数据加密、安全审计等，并落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。
	1. 互联网医疗健康信息安全组织管理
		1. 制度管理

在开展互联网医疗健康信息安全制度管理时，应满足以下要求：

1. 应对互联网医疗健康服务的各类信息安全管理内容建立适宜的安全管理制度、安全影响评估制度等；
2. 应制定互联网医疗健康信息安全策略；
3. 应建立互联网医疗健康信息安全管理的组织和岗位，根据相关政策和规范要求，明确具体管理组织职责和岗位要求，明确汇报决策机制；
4. 应定期对互联网医疗健康信息安全管理工作进行全面自查，并作出整改建议。
	* 1. 人员管理

在开展互联网医疗健康信息安全人员管理时，应满足以下要求：

1. 应建立互联网医疗健康信息安全管理领导人负责制，主管领导是网络信息与数据安全第一负责人，分管领导是直接责任人；
2. 应划分不同的管理员角色进行互联网医疗健康信息安全管理，明确各个角色的责任和权限；
3. 应定期开展互联网医疗健康信息安全教育与培训，确保相关人员具备信息安全保护能力；
4. 应与从事互联网医疗健康信息处理岗位上的相关人员签署保密协议，进行安全审查，明确安全职责。对第三方组织和个人，涉及互联网医疗健康信息处理业务，应签署保密协议，并要求履行保密义务。
	* 1. 应急管理

在开展互联网医疗健康信息安全应急管理时，应满足以下要求：

1. 应制定互联网医疗健康信息安全事件应急预案，落实岗位职责，并及时对应急预案进行维护和更新；
2. 应定期（至少每年一次）组织相关人员进行应急响应培训和应急演练；
3. 应根据事件影响，区分信息安全事件严重等级，根据不同等级采取不同应急处置及上报程序。

参考文献

[1]《关于促进和规范健康医疗大数据应用发展的指导意见》

[2]《中华人民共和国人类遗传资源管理条例的》

[3]《中华人民共和国网络安全法》

[4]《人工智能辅助治疗技术管理规范（试行）》

[5]《中华人民共和国个人信息保护法 （草案）》

[6]《电子病历应用管理规范（试行）》

[7]《互联网诊疗管理办法（试行）》

[8]《互联网医院管理办法（试行）》

[9]《远程医疗服务管理规范（试行）》

[10]《“互联网+护理服务”试点工作方案》

