北京市卫生健康大数据与政策研究中心
Beijing Municipal Health Big Data and Policy Research Center
北京市医院管理研究所
Beijing Institute of Hospital Management

互联网诊疗患者个人信息保护制度（范本）

[2023版]

二〇二三年 九月

北京市卫生健康大数据与政策研究中心 编

编者名单

主编： 琚文胜

编写专家： 郑攀、尚邦治、潘轶竹、闫雪

编写成员： 张世红、白玲、史森、衡爽、杨小冉

为加强互联网诊疗服务中患者个人信息和隐私保护，维护患者合法权益，规范医务人员对用户个人信息及隐私的保护行为，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国医师法》、《民法典》、《信息安全技术个人信息安全规范》、《互联网信息服务管理办法》、《关于印发互联网诊疗管理办法（试行）等 3 个文件的通知》、《互联网诊疗监管细则（试行）》等有关规定，制定本制度。

（一）本制度所称的互联网诊疗患者个人信息，是指患者在互联网诊疗服务过程中产生的能够单独或者与其他信息结合识别特定自然人（患者）的各种信息。其中，自然人（患者）的私人生活安宁和不愿为他人知晓的私密信息为患者隐私信息。个人信息主要包括个人基本信息（含姓名、肖像、身份证号、手机号、家庭住址等）、检查检验报告、病历记录、诊疗对话等。

（二）医务人员、管理人员和技术人员等人员在处理（收集、存储、使用、加工、传输、提供、公开等）个人信息时，应当按照法律法规有关规定，遵循合法、正当、必要和诚信原则，依法保护患者的个人信息及隐私安全。不得非法收集、使用、加工、传输、买卖、提供或者公开他人个人信息。

（三）医务、信息安全和技术部门应当采取必要的管理和技术措施，确保个人信息安全和信息质量，并防止未经授权的访问以及个人信息泄露、篡改、丢失。

（四）发生或者可能发生个人信息泄露、篡改、丢失的，有关人员应当及时采取补救措施，并告知医院信息安全部门（或负责人），同时，按照规定要求履行患者告知义务。构成网络安全事件的，按照规定报告有关主管部门。

（五）处理患者个人信息应当取得患者知情同意，法律法规规定的情形除外。做好患者告知服务，与患者在线签订《互联网医疗服务协议》及《个人隐私保护协议》。

（六）医务人员收集患者的个人信息及医疗健康信息，应符合医学诊疗规范且有助于帮助用户解决疾病和健康问题，不应要求患者提供疾病和健康问题之外的无关信息。

（七）访问权限管理

1.按照最小可用原则进行患者个人信息数据访问授权。医务部门（或病案管理等有关部门）负责数据使用的权限管理，根据不同人员的业务和管理情况授予不同的访问权限。

2.医务人员可在授权范围内调阅使用患者个人信息和医疗健康信息。非授权范围的个人信息使用应当经过医务部门（或相关部门）审批并做好数据使用的记录管理，必要时对个人信息采取脱敏处理。

3.对涉及患者隐私的病历书写和调阅，除相关诊疗人员因医疗活动需要外，其他人员不得进行。应用者（包括提供服务医生、药师、科室管理员、管理部门等）如需调阅涉及个人隐私病历的，需经医务部门（或相关部门）审批通过，并做好数据使用的记录管理，必要时对个人隐私信息采取脱

敏处理。

（八）所有接触到个人信息人员应签订个人信息保护承诺书。

（九）参加互联网诊疗的医务人员登录系统需进行双因素身份认证（至少包括登录口令、短信验证码、生物特征识别(人脸和指纹等)信息、电子签名 USBkey 等中的两个因素）。

（十）就诊人添加需实名认证，如身份证、医保卡、生物特征识别等，可与公安认证或线下实名认证对接实现。

（十一）所有用户应妥善保存好账户和口令，不得以任何理由任何方式将账户转让、借与他人使用。如因账户、口令、手机和电脑被借用造成个人信息泄露，当事人须承担相关责任。

（十二）未经患者本人授权（法律法规规定不需本人同意的情况除外），所有用户不得向任何人提供互联网诊疗信息系统能查看到的个人信息及医疗健康信息。所有用户不得以复制、下载、截屏、拍照或其他方式存储、处理、传输包含个人信息、诊疗信息等图文数据。

（十三）定期（每年至少一次）开展个人信息保护法律法规、政策制度等相关知识培训，提高服务和技术人员的安全保护和风险防范意识。

（十四）建立和健全先进实用、完整可靠的信息安全体系，加强互联网诊疗服务的信息管理和数据安全防护。采取技术手段，保证数据存储、传输和应用的安全，保证互联网

诊疗服务产生的数据的访问、修改、下载等记录全程留痕、可追溯，并做好日常管理和监督。

（注：本制度只是范本，医疗机构可根据本机构具体情况进行裁剪修改、完善细化）