君合研究简讯

JUNHE

2022 年 11 月 9 日

网络安全法律热点问题

《医疗卫生机构网络安全管理办法》要点解读

2022 年 8 月 8 日，国家卫生健康委员会、国家中医药管理局、国家疾病预防控制局发布了《医疗卫生机构网络安全管理办法》（以下简称《管理办法》）。《管理办法》旨在指导各级医疗卫生机构开展网络安全管理工作，推动《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》等相关法律法规在“互联网+医疗健康”领域的具体落实。

《管理办法》主要从网络安全和数据安全两个角度进行规范，同时也对医疗卫生机构应对网络安全风险事件、构建相关管理保障提出了具体要求。在此，我们将对《管理办法》中的规定要点进行梳理和解读，为医疗卫生机构开展网络安全和数据合规提供一些思路。

一、《管理办法》的适用范围和监管框架

在适用主体方面，《管理办法》适用于各医疗卫生机构运营网络的安全管理，包括未纳入区域基层卫生信息系统的基层医疗卫生机构。

在适用对象方面，《管理办法》关注的是医疗卫生机构运营的网络信息系统，和医疗卫生机构通过网络处理的各种电子数据，例如业务数据、医疗设备数据、个人信息及其数据衍生物。

在《管理办法》下，由国家卫生健康委员会、国家中医药管理局、国家疾病预防控制局负责统筹规划、指导、评估、监督医疗卫生机构的网络安全工作，县级以上地方卫生健康行政部门负责本行政区域内的指导监督工作。

二、医疗卫生机构的网络安全管理要求

基于现有的医疗健康相关法规、政策和国家标准，《管理办法》主要从如下几个方面，对医疗卫生机构的网络安全管理工作提出了具体要求：

1、在组织架构上强化责任制

各医疗卫生机构应成立网信工作领导小组，在网络建设过程中明确各网络的主管部门、运营部门、信息化部门、使用部门等管理职责。对于有二级及以上网络的医疗卫生机构，应明确负责网络安全管理工作的职能部门，以及安全主管、安全管理员等岗位职责。

2、落实网络安全等级保护定级、备案、测评、安全建设整改等工作

（1）定级：新建网络应在规划和申报阶段确定网络安全保护等级。

（2）备案：第二级以上网络应在定级后 10 个工作日内向公安机关备案，并将备案情况报上级卫

生健康行政部门。

（3）测评：新建网络应在上线运行前进行安全性测试；第二级的网络应委托等保测评机构定期测评，涉及 10 万人以上个人信息的网络至少三年开展一次测评，其他网络至少五年开展一次测评；第三级或第四级的网络应委托等保测评机构每年至少 1 次开展测评。

3、每年开展网络安全自查整改工作

包括开展文档核验、漏洞扫描、渗透测试等多种形式的安全自查，对信息资产进行梳理，根据自查结果进行整改并向有关监管机构报备。

4、对关键信息基础设施运营者的要求

如医疗卫生机构属于关键信息基础设施运营者，应对安全管理机构负责人和关键岗位人员进行安全背景审查。

5、加强安全管控措施、网络监测及备份

各医疗卫生机构需要加强运维现场的物理安全防护措施和通过互联网远程运维的安全管控措施，持续监测网络运行状态。特别地，第三级及以上的网络应保障关键链路、关键设备冗余备份，有条件时应建立应用级容灾备份。

6、加强网络全链条参与者的安全管理

医疗卫生机构还应关注整个网络全链条参与者的安全管理，包括采购的第三方网络产品和服务、医疗设备、运维服务等，定期进行检查和评估，防止第三方安全事件的发生。

7、对特定事项的安全风险评估

《管理规定》专门提到，医疗卫生机构在应用大数据、人工智能、区块链等新技术开展服务时，应在上线前开展安全风险评估并进行安全管控。此外，对废止网络及其相关设备也应当进行风险评估，确保其中的数据得到安全处置。

三、医疗卫生机构的数据安全管理要求

从数据安全的角度，《管理办法》主要从如下几个方面，对医疗卫生机构提出了具体要求：

1、在组织架构上强化责任制

各医疗卫生机构应建立数据安全管理组织架构，明确数据管理部门、业务部门、信息化部门在数据安全管理全生命周期中的权责。

2、开展数据资产管理

各医疗卫生机构应每年对数据资产进行全面梳理，依据数据的重要程度以及遭到破坏后的危害程度对数据进行分类分级。

3、履行数据安全保障义务

包括建立健全内部数据安全管理制度、操作规程及技术规范，开展数据安全风险评估，组织数据安全教育培训，建立完善数据使用申请及批准流程等。

4、加强数据全生命周期安全管理

（1）收集：加强数据收集合法性管理，在收集过程中采取数据脱敏、数据加密、链路加密等防控措施。

（2）传输：明确不同安全级别数据的加密传输要求，加强传输过程中的接口安全控制。

（3）存储：各医疗卫生机构应在境内存储数据，并采取备份、加密等安全措施，在涉及云上存储时应进行安全风险评估。

（4）向境外提供：原则上，数据全生命周期活动应在境内开展。因业务确需向境外提供的，应当进行安全评估或审核，在影响或者可能影响国家安全时还需提交国家安全审查。

（5）使用权限：各医疗卫生机构应加强数据使用的权限范围管理和批准流程管理，防止数据越权使用、超范围使用、未经批准传递至部门外或泄露。

（6）发布共享：各医疗卫生机构应对此进行安全风险评估，数据上报的提出方应确定上报范围和上报规则。

（7）数据销毁：应采用确保数据无法还原的销毁方式，重点关注数据残留风险及数据备份风险。

5、对人脸识别技术应用的特殊要求

值得注意的是，《管理办法》针对医疗卫生机构开展人脸识别或人脸辨识的场景，提出了如下几项更加细化的管理要求：

- 应同时提供非人脸识别的身份识别方式，不得因数据主体不同意收集人脸识别数据而拒绝其使用基本业务功能
- 人脸识别数据不得用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等
- 采取安全措施存储和传输人脸识别数据，例如加密存储和传输
- 采用物理或逻辑隔离方式分别存储人脸识别和个人身份信息

四、应对网络安全风险和安全事件的要求

如医疗卫生机构的网络安全管理工作不到位，将存在网络漏洞隐患、网络安全风险增大的可能性，以及发生个人信息和数据泄露、毁损、丢失和网络系统遭攻击、入侵、控制等网络安全事件的可能性。如上述情况发生时，《管理办法》要求各医疗卫生机构应当：

（1）立即启动应急预案，采取必要的补救和处置措施；

（2）及时以电话、短信、邮件或信函等多种方式告知相关主体；

（3）及时向卫生健康行政部门、公安机关等主管部门报告，做好现场保护、留存相关记录，为监管部门依法开展调查活动提供技术支持和协助。

此外，如监管机构在检查过程中发现医疗卫生机构存在网络安全漏洞和隐患等问题，医疗卫生机构应及时整改，杜绝重大网络安全事件发生。

为更好地应对网络安全风险事件，《管理规定》要求各医疗卫生机构加强网络安全信息通报机制的建设，建立完善网络安全相关应急处置机制并积极组织应急演练。三级医院可以对此探索建设势态感知平台，用于及时收集、汇总、分析网络安全信息，及时通报预警和处置网络安全威胁。

五、我们的观察

总体来说，《管理规定》的大部分内容是建立在现行网络安全和数据安全相关法规、政策和国家标准的基础上，结合医疗健康领域的特征和管理需求，对医疗卫生机构开展网络安全管理工作提出的更加具体的合规要求。例如，在网络安全管理方面，《管理规定》进一步细化了《网络安全法》第二十一条中网络运营者的一般性网络安全保护义务，以及第三十四条中关键信息基础设施运营者应当履行的特殊安全保护义务；在数据安全管理方面，进一步细化了《数据安全法》第二十七条中数据处理者的一般性数据安全保护义务。

在医疗卫生机构开展网络安全等级保护工作方面，《管理规定》参考了现行法律法规、国家标准的规定。

在医疗卫生机构开展数据全生命周期安全管理方面，《管理办法》参考了 2018 年 7 月 12 日国

家卫健委印发的《国家健康医疗大数据标准、安全和服务管理办法（试行）》、2021 年 7 月 1 日实施的 GB/T 39725-2020《信息安全技术 健康医疗数据安全指南》等文件。

特别地，我们注意到《管理规定》专门提及了对医疗卫生机构运用人脸识别技术的要求，在目前线下医疗卫生机构和互联网医院开展业务的过程中，这种场景也十分常见，但均未超出现行法律法规、相关国家标准或征求意见稿的范畴。

六、结语

作为专门针对医疗卫生机构开展网络安全、数据安全管理的首份指导文件，《管理规定》大部分规定没有超出现行网络安全和数据安全相关法规、政策和国家标准的范围，同时吸收借鉴了个别法规、国标征求意见稿的内容，针对医疗卫生机构在“互联网+医疗健康”领域的特殊场景提出了部分新要求。在我国的医疗健康领域的网络安全和数据监管规范呈现着高度分散化的背景下，《管理办法》对医疗卫生机构网络安全管理的相关要求进行了汇总，并结合行业特征进行了细化和加强，可以为医疗卫生机构切实开展网络安全和数据合规工作提供比较清晰的路径指引。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com
苏若昕　律　师　电话：86 10 8553 7732　邮箱地址：surx@junhe.com