医疗卫生机构数据安全新规落地，医疗数据服务、共享单位有哪些注意要点？

作者：卢意光 | 邓梓珊

2026 年 2 月 14 日，国家卫生健康委、公安部、国家网信办、国家中医药局、国家疾控局联合发布《医疗卫生机构数据安全和个人信息保护管理办法(试行)》(国卫规划发[2026]6 号，"《办法》")，自印发之日起施行。这是医疗卫生领域首部系统规定数据安全和个人信息保护的部门规章，标志着医疗健康数据合规监管进入新阶段。

《办法》共七章四十条，对医疗卫生机构的数据分类分级、全生命周期安全管理、数据共享与对外提供、个人信息保护、跨境传输等方面作出全面规定。对于医疗机构与医药企业而言，《办法》最值得关注的是对**数据共享、委托处理**环节的明确要求——这直接影响到真实世界研究、临床试验、科研合作等常见业务场景。为此，我们特准备本快讯，帮助相关机构和企业更好地理解《办法》核心要求，做好合规准备工作。

一. 数据分类分级——合规义务的基石

《办法》明确医疗卫生机构数据分为核心数据、重要数据和一般数据三类，并落实分类分级保护制度。不同类别级别的数据同时被处理且难以分别采取保护措施的，按照其中级别最高的要求实施保护。不得通过邮箱、网盘、社交软件等传输核心数据、重要数据和敏感数据。

《办法》特别指出，个人信息达到一定精度、规模时可能构成重要数据。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

数据级别	保护要求
核心数据	四级等保或关键信息基础设施保护要求；优先使用商用密码、安全可信产品；安全事件溯源日志留存不少于 3 年
重要数据	三级等保；年度风险评估并向省级卫健部门报送；提供、委托处理、共同处理前需专项风险评估；向他人提供、委托处理、共同处理重要数据的，相关日志留存不少于 3 年
一般数据	按分类分级要求实施保护

我们建议：医疗卫生机构应尽快开展数据资产盘点，识别重要数据和核心数据，并向属地卫生健康行政部门报送。医药企业在与医疗机构开展数据合作前，应主动了解数据的级别属性，以便匹配相应的保护措施和合规程序。

二. 数据共享与对外提供——核心关注

(一) 对外提供重要数据(含委托处理)应进行风险评估

《办法》第十条规定，医疗卫生机构向其他数据处理者提供、委托处理、共同处理重要数据的，应当:

1. **通过合同等方式约定**处理目的、方式、范围以及安全保护义务;
2. **对数据接收方履行义务的情况进行监督**;
3. **提供前进行风险评估**(履行法定职责或法定义务的除外)。

我们提醒：上述要求意味着，医疗机构与医药企业、科研机构开展涉及重要数据的真实世界研究、临床试验数据共享时，合同中必须明确约定数据安全保护义务，且医疗机构有持续监督责任。医药企业作为数据接收方，应配合医疗机构履行监督要求，避免超范围使用数据。

(二) 鼓励数据共享，明确对外提供数据的审批流程

《办法》第十二条支持医疗卫生机构共享、调用数据；《办法》第十三条明确支持医疗卫生机构加强数据要素开发利用工作，但应确保个人信息安全。鼓励医疗卫生机构通过“原始数据不出域，数据可用不可见，数据可控可计量”等方式，促进医疗卫生机构数据依法合理有效利用。在此基础上，《办法》还明确了对外提供数据的审批程序：涉及对外提供医疗卫生机构数据的，需按相关要求报审，执行"业务管理部门同意→医疗卫生机构领导核准→信息技术部门支撑执行"的工作程序。

此外，第十五条还要求医疗卫生机构**及时将对外提供数据的情况报告属地卫生健康行政部门**。

我们提醒：未经网络安全和信息化工作领导小组或领导班子批准，任何部门和个人不得将数据传递至医疗卫生机构之外。这意味着，仅签订合作协议或达成其他非正式安排的情况下，医药企

业与医疗机构的数据共享安排将无法满足合规要求，必须走正式审批流程。

(三) 探索公共数据资源授权运营机制

《办法》第十四条涉及医疗卫生机构的公共数据资源开发利用，要求医疗卫生机构按照公共数据资源授权运营实施规范，探索建立数据分类分级授权运营机制，将授权运营纳入医疗卫生机构领导班子集体决策范围，明确授权条件、运营模式、运营期限、退出机制和安全管理责任，授权符合条件的运营机构开展公共数据资源开发、产品经营和技术服务。

三. 委托处理与共同处理

《办法》第十六条明确，医疗卫生机构委托他人处理或与他人共同处理医疗卫生机构数据的，**数据安全责任不因委托而改变**。医疗卫生机构应当经过严格的审批程序，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。涉及云计算服务的，应选择通过云计算服务安全评估的云计算服务。

《办法》第二十二条强调，非本医疗卫生机构人员在无监管情况下，不得对信息系统或医疗设备进行远程运维，必须获得授权；**建设运维期间，收集产生的医疗卫生机构数据未经授权不得用于其他用途**，服务完成后按照约定对医疗卫生机构数据予以返还或销毁；信息系统建设运维项目的承担单位，未经批准不得转包、分包。

对于委托处理个人信息，第二十七条还要求:

1. 事前进行个人信息保护影响评估;
2. 签订委托协议和保密协议;
3. 明确委托处理范围、目的、期限、处理方式、个人信息种类、保护措施;
4. 服务完成后，受托方应将个人信息返还或删除，不得保留。

四. 个人信息保护专项要求

(一) 调阅权限管理

医疗机构应当: 区分医疗、教学、科研、公共卫生紧急情况等合法调阅情形; 实行动态授权管理，离职、转岗人员及时回收权限; 推广授权管理、日志存档、数字水印等技术。

(二) 禁止性行为

- 不得超授权调阅个人信息;
- 未经本人或监护人同意，不得超出工作需要提供个人信息;
- 不得在公共区域显示患者个人信息;

- **不得通过通讯软件、社交媒体传输患者个人信息**;
- 不得通过拍照、截图等方式公开患者个人信息。

五. 违规责任

《办法》第三十二条至第三十五条明确了违规行为的法律责任:

违法行为	法律责任
医疗卫生机构的医疗信息安全制度不健全导致信息泄露	责令改正、警告、罚款; 情节严重可责令停止执业活动, 对直接负责人依法追究法律责任
医疗卫生机构相关人员泄露公民个人信息	行政处罚; 政府举办机构的依法给予处分
非法收集、使用、买卖个人健康信息	治安管理处罚; 构成犯罪的追究刑事责任
泄露患者隐私和个人信息	承担侵权责任

六. 合规建议

(一) 医疗机构

即时行动:

- 盘点数据资产, 识别重要数据和核心数据;
- 检查现有数据共享合同、数据处理协议是否约定安全保护义务, 供应商是否存在违反《办法》的情况;
- 核查数据提供审批流程是否符合规定;
- 建立对外提供数据台账。

近期行动:

- 完善数据分类分级管理制度;
- 建立数据对外提供审批流程;
- 开展数据安全风险评估;
- 组织全员数据安全培训。

(二) 医药企业

在与医疗机构开展数据合作时:

- **主动了解数据级别**, 匹配相应保护措施;
- **配合医疗机构履行监督义务**, 避免超范围使用;
- **完善合同约定**, 明确数据安全保护责任;
- **规范数据出境**, 涉及跨境传输需完成合规程序;
- **避免非正式数据共享**, 所有数据获取需走正式审批流程。

如您希望就相关问题进一步交流，请联系：

卢意光
+86 21 3135 8668
yiguang.lu@llinkslaw.com

邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野