君合研究简讯

JUNHE

2021 年 3 月 31 日

信息保护和网络安全法律热点问题

《健康医疗数据安全指南》将于 7 月 1 日正式实施

2020年12月14日，国家市场监督管理总局和国家标准化管理委员会联合发布了《信息安全技术 健康医疗数据安全指南》（GB/T 39725—2020，以下简称“**《指南》**”）。《指南》将于2021年7月1日生效实施。

在“互联网+医疗健康”和智慧医疗发展的大趋势下，《指南》意图综合实现多重目标，既确保健康医疗数据的保密性、完整性和可用性，保护个人信息、公众利益和国家安全，又能促进健康医疗数据和业务发展的需求。《指南》的主要内容总结如下。

一、健康数据分类体系

《指南》对健康数据类别范围、数据等级、相关角色、流通使用场景和数据开放形式进行了分类，以便于针对不同场景、不同数据提出区别化、精细化的安全措施要求。

1、 健康医疗数据

健康医疗数据是指，个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据，包括群体总体分析结果、趋势预测、疾病防治统计数据等。（第3.2条）《指南》将健康医疗数据分为如下几个类别，并进行了举例：

- ***个人属性数据***：是指单独或者与其他信息结合能够识别特定自然人的数据，如姓名、身份证、电话。
- ***健康状况数据***：是指能反映个人健康情况或同个人健康情况有着密切关系的数据，如主诉、现病史、检验检测数据、遗传咨询数据。
- ***医疗应用数据***：是指能反映医疗保健、门诊、住院、出院和其他医疗服务情况的数据，如门诊病历、住院医嘱检查检验报告、入院记录。
- ***医疗支付数据***：是指医疗或保险等服务中所涉及的与费用相关的数据，如医保支付信息、交易金额、保险状态。
- ***卫生资源数据***：是指那些可以反映卫生服务人员、卫生计划和卫生体系的能力与特征的数据，如医院基本数据、医院运营数据。
- ***公共卫生数据***：是指关系到国家或地区大众健康的公其事业相关数据，如环境卫生数据、传染病疫情数据、出生死亡数据。（第6.1条）

2、 健康医疗数据的分级

根据数据重要程度、风险级别以及对个人健康医疗数据主体可能造成的损害和影响，健康数据从

低到高分为五级。

- ***第1级***：可完全公开使用的数据。包括可以通过公开途径获取的数据。
- ***第2级***：可在较大范围内供访问使用的数据。例如不能标识个人身份的数据，各科室医生经过申请审批可以用于研究分析。
- ***第3级***：可在中等范围内供访问使用的数据，如果未经授权披露，可能对个人健康医疗数据主体造成中等程度的损害。例如经过部分去标识化处理，但仍可能重标识的数据，仅限于获得授权的项目组范围内使用。
- ***第4级***：在较小范围内供访问使用的数据，如果未经授权披露，可能会对个人健康医疗数据主体造成较高程度的损害。例如可以直接标识个人身份的数据，仅限于参与诊疗活动的医护人员访问使用。
- ***第5级***：仅在极小范围内且在严格限制条件下供访问使用的数据，如果未经授权披露，可能会对个人健康医疗数据主体造成严重程度的损害。例如特殊病种（例如艾滋病、性病）的详细资料，仅限于主治医护人员访问且需要进行严格管控。（第6.2条）

3、 相关组织或个人的角色

针对特定数据特定场景，相关组织或个人可划分为以下四种不同情形：

- ***个人健康医疗数据主体***（以下简称“**主体**”或“**数据主体**”）；
- ***控制者***：即能够决定健康医疗数据处理目的、方式及范围等的组织或个人；
- ***处理者***：即代表控制者采集、传输、存储、使用、处理或披露其掌握的健康医疗数据，或为控制者提供涉及健康医疗数据的使用、处理或者披露服务的相关组织或个人；
- ***使用者***：即针对特定数据的特定场景，不属于主体，也不属于控制着和处理者，但对健康医疗数据进行利用的相关组织或个人。（第6.3条）

上述定义的逻辑与《民法典》和《个人信息保护法（草案）》对于个人信息处理者的定义有一定差异，在一定程度上考虑了欧盟的分类标准，但又增加了使用者的定义，在《个人信息保护法》出台后是否会相应调整还待观察。

二、使用披露原则

《指南》第 7 条规定了 17 项具体的使用披露规则。对于个人健康医疗数据的收集和使用，《指南》遵循了个人信息收集、使用的告知同意原则，但同时规定了相关例外场景、回溯查询权、数据出境等创新性规定。健康医疗领域的伦理性和专业性极强，患者难以了解数据的具体安全状况，因此专业机构和专业人员需要承担更多的责任。尽管这些规定在一定程度上反映了医疗机构等在实践中需要更灵活、广泛的处理个人健康数据权限的要求，但相关授权在实践中是否能得到政府部门的认可需进一步观察。这些规定总结如下：

1、 无需个人授权使用及披露个人健康医疗数据

控制者在没有获得主体的授权，在以下情况可以使用或披露相应个人健康医疗数据：（1）向本人提供时；（2）治疗、支付或保健护理时；（3）涉及公共利益或法律法规要求时；（4）受限制数据集用于科学研究、医学/健康教育、公共卫生目的时。受限制数据集是指经过部分去标志化处理，但认可识别相应个人并因此需要保护的个人健康医疗数据集。在上述情况下，控制者可依靠法律法规要求、职业道德、伦理和专业判断来确定哪些个人健康医

疗数据允许被使用或披露。（第 7.b）条）该等规定是否与最终出台的《个人信息保护法》相一致还值得观察。

控制者可以使用治疗笔记用于治疗，在进行必要的去标识化处理后，可以在未经个人授权的情况下使用或披露治疗笔记进行内部培训和学术研讨。（第 7.i）条）。去标识化处理的具体要求和方法建议在第 10.2 条进行了规定。

上述规定似乎赋予控制者在诊断、治疗、支付、健康服务等过程中独立决定个人健康数据使用及披露的权利，其与《民法典》及未来的《个人信息保护法》项下个人信息授权同意原则是否相冲突待进一步解释。

2、 数据主体权利行使

《指南》第 7 条规定了主体行使其相应数据主体权利的原则，包括访问和查询权、获得副本的权利、更正和补充权、回溯查询权(即数据主体有权对控制者或其处理者使用或披露数据的情况进行历史回溯查询，最短回溯期为六年)。

3、 控制者自主决定个人健康数据的使用及披露

主体有权要求控制者在诊断、治疗、支付、健康服务等过程中限制使用或披露其个人健康医疗数据，以及限制向相关人员披露信息；控制者没有义务同意上述限制请求，但一旦同意，除非法律法规要求以及医疗紧急情况下，控制者宜遵守约定的限制。（第 7.h）条）

4、 数据利用

第 7 条将数据利用涉及的情形分别进行规定（除数据出境外）：

第一，受控制数据集的使用。控制者在确认数据使用的合法性、正当性和必要性，并确认使用者具备相应数据安全能力，且使用者签订了数据使用协议并承诺保护受限制数据集中的个人健康医疗数据后，可将受限制数据集用于科学研究、医疗保健业务、公共卫生等目的；使用者只能在协议约定的范围内使用数据并承担数据安全责任，在使用数据完成后，宜按照控制者要求归还、彻底销毁或者进行其他处理。未经控制者许可，使用者不能将数据披露给第三方。（第 7.m）条）

第二，匿名化的数据。如果控制者针对个人健康医疗数据汇聚分析处理后得到了不能识别个人的健康医疗相关数据，该数据不再属于个人信息，但其使用和披露宜遵守国家其他相关法规要求。（第 7.n）条）

第三，数据平台的适用。建议控制者在对外进行数据开发合作利用时，采用“数据分析平台”开放形式，对于使用披露进行严格管控。

5、 数据出境

控制者不宜将健康医疗数据在境外的服务器中存储，不托管、租赁在境外的服务器。控制者因为学术研讨需要，需要向境外提供相应数据的，在进行必要的去标识化处理后，经过数据安全委员会讨论审批同意，数量在 250 条以内的非涉密非重要数据可以提供，否则宜提请相关部门审批。不涉及国家秘密、重要数据或者其他禁止或限制向境外提供的数据，经主体授权同意，并经数据安全委员会讨论审批同意，控制者可向境外目的地提供个人健康医疗数据，累计数据量宜控制在 250 条以内，否则宜提请相关部门审批。（第 7.o）-q）条）

现行法律、法规对健康数据的出境规定了严格限制，例如《国家健康医疗大数据标准、安全和服务管理办法（试行）》规定，健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。《个人信息保护法（草案）》也对于信息出境作出了一系列的规定。对于《指南》提

出的无需政府部门审批即可出境的规定是否能构成相关豁免有待实践中进一步观察。

三、安全措施

《指南》第 8 条、第 9 条和第 10 条分别从安全措施要点、安全管理和安全技术三个方面为健康医疗数据保护提供了指南。

1、 安全措施要点

《指南》要求可以根据数据保护的需要进行数据分级，对不同级别的数据实施不同的安全保护措施，重点在于授权管理、身份鉴别、访问控制管理。第 8 条针对不同数据分级及数据流通使用场景具体规定了重点关注的安全措施，例如主体-控制者间数据流通、控制者-主体间数据流通、控制者内部数据使用、控制者-处理者间数据流通、控制者间数据流通和控制者-使用者间数据流通。

2、 安全管理

第 9 条从组织、过程（包括规划、实施、检查、改进）和应急处置三个方面规定了控制者宜有针对性地采取安全措施，并对实施措施后的效果进行检查，持续改进。控制者可参照附录 C 建立数据使用管理办法，参照附录 D 对数据申请进行审批，参照附录 E 与处理者（使用者）签署数据处理（使用）协议，参照附录 F 进行自查。

根据该条要求，相关组织应形成持续有效的机构、制度、流程、培训等一体化的合规体系搭建和管理，这与《个人信息保护法（草案）》的原则相一致，同时，由于健康医疗数据的敏感性，《指南》对于机构设置、会议频率、流程方案等方面提出了更加细节的要求，值得企业关注和对标。

3、 安全技术

第 10 条对通用安全技术和去标识化进行了指导。例如，对于去标识化，《指南》列示了对姓名、联系方式、日期、出生日期、年龄、号码和医疗机构内部所用号码去标识化的方法建议，去标识化策略、流程和结果宜由数据安全委员会审批。

四、典型场景数据安全

最后，《指南》则根据数据的使用主体和用途，将数据使用场景分为：医生调阅数据、患者查询数据、临床研究数据、二次利用数据、健康传感数据、移动应用数据、商业保险对接和医疗器械数据，并依附于每个场景对上述各条提出了具体化建议。下述以医生调阅数据和临床研究数据安全为例说明。

医生调阅数据。首先，对于数据分级，医生调阅场景下数据可分为默认级、告知级和授权级，分别对应数据分级中的第2级、第3级和第4级；其次，《指南》具体化了医生的角色定义和权限分配、如何将数据按分级和颗粒度标注、身份鉴别方式和数据调阅方式。（第11.1条）

临床研究数据安全。《指南》考虑了不同临床研究类型，如回顾性临床研究、前瞻性临床研究、临床基础研究、临床应用研究、临床路径研究、产品上市前研究和产品上市后研究、基于真实世界数据的临床研究、涉及人工智能的研究等，并对涉及的相关方的角色进行了分类。例如，对回顾性临床研究而言，申办者根据需要从临床研究机构获得既往数据从事医药/医疗产品和诊疗方案研究。临床研究机构、申办者共同承担控制者的角色，受试者是主体。《指南》从伦理审查及知情同意、数据分级、数据采集、数据传输数据存储、数据使用、数据发布和共享、审计管理等角度对临床研究数据的使用规定了安全保护要求。（第11.3条）

五、我们的观察

《指南》既借鉴了国外立法和标准，如美国HIPPA法案和ISO 27799、NIST800-66等标准，又结合了国内实践及标准，为健康医疗数据的应用提出本土化建议。《指南》深入日常使用场景，对于医疗

健康这一专业领域个人信息及健康数据利用及合规保护的价值平衡进行了有益尝试。一方面，《指南》为健康医疗数据控制者保护相关数据采取安全措施提供了实操性参考依据；另一方面，《指南》并不具有强制性法律效力，其相关规定，特别是与现有法律法规的规定或相关征求意见稿的规定有一定差异的条款，未来在实践之中如何实施，还有待进一步观察。

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
董俊杰　律　师　电话：86 10 8540 8722　邮箱地址：dongjj@junhe.com