医疗数据合规白皮书

发起单位

湖北数据集团 HUBEI DATA　　北京市京师（武汉）律师事务所 BEIJING JINGSH LAW FIRM WUHAN OFFICE

中部数据流通服务中心　　中部健康医疗大数据（湖北）有限公司

参编单位（排名不分先后）

东湖高新公共卫生服务中心 武汉市第九医院健康管理中心 湖北病理科技有限公司 北京市京师（深圳）律师事务所 北京市京师（成都）律师事务所 北京市京师（长沙）律师事务所 北京市京师（青岛）律师事务所 北京市京师（郑州）律师事务所 上海中联（武汉）律师事务所 北京瀛和（广州）律师事务所 湖北观筑律师事务所 广西成一律师事务所

编委会

王忠浩 李晓宇 魏 欣 干志文 余 阳 姜保国 彭 聪 古 伟 段先明 李文彬 李 柏 钟 正 刘晨璐 孙 童 徐鑫沂 胡 涛 曹治元 付庆刚 饶国荣 徐之桓 邓正聪 杨光勇 陈岚 王岩飞 樊思琪 聂雯珺 张铁臣 邓子怡 王海文 姚雪芹 张茗莉 张嘉骏 周莹 姜美红 刘增 潘月星 闫和明 余凯 冯丹 李佳玥 陈双 朱波琪 罗虎昌 万寿 袁海强 韦炜

目录

一、医疗数据概述

医疗数据是指在医疗保健过程中产生的所有与患者健康、疾病状态及医疗服务相关的信息，涵盖从个人诊疗到公共卫生管理的多种类型数据。主要包括在疾病防治、健康管理、医疗管理、医学研究等过程中产生的各种数据，[1]包括患者的个人信息、病历记录、药物购买与使用情况、设备数据、系统记录等，以及经加工处理之后得到的健康医疗相关电子数据。这些数据通常来源于医疗健康相关的医院信息系统（HIS）、电子病历系统（EMR）等信息系统及临床治疗、药物销售等活动。[2]

根据国家标准GB/T 39725-2020《信息安全技术-健康医疗数据安全指南》，将医疗数据分为个人属性数据、健康状况数据、医疗应用数据、医疗支付数据、卫生资源数据以及公共卫生数据等类别，[3]具体内容如下表所示：

数据类别	**范围**
个人属性数据	1）人口统计信息，包括姓名、出生日期、性别、民族、国籍、职业、住址、工作单位、家庭成员信息、联系人信息、收入、婚姻状态等； 2）个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像、健康卡个人属性数据号、住院号、各类检查检验相关单号等； 3）个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等； 4）个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等； 5）个人健康监测传感设备ID等。
健康状况数据	主诉、现病史、既往病史、体格检查（体征）、家族史、症状、检验检查数据、遗传咨询数据、健康状况可穿戴设备采集的健康相关数据、生活方式、基因测序、转录产物测序、蛋白质分析测定、代

[1] 参见谢小萍;何晓波;高雅洁;李卫：《涉及健康医疗大数据研究的伦理审查问题思考》，载《中国医学伦理学》2021年；参见王哲;邓勇：《健康医疗数据权利归属制度构建：现状、必要性与关注点》，载《卫生软科学》2024年。

[2] 参见网址https://mp.weixin.qq.com/s/zFp6ntAaH6H-DCp2TgBD7Q。

[3] 参见周建伟：《浅析智慧医疗数据合规要点》，载《今日科技》2021年；参见陈怡：《健康医疗数据共享与个人信息保护问题研究》，载《情报杂志》2023年。

	谢小分子检测、人体微生物检测等。
医疗应用数据	门（急）诊病历、住院医嘱、检查检验报告、用药信息、病程记录、手术记录、麻醉记录、输血及医疗应用数据录、护理记录、入院记录、出院小结、转诊（院）记录、知情告知信息等。
医疗支付数据	1）医疗交易信息，包括医保支付信息、交易金额、交易记录等；医疗支付数据； 2）保险信息，包括保险状态、保险金额等。卫生资源数据医院基本数据、医院运营数据等。
卫生资源数据	医院基本数据、医院运营数据等。
公共卫生数据	环境卫生数据、传染病疫情数据、疾病监测数据、疾病预防数据、出生死亡数据等。

*来源：GB/T 39725-2020《信息安全技术 健康医疗数据安全指南》

二、医疗数据相关法律、行政法规、部门规章等规范性文件

法律	《中华人民共和国民法典》
	《中华人民共和国刑法》
	《中华人民共和国个人信息保护法》
	《中华人民共和国数据安全法》
	《中华人民共和国网络安全法》
	《中华人民共和国生物安全法》
	《中华人民共和国基本医疗卫生与健康促进法》
行政法规	《全国人口普查条例》
	《关键信息基础设施安全保护条例》
	《医疗机构管理条例》
	《中华人民共和国人类遗传资源管理条例》
	《医疗保障基金使用监督管理条例》
	《网络数据安全管理条例》
部门规章	《医疗机构病历管理规定》
	《人口健康信息管理办法（试行）》

	《国家健康医疗大数据标准、安全和服务管理办法（试行）》
	《医疗器械临床试验质量管理规范》
	《医疗器械说明书和标签管理规定》
	《人类遗传资源管理条例实施细则》
规范性文件	《数据出境安全评估办法》
	《网络安全审查办法》
	《电子病历系统功能规范（试行）》
	《电子病历应用管理规范（试行）》
	《医疗卫生机构网络安全管理办法》
	《远程医疗信息系统建设技术指南》
	《医疗器械网络安全注册技术审查指导原则》
	《人工智能医用软件产品分类界定指导原则》
	《涉及人的生命科学和医学研究伦理审查办法》
	《电子病历共享文档规范》系列标准
	《药品记录与数据管理要求（试行）》
	《药物临床试验质量管理规范（2020 修订）》
	《互联网诊疗管理办法（试行）》
	《互联网医院管理办法（试行）》
	《互联网医院基本标准（试行）》
	《远程医疗服务管理规范（试行）》
	《真实世界数据用于医疗器械临床评价技术指导原则（试行）》
	《卫生健康行业数据分类分级指南（试行）》
	《用于产生真实世界证据的真实世界数据指导原则（试行）》
政策文件	《深化医药卫生体制改革 2024 年重点工作任务》
	《关于进一步完善医疗卫生服务体系的意见》
	《“十四五”全民健康信息化规划》
	《关于促进“互联网+医疗健康”发展的意见》
	《关于促进和规范健康医疗大数据应用发展的指导意见》

	《关于推进医疗机构远程医疗服务的意见》
	《卫生行业信息安全等级保护工作的指导意见》
国家标准	《信息安全技术 信息系统通用安全技术要求》(GB/T 20271-2006)
	《信息技术 安全技术 信息安全管理体系 要求》（GB/T 22080-2016）
	《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)
	《信息安全技术 个人信息安全影响评估指南》(GB/T 39335-2020)
	《信息安全技术 个人信息安全规范》（GB/T 35273-2020）
	《信息安全技术健康医疗数据安全指南》（GB/T 39725-2020）
	《信息安全技术 基因识别数据安全要求》（GB／T 41806-2022）
	《医疗器械 质量管理体系 用于法规的要求》(GB/T 42061-2022 ）
	《数据安全技术 数据分类分级规则（GB/T 43697-2024）》
行业标准	《面向互联网应用的健康医疗数据应用脱敏技术要求》（YD/T 6184-2024）
	《医疗器械软件 软件生存周期过程》(YY/T 0664-2020)
	《远程医疗信息系统基本功能规范》（WS/T 529—2016）
	《基于人工智能的多中心医疗数据协同分析平台参考架构》(YD/T 4043-2022）
	《互联网医疗健康信息安全管理规范（征求意见稿）》
	《医疗器械生产许可与备案管理基本数据集（征求意见稿）》
	《医疗器械经营许可与备案管理基本数据集（征求意见稿）》

*为方便阅读，以下正文中涉及的法律法规将采用简称，如《民法典》《个人信息保护法》《人类遗传资源管理条例》。

三、医疗数据的法律属性

（一）个人信息与隐私权属性

根据《个人信息保护法》第二十八条明确将医疗健康信息列为敏感个人信息，处理此类信息时需单独取得患者书面同意。《民法典》第一千零三十四条规定，

自然人的健康信息受法律保护，泄露患者隐私需承担侵权责任。在医疗实践中产出的个人属性数据、健康状况数据、医疗应用数据、医疗支付数据均属于个人信息；收入信息、社保卡信息、个人生物识别信息、健康状况数据、医疗应用数据、医疗支付数据均属于敏感个人信息。个人医疗数据直接关联个体健康状况，如基因数据、传染病史等可能引发歧视或人身风险。因此，患者对诊疗数据的收集、使用共同享有控制权，医疗数据处理者在采集这些信息时需要履行充分的告知义务并取得患者的单独同意。

在医疗实践中产生的基因、遗传咨询数据、基因测序、转录产物测序、蛋白质分析测定、代谢小分子检测均属于遗传资源信息。国务院发布的《人类遗传资源管理条例》中对人类遗传资源的各项管理予以规定。该条例指出，人类遗产资源包括人类遗传资源材料和人类遗传资源信息。其中，人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料；人类遗传资源信息则是指利用人类遗传资源材料产生的数据等信息资料。[4]医疗与医学研究活动中，涉及对人类遗传资源信息的处理时，需遵守该条例的相关规定。

（二）公共数据与国家战略资源属性

公共数据是国家机关、事业单位以及其他依照法律法规授权，具有管理公共事务职能或提供公共服务的组织，在依法履行公共管理职责或者提供公共服务过程中收集、产生的数据。[5]医疗数据的权属涉及三方主体：公民、医疗数据处理者和政府部门。公民作为原始医疗数据的产生者，往往基于隐私权，有权对医疗数据的开发和利用加以限制，以维护其合法权益。医疗数据处理者在履行公共服务职能过程中产生或获取的，以一定形式记录保存的，与公众健康相关的数据（包括但不限于疾病监测数据、疫苗接种数据、医疗费用统计数据等）为公共数据。

[4] 参见李雅琴;惠学：《人类遗传资源提供者利益分享的正当性探讨》，载《中国医学伦理学》2021 年。
[5] 参见黄朝椿：《论基于供给侧的数据要素市场建设》，载《中国科学院院刊》2022 年。

这些数据反映了区域乃至国家整体医疗状况，对政府单位进行公共卫生决策、医疗资源分配等具有重要意义。

医疗数据作为公共数据的重要组成部分，对于公共卫生领域的决策制定具有不可替代的作用。通过对特定范围内的医疗数据进行收集、整合与分析，卫生部门能够实时监测各类疾病的发病趋势、流行特征以及地域分布情况，从而及时制定科学合理的公共卫生防控策略。同时，医疗数据还为公共卫生资源的合理配置提供依据。通过分析不同地区、不同人群的疾病谱和医疗服务需求，卫生部门可以合理规划医疗机构的布局、医疗设备的配备以及医疗卫生人员的分配，提高公共卫生资源的利用效率。

在国家实施健康中国战略的大背景下，医疗数据发挥着关键作用。健康中国战略旨在提高全民健康水平，实现健康公平，而医疗数据是评估健康中国战略实施效果的重要依据。通过对医疗数据的长期跟踪和分析，可以监测居民健康素养水平的提升情况、疾病预防控制效果、医疗服务可及性和质量改善情况等，为战略的调整和优化提供数据支持。例如，通过对不同地区居民健康体检数据的分析，了解居民的健康状况和主要健康问题，针对性地开展健康教育和健康促进活动，增强居民的健康意识和自我保健能力。同时，医疗数据的整合与共享有助于打破医疗信息孤岛，促进医疗服务的协同发展，提升整体医疗服务水平，为实现健康中国战略目标奠定坚实基础。

（三）重要数据与国家安全属性

医疗数据与患者个人关系密切，同时还涉及国家安全问题，因此在数据分级上很可能涉及对敏感个人信息、重要数据或核心数据的分类分级。如果构成重要数据或核心数据，就需要符合重要数据或核心数据的相关规定来进行合规管理。

根据《数据安全技术 数据分类分级规则（GB/T 43697-2024）》的级别确定规则，重要数据指特定领域、特定群体、特定区域或达到一定精度和规模的，一

旦泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。[6]核心数据指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

根据国家卫健委2024年发布的《卫生健康行业数据分类分级指南（试行）》第十二条规定，原则上应纳入重要数据的建议范围：（一）涉及100万人及以上个人信息或10万人及以上敏感个人信息；（二）全国性的业务数据，如涉及10万人的群体健康生理状况数据;涉及1万人的族群生物特征数据、医疗资源数据;涉及10万人的诊疗数据、医疗救援保障数据、特定药品实验数据等；（三）经评估的其他数据。第十三条规定，原则上应纳入核心数据的建议范围：（一）1000万人以上个人信息或100万人以上敏感个人信息；（二）覆盖某一重要群体全部个体的数据，特定时期特定区域的群体数据；（三）涉及1000万人及以上，经过计算加工生成的，对数据描述对象有较深刻画程度，且影响国家安全的衍生数据；（四）经评估的其他数据。

从上述对重要数据和核心数据的界定来看，覆盖范围广、数据体量高的医疗数据构成重要数据或核心数据的门槛相对较低，因此需要履行更为严苛的合规义务，在确保合规的前提下才能进行流通。

四、医疗数据全生命周期合规要点

（一）医疗数据一般性合规要点

1.数据处理者应尽的安全保障义务

（1）安全认证要求

①网络安全等级保护三级认证：“三级等保”是我国对非银行机构的最高等

[6]参见《数据安全技术 数据分类分级规则》（GB/T 43697-2024）。

级保护认证，被定级为等保三级的系统主要适用于金融、医疗、政务等高敏感行业。通过“三级等保”认证，表明企业的信息安全管理能力达到国内最高标准。“三级等保”的技术要求主要包括物理安全、网络安全、主机安全、应用安全和数据安全五个方面。

物理安全：机房应区域划分至少分为主机房和监控区两个部分；机房应配备电子门禁系统、防盗报警系统、监控系统；机房不应该有窗户，应配备专用的气体灭火系统、备用发电机。

网络安全：应绘制与当前运行情况相符合的拓扑图；交换机、防火墙等设备配置应符合要求，例如应进行 Vlan 划分并确保各 Vlan 逻辑隔离，配置 Qos 流量控制策略，并设置访问控制策略，重要网络设备和服务器应进行 IP/MAC 绑定等；应配备网络审计设备、入侵检测或防御设备；交换机和防火墙的身份鉴别机制要满足等保要求，例如用户名密码复杂度策略、登录访问失败处理机制、用户角色和权限控制等；网络链路、核心网络设备和安全设备，需要提供冗余性设计。

主机安全：服务器的自身配置应符合要求，例如应具备身份鉴别机制、访问控制机制、安全审计机制和防病毒等，必要时可购买第三方的主机和数据库审计设备；服务器（应用和数据库服务器）应具备冗余性，例如支持双机热备或集群部署等；服务器和重要网络设备在上线前需要进行漏洞扫描评估，不应有中高级别以上的漏洞（例如 Windows 系统漏洞、Apache 等中间件漏洞、数据库软件漏洞、其他系统软件及端口漏洞等）；应配备专用的日志服务器保存主机、数据库的审计日志。

应用安全：应用自身的功能应符合等保要求，例如应具备身份鉴别机制、审计日志、通信和存储加密等；应用端应考虑部署网页防篡改设备；应用的安全评估（包括应用安全扫描、渗透测试及风险评估），应确保不存在中高级风险以上的安全漏洞（例如 SQL 注入、跨站脚本、网站挂马、网页篡改、敏感信息泄露、

弱口令和口令猜测、管理后台漏洞等）；应用系统产生的日志应保存至专用的日志服务器。

数据安全：应建立数据本地备份机制，确保每日备份至本地，并存放于异地；如系统中存在核心关键数据，应通过网络等方式提供异地数据备份功能，确保数据安全性。三级等保的管理制度要求涵盖安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理。

②ISO 体系认证：截至目前，国际标准化组织（ISO）已经发布了 25,000 多项标准，涵盖了技术、管理和制造的各个领域。其中适用于医疗数据的 ISO 标准主要有 ISO 7101、ISO 13485、ISO 14971、ISO 15189、ISO/IEC 27001、ISO/ASTM TR 52916、ISO/IEC 20000、ISO/IEC 27701 等。

（2）数据安全组织设立要求

数据处理者应成立网络安全和信息化工作领导小组，由单位主要负责人担任领导小组组长。网络数据安全负责人应当具备网络数据安全领域的专业知识和相关管理经验，并由数据处理者的管理层成员担任。网络数据安全负责人的核心职责包括但不限于监督数据安全策略的实施、组织定期的安全培训与演练、协调应对数据安全事件等，并依法享有直接向有关主管部门报告所在单位网络数据安全状况的权利，以确保在数据安全事件发生时，能够迅速、准确地传达信息，争取宝贵的应对时间。

（3）数据安全制度要求

各数据处理者应建立健全数据安全制度、操作规程及技术规范，涉及的管理制度每年至少修订一次。依据《数据安全法》《网络安全法》和《个人信息保护法》等规范性文件的要求，数据处理者至少应当建立数据分类分级制度、访问控制与权限控制制度、数据安全评估与审计制度、应急预案与事件响应制度、数据安全培训制度等。

序号	制度名称	核心要素	法律/标准依据
1	数据分类分级制度	分类（6 大类）、分级（3 级/5 级）、敏感性分级（核心/重要/一般）、差异化保护、动态调整	《数据安全法》《个人信息保护法》《网络数据安全管理条例》《信息安全技术 健康医疗数据安全指南》《数据安全技术 数据分类分级规则》
2	访问控制与权限控制制度	身份鉴别（双因素）、权限分级（RBAC）、操作可追溯（日志留存）	《个人信息保护法》《网络安全法》《信息安全技术 健康医疗数据安全指南》《电子病历应用管理规范（试行）》
3	数据安全评估与审计制度	操作日志记录、DSMM 评估、第三方审计	《数据安全法》《网络安全等级保护条例》
4	应急预案与事件响应制度	应急预案制定、应急演练、事件追责	《数据安全法》《网络安全法》
5	数据安全培训制度	由数据安全负责人和组织定期负责开展数据安全教育培训	《数据安全法》

①数据分类分级制度

根据法律法规的相关要求，医疗数据处理者应每年对本单位所储存的医疗数据进行全面梳理，依据医疗数据的重要程度、遭到破坏后的危害程度，建立本单位数据分级标准。医疗数据处理者既可在专业人员的辅助下，依据本单位的医疗数据所涉及的疾病范围、规模大小等，建立本单位的数据分级标准，也可参考《信息安全技术 健康医疗数据安全指南（GB/T 39725-2020）》中的分级标准。

数据级别	级别定义	适用场合
1 级	可完全公开使用的数据	公告
2 级	可在较大范围内供访问使用的数据	管理、研究、教育与统计分析
3 级	可在中等范围内供访问使用的数据	服务对象告知
4 级	可在较小范围内访问使用的数据，一旦泄露对数据主体造成较高程度损害	个性化服务于管理
5 级	仅能在极小范围内，在严格限制条件下供访	特殊疾病诊疗

	问使用的数据， 一旦泄露会对数据主体造成严重程度的损害	

同时，医疗数据处理者应按照一定的标准和规则对医疗数据进行分类和整理，不仅有助于提高数据的组织性、可访问性和可用性，为医疗服务、医疗管理、医学研究等提供有力支持，还能够为医疗数据后续存储过程中的应急响应、容灾备份和权限控制制度的落实提供基础。《信息安全技术 健康医疗数据安全指南（GB/T 39725-2020）》也为医疗数据处理者提供了可参考的分类标准。

数据类别	**范围**
个人属性数据	1）人口统计信息，包括姓名、出生日期、性别、民族、国籍、职业、住址、工作单位、家庭成员信息、联系人信息、收入、婚姻状态等；
	2）个人身份信息，包括姓名、身份证、工作证、居住证、社保卡、可识别个人的影像图像、健康卡号、住院号、各类检查检验相关单号等；
	3）个人通讯信息，包括个人电话号码、邮箱、账号及关联信息等；
	4）个人生物识别信息，包括基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等；
	5）个人健康监测传感设备 ID 等。
健康状况数据	主诉、现病史、既往病史、体格检查（体征）、家族史、症状、检验检查数据、遗传咨询数据、可穿戴设备采集的健康相关数据、生活方式、基因测序、转录产物测序、蛋白质分析测定、代谢小分子检测、人体微生物检测等。
医疗应用数据	门（急）诊病历、住院医嘱、检查检验报告、用药信息、病程记录、手术记录、麻醉记录、输血记录、护理记录、入院记录、出院小结、转诊（院）记录、知情告知信息等。
医疗支付数据	1）医疗交易信息，包括医保支付信息、交易金额、交易记录等；
	2）保险信息，包括保险状态、保险金额等。
卫生资源数据	医院基本数据、医院运营数据等。
公共卫生数据	环境卫生数据、传染病疫情数据、疾病监测数据、疾病预防数据、出生死亡数据等。

此外，医疗数据并非一直保持静态存储状态，在采集、交换、使用等过程中，

医疗数据处理者需进行动态的数据分类分级，包括对增量医疗数据的持续性分类分级，对已有数据产生变化的医疗数据的持续梳理，以保证医疗数据的动态分类分级，确保数据安全和合规性。

②数据安全培训制度

医疗数据处理者，为保障医疗数据处理、使用过程的安全性、隐私性和合规性，应制定一系列针对内部员工及数据相关人员的培训计划、流程和规范，以提升员工的数据安全意识和技能，以确保医疗数据在收集、存储、处理、传输和使用等各个环节的安全性。具体而言，医疗数据处理者单位内部的数据安全培训可以从法律法规和政策解读、数据安全技术与工具、实际案例分析三个角度，基于医疗数据分类分级及岗位风险图谱，制定差异化培训方案。

③数据访问权限控制制度

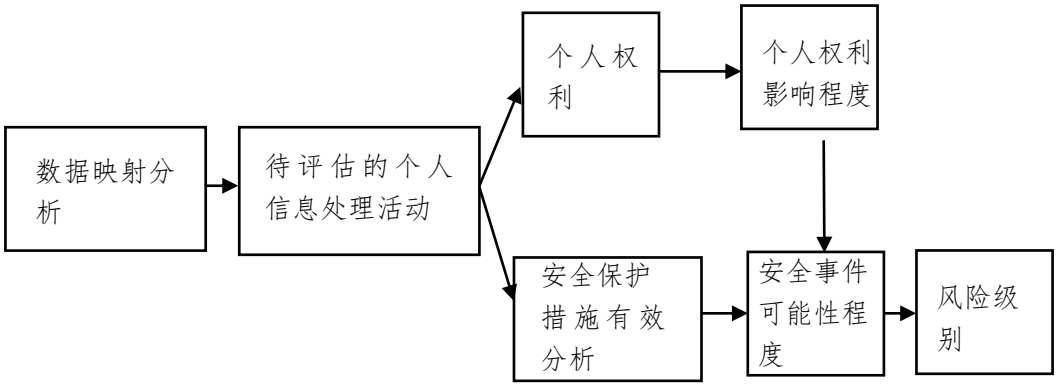
参照《医疗卫生机构网络安全管理办法》的相关规定，建议医疗数据处理者单位内部严格规定不同人员的权限，加强数据使用过程中的申请及批准流程管理，确保数据在可控范围内使用，加强日志留存及管理工作，杜绝篡改、删除日志的现象发生，防止数据越权使用。以医疗机构为例，医疗机构可建立数据全生命周期权限控制制度和应急访问机制。权限管理应根据科室内部入职、转岗、调岗、离职情况，自动触发权限分配和控制，如离职后 72 小时内强制回收失去的权限，并扫描残留服务器。应急访问机制旨在保证紧急状态下，如公共卫生事件、急诊抢救等情况，系统基于生命体征监测数据或医务人员的主动申请，解锁患者过往全部医疗数据。但医疗机构可要求在事后一定时间内补填《紧急访问说明》并提交。对于不同科室和人员的权限分配，遵循最小权限原则，例如：管理员仅可配置系统，医生仅可访问对应科室患者数据，且禁止使用默认账户直接操作系统，并对所有登录行为经过多因素认证，例如“密码+动态令牌”或“密码+生物特征”组合验证。此外，医疗机构数据存储服务器应对所有访问人员的操作进行记录并

留存，包括访问时间、用户身份、操作类型、涉及的数据范围及操作源 IP 地址，日志文件需加密存储并定期备份，防止篡改。

④数据安全评估、审计管理制度

医疗数据处理者应对已定级备案网络的安全性定期进行检测评估，第三级或第四级的网络应委托等级保护测评机构，每年至少开展一次网络安全等级测评。第二级的网络应委托等级保护测评机构定期开展网络安全等级测评，其中涉及 10 万人以上个人信息的网络应至少每三年开展一次网络安全等级测评，其他网络至少每五年开展一次网络安全等级测评。此外，医疗数据处理者在网络运营过程中，应每年开展文档核验、漏洞扫描、渗透测试等多种形式的安全自查，及时发现可能存在的问题和隐患。

涉及重要数据的医疗数据处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括所处理的重要数据的种类、数量，数据处理活动的开展情况，面临的数据安全风险及其应对措施等。风险评估标准可参照《信息安全技术 健康医疗数据安全威胁分析模型（GB/T 39477-2020）》更新威胁库。此外，由于部分医疗数据能够直接关联到患者个人，属于患者个人信息，其数据安全风险评估，应遵循《个人信息安全影响评估指南（GB/T 39335-2020）》中提供的实施标准和流程。



⑤数据安全应急响应制度

涉及网络运营的医疗数据处理者应当制定网络安全事件应急预案和应急处置机制，通过组织应急演练、开展网络安全攻防演练的方式，提升自身保护和对抗能力，减少计算机病毒、网络攻击、网络侵入等安全风险。在发生危害网络安全的事件时，相关数据安全负责人应立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。可参考《信息安全技术 信息安全应急响应计划规范》（GB/T 24363-2009）从应急响应计划的编制准备、应急响应计划的流程到应急响应计划的测试与维护等方面构建自身的应急响应制度。

2.医疗数据来源合规要点

（1）医疗数据采集与个人授权

①医疗数据采集规则

A.数据依规采集

根据《网络安全法》《数据安全法》和《个人信息保护法》的相关规定，医疗数据采集应遵循合法、正当、必要原则，明示收集目的与范围，并经被收集者（数据主体）同意。禁止通过欺诈、诱骗等非法手段获取医疗数据，强调最小必要原则，仅收集与诊疗直接相关的必要数据。采集个人健康医疗数据前，需充分告知并取得个人同意。涉及敏感个人信息时，需获得单独同意，告知内容包括数据收集目的、方式、范围、使用期限、数据主体权利及保护措施等。此外，《个人信息保护法》第十三条规定为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需，数据处理者无需经过患者同意，即可处理个人信息。

环节	合规要求	法律依据	实务操作示例
目的限定	仅限诊疗、科研等法定用途	《个人信息保护法》第六条	在隐私政策中明确列出数据使用场景（如糖尿病管理、药物研发）

告知同意	分层次告知+单独同意+动态同意机制	《网络安全法》第四十一条	采用分级弹窗：首次收集时告知核心功能所需数据，新增用途时需二次授权
最小必要	数据量与频率最低化，避免重复采集	《个人信息保护法》第六条	血糖仪仅收集血糖值，不强制要求绑定身份证号
特殊场景	紧急公共卫生事件可豁免同意	《个人信息保护法》第十三条	突发传染病监测时，疾控机构可依法直接调取患者轨迹数据

B.数据统一标准采集

为了确保医疗数据的准确性，数据处理者必须制定统一的医疗数据采集标准。统一的标准可以减少信息录入的重复工作，也能够保证数据在数据处理者内部各部门之间的数据一致性和可比性。以医院采集病案数据为例，医院应根据国际标准，并结合实际工作情况，制定符合医院特点的采集规范。世界卫生组织（WHO）发布的国际疾病分类（ICD）系统为全球病案数据采集提供了统一标准。医院应当依据该标准对患者的诊断进行分类，使得病案数据在全球范围内具有可比性。此外，ICD-10 和 ICD-11 版本的使用，有助于确保数据的统一性，便于医院之间的数据共享和合作。而在国内实践中，医院可以通过建立病案管理委员会，持续完善并细化数据采集流程，在全院范围内进行推广，确保院内病案数据采集标准的统一和规范。

②个人授权规则

A.首次授权

《国家健康医疗大数据标准、安全和服务管理办法（试行）》第二条特别规定：“国家在保障公民知情权、使用权和个人隐私的基础上，根据国家战略安全和人民群众生命安全需要，加以规范管理和开发利用。”据此，处理医疗数据在遵守数据安全的一般性原则与医疗领域伦理原则的基础上，还应重点关注《民法

典》《个人信息保护法》等法律对个人信息主体权利的保护。依据我国《个人信息保护法》的相关规定，个人信息处理者在处理个人信息时应获取个人明确的书面同意，处理敏感个人信息应当取得个人单独同意。医疗数据处理者对于个人医疗数据在必要的范围内经过一次采集后，应避免对个人医疗数据进行重复、多头采集。以患者就医场景为例，医疗机构如需对患者医疗数据进行采集，可在患者就诊时通过医院小程序、手机应用或线下签署《医疗数据使用授权协议》（详见附件 1）。此外，医疗机构处理不满十四周岁未成年人的医疗数据时，应当取得未成年人的父母或者其他监护人的同意。[7]医疗机构也应在内部应当制定专门的不满十四周岁的未成年人的个人医疗数据处理规则，以符合相关法律法规的要求。

B. 新增授权

个人医疗数据作为敏感个人信息，一旦处理目的、处理方式、处理期限、保护措施发生变更，医疗数据处理者应当重新取得个人的明确同意。就重新取得个人明确同意的方式而言，医疗数据处理者可线上通过短信、系统弹窗，线下通过个人重新签署补充协议的方式，重新获取个人授权，并保留操作日志和个人签署记录。

C. 告知义务的履行

《个人信息保护法》要求医疗数据处理者在获取个人医疗数据授权时，为保障个人知情权，应告知个人以下内容：医疗数据处理者的名称、医疗数据处理者对于医疗数据的处理目的、处理方式，处理的医疗数据的种类、保存期限、个人行使权利的内部方式和程序等。涉及敏感个人信息的，还应向个人告知处理敏感个人信息的必要性以及对个人权益的影响，依照《个人信息保护法》第十八条规定可以不向个人告知的除外。

相关法规	主要内容	具体要求

[7] 参见《2023 中国健康医疗行业企业数据出境实用指南及方案介绍》，网址为：https://max.book118.com/html/2023/1122/6054005000010012.shtm。

《互联网个人信息安全保护指南》	个人信息共享授权告知义务	1.在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息；[8] 2.将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记。
《APP违法违规收集使用个人信息自评估指南》	个人信息共享、转让、公开披露的要求	运营者应当在隐私政策中明确对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接受方类型或身份等。

D.授权撤回机制

医疗数据处理者应当为个人提供医疗数据的授权撤回渠道。个人可以通过线上或者线下的方式来撤回医疗数据的采集或是使用授权，撤回授权后，医疗数据处理者应当完成数据链路清除，但已经过匿名化处理且无法关联个人身份的科研数据除外。

综上，医疗数据处理者应在《医疗数据使用授权协议》中明确告知个人授权共享的数据范围、共享目的、接收方主体信息、联系方式、个人权利（如知情权、撤回权、访问权、删除权、修改权、限制处理权、数据转移权等）、数据处理者的安全保护措施和制度、授权期限、授权的撤回、免责情形等，在数据共享目的的授权中，不得概括同意，应当逐项列明，以征得个人的明确同意。

（2）第三方来源数据

①审查第三方资质及数据安全保障能力

在审查第三方资质时，需要确认第三方是否具备合法的数据获取资质，查验第三方机构营业执照、经营许可证（如涉及医疗须具备《医疗机构执业许可证》）及与数据处理相匹配的资质（如网络运营公司须具备《增值电信业务经营许可证》，涉及人类遗传资源数据，需确认其是否满足《人类遗传资源管理条例》所列明的要求；涉及关键信息基础设施的，还需确认第三方是否被纳入监管范围并履行相

[8] 参见《互联网个人信息安全保护指引》，网址为：https://max.book118.com/html/2019/1108/8124060046002062.shtm。

应义务）对第三方进行数据安全保障能力评估时，应评估第三方是否符合网络安全等级保护要求，如物理存储安全、网络加密安全、系统应用安全、数据备份安全等。

②确保第三方数据来源合法和授权合规

第三方数据收集必须基于《个人信息保护法》《数据安全法》等法律规定的合法性基础，数据采集时还需遵循“最少必要原则”，该原则与行政法领域的“比例原则”类似，《信息安全技术健康医疗数据安全指南》（GB/T 39725-2020）第 8.3 条对其进行了定义，即指采集的数据不应当超范围采集，应当根据业务和管理要求，以最少且够用的标准进行。为进一步审查数据的合法性，可以要求第三方提供数据来源合法性承诺及合法性证明材料，包括取得数据提供方对自行生产、公开收集、间接获取等数据来源的说明及对数据权属的合法性承诺函等。

③签署数据处理协议

为了避免数据提供方与数据接收方可能存在的法律纠纷，在签署数据处理协议时，就应当对数据本身（数据类型、内容、质量、数量等）、双方涉数权利义务、法律责任等内容进行明确的约定。作为数据接收方，尤其应当确保数据授权使用范围满足实际处理的需要。同时，在签署数据处理协议后，双方均须严格按照协议约定处理数据。

（3）数据质量控制

在医疗数据采集和录入时，数据处理者应对数据质量进行严格、准确地控制。数据质量的优劣通常通过数据质量六性进行判断，包括：准确性（数据是否真实反映客观事实）、完整性（数据在创建、传输过程中无缺失和遗漏）、一致性（多源数据逻辑一致）、有效性（数据的值、格式符合业务标准）、唯一性（同一数据只能有唯一的标识符）、时效性（数据是否按预期时间更新）。以医疗机构对患者数据的采集录入过程为例，在数据录入流程上医疗机构可采用电子病历系统

（EMR）、医疗设备接口等自动化采集技术，减少人工录入错误，同时通过逻辑校验（如性别与诊断关联）、非空校验、存在性校验等确保数据逻辑合理性。其次,要确保数据采集的完整性和一致性,在数据分类时参考国际统一编码体系(如ICD、LOINC）进行分类，确保跨系统的一致性。在收集患者数据时要实现患者身份标识唯一化，避免重复记录，确保不同来源数据（如病历与质控记录）的关联性。最后，要确保数据收集的时效性，数据记录需符合临床时间逻辑，并实时更新以反映最新状态。

（4）数据匿名化处理

医疗数据处理者在对医疗数据进行处理时,应对医疗数据中能够关联到具体个人的信息进行匿名化，如姓名、性别、年龄、住院号、门诊号、疾病部位等。匿名化处理是指个人信息经过处理后无法识别特定自然人且不能复原的过程。[9]经匿名化处理后的数据不再属于个人信息。通常来说，匿名化的第一步是处理那些能直接识别出个人的数据，比如将直接标识符假名化、加密、抑制或者屏蔽这些信息；第二步，再处理那些间接能识别出个人的数据，比如泛化、随机化改变这些信息。在此过程中，应确保匿名化处理符合相关法律法规，避免重新识别个人信息的风险。 假设进行一个关于睡眠质量的临床研究，研究者收集了参与者的睡眠期间医疗数据，包括他们的睡眠模式、心率、呼吸频率等生理指标。原始数据包括：• 姓名：张三• 年龄：20 岁• 性别：女• 睡眠数据：包括连续 7 晚的心率、呼吸频率等。匿名化处理后的数据包括：• 姓名：＊；• 年龄：大于 18 岁；• 性别：*；• 睡眠数据：心率平均值、呼吸频率平均值等。在这个例子中，匿名化处理不仅从数据集中移除了姓名、年龄和性别，而且对睡眠期间医疗数据进行了聚合处理（将数据集中的原始数据转换成更高层次的、概括性的信息），

[9] 参见《数据要素“三权分置”理论范式及其实践路径研究》，网址为：https://max.book118.com/html/2023/0921/6140051030005232.shtm。

以避免通过特定的生理指标反推出个人身份。此外，应定期评估匿名化技术的有效性，确保匿名化数据在多重分析背景下不再具有可识别性。

3.医疗数据存储合规要点

（1）存储空间

①物理服务器存储空间:参见上述主体资质部分,为充分保障医疗数据安全,医疗数据处理者可参照网络安全等级保护三级认证的相关要求,进行合规整改和提升。其中，建议机房区域至少划分为主机房和监控区两个部分，配备电子门禁系统、防盗报警系统、监控系统，机房不应该有窗户，并应配备专用的气体灭火、备用发电机。也可根据自身的数据安全需求，选择采用生物识别门禁（如指纹/虹膜识别）结合 24 小时监控录像，并对服务器机柜采用独立上锁、防火防潮、防电磁泄漏等技术措施。

②存储地点:医疗数据原则上一般存储在境内。《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十二条规定，健康医疗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。对于跨境数据传输，医疗数据处理者应确保所涉及的国家或地区具备适当的数据保护水平，并遵循相关国际法规。

（2）存储期限

个人健康医疗数据的保存期限应为实现自然人授权医疗数据处理者使用的目的所必需的最短时间。此外,不同医疗数据存储期限也存在着各种各样的限制,以病历数据、处方数据、药品及医疗器械销售信息数据为例，其保存期限及要求详见下表：

《互联网诊疗监管细则（试行）》	互联网诊疗病历记录按照门诊电子病历的有关规定进行管理，保存时间不得少于 15 年。诊疗中的图文对话、音视频资料等过程记录保存时间不得少于 3 年。

《处方管理办法》	普通处方、急诊处方、儿科处方保存期限为1年，医疗用毒性药品、第二类精神药品处方保存期限为2年，麻醉药品和第一类精神药品处方保存期限为3年。处方保存期满后，经医疗机构主要负责人批准、登记备案，方可销毁。
《药品网络销售监督管理办法》	药品网络销售企业应当完整保存供货企业资质文件、电子交易等记录。销售处方药的药品网络零售企业还应当保存处方、在线药学服务等记录。相关记录保存期限不少于5年，且不少于药品有效期满后1年。
《医疗器械网络销售监督管理办法》	从事医疗器械网络销售的企业应当记录医疗器械销售信息，记录应当保存至医疗器械有效期后2年；无有效期的，保存时间不得少于5年；植入类医疗器械的销售信息应当永久保存。相关记录应当真实、完整、可追溯。
《医疗机构病历管理规定》	门（急）诊病历由医疗机构保管的，保存时间自患者最后一次就诊之日起不少于15年；住院病历保存时间自患者最后一次住院出院之日起不少于30年。

（3）数据加密和介质管控

数据加密是数据系统中保护数据隐私和防止非法访问、泄露或篡改的主要技术之一。医疗数据处理者应采用安全的通信协议或安全的网络传输通道进行加密传输，确保医疗数据在传输过程中的安全性。静态存储的数据推荐使用AES-256或国密算法SM4进行全盘加密，密钥必须通过硬件安全模块（HSM）或密钥管理系统（KMS）独立托管，实现密钥与数据的物理分离。数据传输过程中需启用TLS 1.3或IPSec等强加密协议，禁用SSL 3.0、TLS 1.0等存在漏洞的旧版协议。

介质管控要求医疗数据处理者对存储介质进行严格管理。可以基于上述医疗数据分级的管理要求，通过介质管控的自动化工具对介质进行登记、控制和定期审计，确保只有授权人员才能访问和使用这些介质。介质管控还包含对医疗数据的备份和恢复策略的管理，以防止医疗数据丢失或损坏，满足合规性要求。应定期测试备份数据的恢复能力，确保在紧急情况下能够快速恢复数据。

4.医疗数据共享合规要点

医疗数据处理者应该对其共享给其他主体的数据进行有效的安全管理，采取必要的技术和组织措施，保障数据的安全。包括采取数据加密、数据备份和恢复、

访问控制等技术措施，以及制定共享协议、建立数据共享管理机构等组织措施。

首先，医疗数据处理者需要对数据接收主体的数据安全能力进行评估，确认其具备相应的数据安全能力，从而保证第三方主体使用、处理数据时的安全和保密性。例如，第三方主体需建立符合等保三级要求的网络安全防护体系，部署数据加密、匿名化处理（如符合个人信息去标识化指南 GB/T 37964 标准）及动态访问控制机制。第三方主体的系统管理体系方面，需取得 ISO 27001 信息安全管理体系认证及 ISO 27799 医疗健康信息安全管理认证，并依据《数据安全能力成熟度模型》（DSMM）达到三级以上能力水平，同时设立专职数据安全官岗位负责合规审查。对第三方的合规性审查应定期进行，并确保数据传输协议满足最新的安全要求。

其次，在医疗数据传输过程中，数据可能会被截获、篡改或泄露。因此，在传输过程中保护数据的隐私性和完整性显得尤为重要。加密技术通过将明文数据转换为密文，确保只有授权方能够解密和读取数据，从而保护数据传输过程的安全。根据网络公开的材料，以下简要罗列了医疗数据可采用的加密传输技术及相应优势与应用前景[10]。

传输方式	**原理与优势**	**应用与前景**
量子加密传输	量子加密传输利用量子态不可克隆特性，通过光纤或自由空间传输光子密钥，任何窃听都会破坏量子态而被察觉，保障密钥传输的绝对安全。 同时基于格密码、哈希函数等构建抗量子算法，如 NIST 选定的 CRYSTALS-Kyber，抵御量子计算机对传统加密算法的攻击。	量子通信天地一号项目实现上万公里保密通信，银行、政府机关等纷纷采用量子加密技术，保护重要信息传输安全。随着技术成熟和成本降低，量子加密有望在更多领域普及，如能源、医疗等，为信息安全筑牢防线。
全同态加密技术	全同态加密技术支持在密文状态下进行数据运算，如检索、分析	全同态加密技术可用于区块链交易隐私保护、AI 隐私保护等，如 Zama 的 fhEVM 为区

[10] 参见星火燎原《数据传输加密新技术及趋势》一文，网址为：https://mp.weixin.qq.com/s/Uqq56uFRAXdsu-nSZg-LYw。

（FHE）	等，实现数据“可算不可见”，保护数据隐私。	块链隐私计算提供支持，推动 Web3 隐私保护发展。在医疗云场景中，全同态加密技术可实现加密基因数据的安全计算，为医疗数据共享和分析提供安全解决方案。未来，全同态加密技术将与区块链、零知识证明等技术结合，将为隐私保护和数据安全提供更全面的解决方案。
区块链融合加密技术	区块链融合加密技术基于智能合约实现密钥自动轮换，提高密钥管理的安全性和效率，降低密钥泄漏风险。区块链融合加密技术的跨链加密协议采用零知识证明技术，在不泄露数据内容的情况下验证数据的真实性，为跨链数据交互提供可靠保障。	区块链融合加密技术为金融、物联网等领域的区块链应用提供了更安全的密钥管理方案。未来，随着区块链技术的发展，跨链通信需求日益增加，跨链加密协议也能够为区块链的互联互通和生态建设提供重要支撑，推动区块链在多领域的融合应用，促进数字经济的发展。
边缘计算加密技术	边缘计算加密技术的轻量级加密算法能够在保证数据安全性的同时，降低边缘设备的计算和能耗负担，提升设备性能。同时动态加密策略可根据设备状态和环境变化灵活调整，实现安全与性能的平衡。	在能源受限的边缘计算场景中，边缘计算加密技术能够提高设备的续航能力和使用寿命，降低设备维护成本，为智能电网、工业物联网等领域的边缘设备提供更灵活高效的加密方案，保障系统稳定运行。目前，该技术广泛应用于物联网设备的数据加密，如智能家居、智能穿戴等。
安全多方计算技术（MPC）	安全多方计算技术能够在保证多个参与方在不泄露各自数据、不共享数据的情况下进行协同计算和联合机器学习，实现数据的隐私保护和价值挖掘。	安全多方计算技术可应用于医疗数据共享、企业数据合作等场景，为数据隐私保护和数据安全利用提供新的思路和方法，促进数据的流通和共享，推动各行业的数字化转型。
零知识证明技术（ZKP）	零知识证明技术的匿名凭证系统可在不泄露数据内容的情况下证明数据的真实性。	未来，随着技术的发展，零知识证明技术能够为区块链等领域提供更安全的隐私保护解决方案，并在身份认证、电子政务、电子商务等领域得到更广泛的应用，为医疗数据应用及数字经济的发展提供安全保障。

最后，医疗数据处理者与第三方主体之间就非公共数据订立数据权属合作协议时，协议至少应当包括以下内容：（1）双方信息；（2）数据交付方式；（3）数据接收方的数据处理权限范围；（4）数据三权归属；（5）数据安全保障的内容及义务方；（6）后续衍生数据产品的权属情况；（7）合约追踪条款；（8）应急预案条款；（9）涉及行政备案或批准的条款。

5. 医疗数据销毁合规要点

（1）销毁制度

《个人信息保护法》中规定在保存期限届满、停止提供服务、处理的目的已经达到或无法达到时，个人信息处理者应当主动删除个人信息。《医疗卫生机构网络安全管理办法》明确要求建立“无法还原”的数据销毁机制，国家药监局《药品数据管理规范》强调建立数据销毁规程，需包含申请审批、执行人资质、销毁方式验证等要素。由此可见，相关法律法规要求销毁医疗数据时应采用确保数据无法还原的销毁方式，并重点关注数据残留风险及数据备份风险。医疗数据处理者也应在医疗数据销毁过程中严格遵循销毁报批、销毁情况记录、销毁安全检测，以确保销毁工作的规范性和安全性。

①明确销毁流程和审批机制

数据销毁应经过严格的审批流程，由数据所有者或使用者提出销毁申请，填写销毁申请表，经相关部门审核和审批通过后方可执行。在执行上，采取三级审批机制，由申请人（数据管理员）到部门负责人（合规审核）再到法务/信息安全部门（最终批准），数据销毁需要两人在场监督并签字确认。在此过程中的责任主体划分可参见表格：

角色	**职责范围**	**合规风险点**
数据管理员	发起销毁申请、初步分类	误判数据价值导致过早销毁
数据安全部门	审核法律依据与业务影响	审批标准执行偏差
IT 部门	执行技术销毁、介质处理	操作未达技术标准
法务部	备案销毁记录、应对监管审查	记录缺失或篡改

②留录和留存销毁证据

对销毁过程进行详细记录，包括销毁内容、销毁时间、操作人等信息，并留存相关证据，这不仅有助于后续的审计和追溯，还能在出现争议时提供有力的证

明，确保数据销毁的合规性和透明度。

③定期审查和更新制度

随着技术的发展和法律法规的变化，定期审查和更新数据销毁管理制度，确保其始终符合最新的合规要求，这包括对销毁流程、技术手段等方面的优化和改进，以适应不断变化的数据安全环境。

（2）销毁方式

①物理销毁

物理销毁是指通过物理或化学方法直接销毁存储介质，例如将硬盘、U 盘等存储设备进行物理性破坏（如粉碎、熔毁）或化学性破坏（如强酸腐蚀），以达到彻底、不可逆的硬盘数据销毁/数据擦除的目的。

②电子销毁

电子销毁分为三大形式，即数据擦除、密钥销毁和逻辑销毁。

数据擦除是针对数据恢复行为而产生的逆向操作，包括格式化擦除、数据覆写、软件擦除、特定算法擦除等。

◆ 格式化擦除：是磁盘控制器将所有扇区清零，并重新写入磁盘引导记录和扇区 ID。

◆ 数据覆写：是将非保密数据写入原存有敏感数据的硬盘簇的过程。使用预先定义的无意义、无规律的信息，反复多次（如 DoD5220.22-M 标准要求 7 次覆写）覆盖硬盘上原先存储的数据，就无法知道原先的数据是“1”还是“0”，也就达到了硬盘数据擦除的目的。[11]

◆ 软件擦除：如 DiskGenius 等软件可以执行数据擦除操作，通过磁盘扇区清零、全盘覆盖数据等方法，让数据无法恢复。

[11] 参见董守吉：《国家秘密全生命周期保护技术》，载《保密科学技术》2023 年。

◆ 特定算法擦除：是指根据写数据的方法和破坏强度，视情况采用如加密擦除、美国国防部的Dod5220.22-M、Gutmann、Schneier算法等国际标准方法。

密钥销毁：适用于云存储环境下的密文数据。该方法不销毁数据本身而是通过销毁密钥的方式实现数据的不可访问。只要用户安全地销毁密钥，就可以保护数据密文无法在多项式时间内被破解，将数据销毁问题转换成密钥生命周期管理问题。

逻辑销毁：是对磁盘扇区进行清零操作，即把硬盘所有扇区用0或1进行多次（建议≥3次）写入，使硬盘上的所有数据丢失，包括分区信息，从而破坏数据的逻辑结构或清除访问权限。

（3）同等方式安全处理

《个人信息保护法》第四十七条规定了个人信息处理者应当主动删除个人信息的情形，也规定了对于难以删除的数据个人信息处理者应采取其他能够保证安全性且达到与删除同等目的的方式进行处理，即“法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。”

在适用应采取同等方式安全处理的情形下，不代表医疗数据处理者可以对无法销毁的医疗数据放任不管：

①医疗数据处理者不得进行任何存储以外的处理行为（包括使用、共享、转让等）；

②在此种情形下仍然需要对所存储的医疗数据履行作为数据处理者的义务，即根据存储数据的体量及敏感程度，采取相应的安全保护措施。比如设置内部人员访问控制、数据加密、定期评估安全风险以及敏感信息单独存储等。其次，对于符合采取同等方式安全处理的数据，医疗数据处理者应建立明确的操作申请和审批流程，确保数据安全操作的合法性和透明度。此外，还需要对该类数据进行

定期评估和审查，确保其继续符合采取同等方式进行安全处理的条件，并在条件不再满足时及时进行销毁。

（二）特殊场景下的医疗数据合规要点

1.处理人类遗传资源信息场景

依据《人类遗传资源管理条例（2024 年修订）》（以下简称为“《管理条例》”）第 2 条：“本条例所称人类遗传资源包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。”

但《人类遗传资源管理条例实施细则》对人类遗传资源信息的范围进行了一定限缩，排除了临床影像数据（如 B 超、PET-CT、核磁共振、X 射线等影像数据、病理诊断等图片数据）、不涉及人群基因研究的临床数据（如血常规、尿常规、肝肾功能、血生化等一般实验室检查信息等）、蛋白质数据和代谢数据。

医疗机构在对先天性疾病、基因疾病的患者开展诊疗活动的过程中，就可能涉及采集患者遗传资源信息，需特别注意合规边界。

（1）特殊告知义务

根据《管理条例》第十二条，医疗机构采集患者遗传资源信息，应当事先告知患者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，并征得书面同意。在告知人类遗传资源提供者前款规定的信息时，必须全面、完整、真实、准确，不得隐瞒、误导、欺骗。

（2）对外提供的行政审批

由于人类遗传资源作为战略性生物资源，其数据安全直接攸关国家生物安全与公共卫生安全体系，《管理条例》要求外方单位需要利用我国人类遗传资源开

展科学研究活动的，必须采取与我国科研机构、高等学校、医疗机构、中方企业合作的方式进行，并经国务院卫生健康主管部门批准。因此医疗机构也应注意在与外方单位进行人类遗传资源信息合作过程中的下列数据安全要求，以获取国务院卫生健康主管部门审批通过：

①对我国公众健康、国家安全和社会公共利益没有危害；

②合作方案的目的、内容、收益分配明确合理；

③通过合作双方各自所在国（地区）的伦理审查；

④重大事项发生变更的，应当办理变更审批手续；

⑤保证中方单位及其研究人员在合作期间全过程、实质性地参与研究，并完全向中方单位开放并向中方单位提供备份；

⑥合作双方应当在国际合作活动结束后6个月内共同向国务院卫生健康主管部门提交合作研究情况报告；

⑦将人类遗传资源信息向外方单位提供或者开放使用的，应当向国务院卫生健康主管部门备案并提交信息备份。

2.伦理安全审查场景

与其他场景所涉数据处理相比，在医疗数据的处理中，伦理判断是其重要的特征。根据《管理条例》第九条规定：“采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，并按照国家有关规定进行伦理审查。”2023年12月1日，科学技术部、教育部、国家卫生健康委等部门联合公布的《科技伦理审查办法（试行）》正式施行。该办法对科技伦理审查的一般程序、简易审查和跟踪的适用条件、流程进行了规定。根据相关法律法规的规定，涉及人的生物医学研究过程中，应进行伦理审查。包括使用现代科学技术开展的生理、心理、病理现象研究，新技术或新产品的人体试验，以及应用流行病学、社会学、心理学等方法进行的科学研究。相关医学研究机构的伦理委员会进行伦理审查时，应

遵循保护隐私原则，如实告知受试者其个人信息的储存、使用及保密措施情况，未经授权不得将受试者个人信息向第三方透露。[12]

医疗健康作为前沿性与伦理性高度交织的领域，在人工智能诊疗、基因数据分析等新技术应用场景中持续面临伦理审查机制与技术创新速度的结构性矛盾。医疗机构采集人类遗传资源信息，应当依法通过伦理委员会审查，确保符合《科技伦理审查办法（试行）》要求。受篇幅所限，本白皮书就相关内容暂不做系统性论述。

3.公共数据授权运营场景

公共数据是指国家机关、事业单位以及其他依照法律法规授权具有管理公共事务职能或提供公共服务的组织，在依法履行公共管理职责或者提供公共服务过程中收集产生的数据。

医疗数据作为公共数据，初步的采集和储存由各级医疗机构负责。依据《全国医院数据上报管理方案—医疗业务（试行）》，省卫健委作为统筹单位，负责牵头指导，融合本省各级医疗机构的诊疗、医保、健康等数据，开展核保评估、药企临床试验、医药供应链等场景建设，提升医疗健康服务水平。

依据《公共数据资源授权运营实施规范（试行）》的相关规定（下称《实施规范》），医疗数据作为公共数据如需在省级平台授权运营时，可参考如下路径：

（1）方案编制：省数据局负责牵头组织编制或指导省卫健委编制公共数据资源授权运营实施方案。省卫健委在省数据局的组织和指导下进行公共数据授权运营实施方案的编制。实施方案需包括十二个方面内容，其中值得注意的是可行性论证、数据安全、个人信息保护措施和应急处置措施。对于可行性论证，《实施规范》要求实施方案应当至少包括授权运营数据全生命周期管理服务、社会需求、市场规模、预期成效、风险防控等。方案编制完成后，由省数据局负责或协

[12] 参见吴卫明：《健康医疗数据的法律与合规问题探析（下）》。

助省卫健委将本地区实施方案报请省人民政府审议。省人民政府依据经济性、社会性、可行性三重标准进行考察，经审定同意的实施方案不得随意变更。

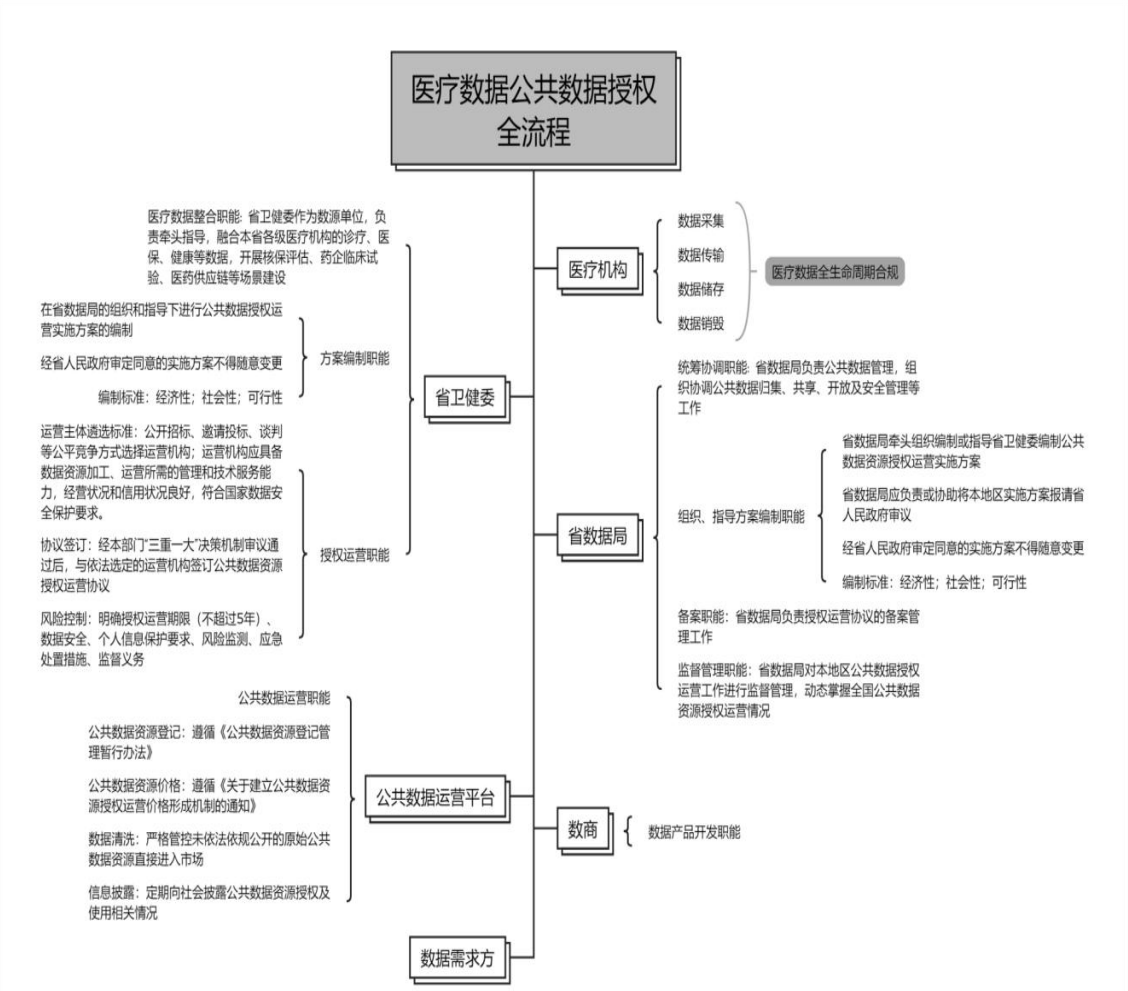
（2）方案实施：省卫健委通过公开招标、邀请投标、谈判等公平竞争方式选择运营机构。相关法律规范要求，运营机构应具备数据资源加工、运营所需的管理和技术服务能力，经营状况和信用状况良好，符合国家数据安全保护要求。选定运营机构后，经省卫健委“三重一大”决策机制审议通过后，与依法选定的运营机构签订公共数据资源授权运营协议。协议中授权运营期限原则上不得超过5年。协议签订后，由省数据局负责公共数据授权运营协议的备案工作。

（3）方案实施的监督管理：省数据局对本地区公共数据授权运营工作进行监督管理，动态掌握公共数据资源授权运营情况。

（4）实施运营：《实施规范》要求运营机构建立健全安全可控的开发利用环境，采用隐私计算等安全可信流通技术。运营机构应当按照要求进行公共数据资源登记，公共数据产品和服务价格要按照国家有关价格政策执行。对此，可进一步参考《公共数据资源登记管理暂行办法》和《关于建立公共数据资源授权运营价格形成机制的通知》。同时《实施规范》还要求运营机构接受社会监督，定期向社会披露公共数据资源授权及使用相关情况。

（5）运营管理：《实施规范》要求，运营机构应建立健全管理制度，强化数据治理，提升数据质量，落实数据分类分级保护制度要求，加强技术支撑保障和数据安全管理，严格管控未依法依规公开的原始公共数据资源直接进入市场，强化涉及公共数据资源授权运营的内控审计。运营机构不得超出授权范围使用公共数据资源，严防数据加工、处理、运营、服务等环节的数据安全风险。

（下文附医疗数据授权全流程的思维导图）



4.医疗领域人工智能场景

随着信息技术的发展、医疗需求的增长以及医疗改革的推动，AI 在医疗中的应用日益广泛，AI 与医疗深度融合后呈现出智能化、高效化和便捷化的特点。

AI 医疗是指通过运用先进的信息技术，如人工智能、大数据、云计算、物联网等，对医疗过程进行智能化管理和优化，从而提高医疗服务的质量和效率。[13]AI 在医疗中的应用，不仅有助于提升医疗服务的精准度和个性化程度，还能为医疗决策提供科学依据，推动医疗行业的创新发展。

《2024 中国 AI 医疗产业研究报告》数据显示，2023 年中国 AI 医疗行业市场规模已达到 973 亿元，其预计到 2028 年将进一步增长至 1598 亿元。

[13] 参见《2024 年中国 AI 医疗产业研究报告》，网址为：https://max.book118.com/html/2024/0719/7156200011006135.shtm。

人工智能在医疗领域的应用形态可分为两类：一类是以诊断设备、机器人和监护仪等硬件设备作为载体，通过人工智能技术的软件组件来驱动和控制这些设备，从而实现其预期功能；另一类是以独立软件形式实现功能，包括手术导航系统、临床辅助决策系统、人工智能大模型等，无需医疗器械硬件的支持[14]。

总体来说，医疗大模型通过高质量的医疗大数据、算力和算法，成为医疗健康产业快速发展的推动力。而医疗器械是医疗大模型的载体，医疗大模型通过各类器械及工具赋能医疗服务。

本部分主要介绍医疗大模型以及人工智能医疗器械合规。

（1）“人工智能+医疗”的行业应用

国家卫生健康委员会办公厅、国家中医药局综合司、国家疾控局综合司于2024年11月6日发布《卫生健康行业人工智能应用场景参考指引》，明确“人工智能+”医疗服务、“人工智能+”医药服务、“人工智能+”健康管理服务、“人工智能+”公共卫生服务等场景的应用方式。

目前AI大模型在医疗行业的主要应用场景包括以下几类：

序号	场景	作用
1	医学影像分析	AI可以帮助医生处理高强度重复的阅片工作，提高影像诊断的效率和准确性。
2	药物研发及精准医疗	AI技术能够加速药物研发的过程，通过对大量的生物数据进行分析和挖掘，帮助药企发现新的药物靶点、预测药物的效果和副作用等。
3	智能诊断辅助	为临床决策提供支持或提供初步诊断意见，通过对话引导患者描述症状，输出可能的疾病列表及紧急程度建议。
4	医疗机器人	医疗机器人可以辅助医生进行手术、康复治疗等操作，提高手术的精度和安全性。例如，微创手术机器人可以在狭小的空间内进行精细的操作，减少患者的创伤和痛苦。

[14]参见甲子光年智库发布：《2024中国AI医疗产业研究报告》，网址为：https://baijiahao.baidu.com/s?id=1805368177650276125&wfr=spider&for=pc。

5	患者交互与健康管理	AI 医生可以为病患提供 7×24 小时症状咨询，通过对个人的健康数据进行分析，提供个性化的健康管理建议，包括饮食、运动、睡眠等方面的指导，帮助人们预防疾病和保持健康。

（2）医疗大模型的合规要点

医疗大模型的合规主要需关注两个层面的问题：第一个层面即大模型本身的合规要素；另一个层面，大部分医疗机构主要是大模型的应用方需关注大模型本地化部署的合规要求。据不完全统计，截至 2025 年 2 月底，约有近百家医院宣布已开始或完成 DeepSeek 在其院内的本地化部署。

①大模型合规要点

在我国当前的监管体系下，医疗大模型应符合相关人工智能及算法的一般性合规要求，主要涉及以下内容：

平台运营合规	1.主体资质：医疗行业大模型涉及多种资质，除传统的增值电信业务经营许可证、B25 类增值电信业务经营许可证（即 ICP 证）、B21 类增值电信业务许可证（即 EDI 证）等互联网领域必备资质外，结合医疗行业的特殊属性还需要具备如医疗器械生产经营许可/备案、互联网药品信息服务资格证书、医疗机构执业许可证、信息系统安全等级保护备案证明等。 2.算法备案：依据《互联网信息服务算法推荐管理规定》，具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息，履行备案手续。 3.大模型备案：依据《生成式人工智能服务管理暂行办法》《生成式人工智能服务安全基本要求》对生成式人工智能服务整体进行备案，该项备案程序在实践中也被称为“大模型备案”。 4.安全评估：算法推荐管理规定、深度合成管理规定以及生成式人工智能管理办法均对安全评估主体作出规定，相关主体应当依据《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》履行安全评估义务。
内容治理	1. 规范生成内容：应当坚持社会主义核心价值观，不得生成煽动颠覆国家政权、推翻社会主义制度，危害国家安全和利益、损害国家形象，煽动分裂国家、破坏国家统一和社会稳定，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，暴力、淫秽色情，以及虚假有害信息等法律、行政法规禁止的内容。[15]

[15] 参见储陈城;魏培林：《生成式人工智能犯罪中研发者刑事责任的认定——以 ChatGPT 为例 》，载《重庆理工大学学报(社会科学)》2023 年。

	2.标识义务：如存在《互联网信息服务深度合成管理规定》第十七条中所列举的可能导致公众混淆或者误认的生成内容，应当进行显著标识。 3.监督、整改及报告义务：发现违法内容的，应当及时采取停止生成、停止传输、消除等处置措施，采取模型优化训练等措施进行整改，并向有关主管部门报告。[16] 4.知识产权合规：从整体上树立“尊重知识产权”的合规理念，应当尊重他人的知识产权，不得擅自使用他人的知识产权，避免侵犯他人专利、商标、著作权等。
网络安全与数据合规	1.数据来源合法性：要使用具有合法来源的数据和基础模型。 2.数据标注义务：制定清晰、具体、可操作的标注规则，标注规则应至少包括标注目标、数据格式、标注方法、质量指标等内容。 3.提高数据质量：采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性。[17] 4.网络安全保障义务：履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。[18] 5.个人信息保护：适用《个人信息保护法》对个人信息的全生命周期进行保护。

②医疗大模型合规要点

具体到医疗行业的大模型开发应用，目前尚未出台具体的法律法规进行规制。除参考上述通用的大模型合规要求之外，主要可参考信通院及行业协会所制定的具体监管要求：

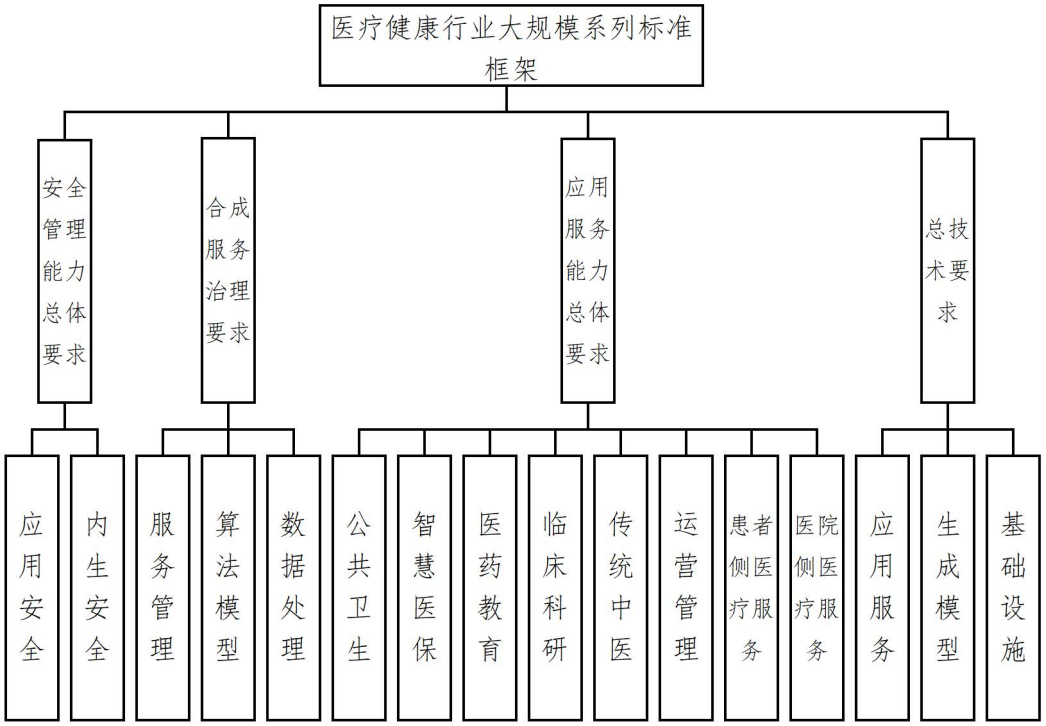
为加快开展“人工智能+医疗健康”工作，培育医疗健康行业新质生产力，中国信通院按照“标准先行”的工作路径，在行业主管部门指导下，与产学研用医各方共同开展医疗健康行业大模型标准研制工作，规范人工智能技术与医疗健康服务的融合路径，推动数字健康产业高质量发展，已形成15项联盟团体标准。

2023年9月25日，中国信通院联合20余家相关产学研用单位共同研究起草的《医疗健康行业大模型应用技术要求第1部分：医院侧医疗服务》《医疗健

[16] 参见《2024人工智能发展白皮书》，网址为：https://max.book118.com/html/2024/0615/8000115120006100.shtm。
[17] 参见阮润生：《生成式人工智能新规发布 A股公司加速掘金》，载《证券时报》2023年。
[18] 参见杨世宏：《金融APP与个人隐私保护的强化问题研究》，载《安徽电子信息职业技术学院学报》2020年。

康行业大模型应用技术要求第 2 部分：患者侧医疗服务》2 项技术要求正式发布，评价指标涵盖场景应用能力、基础模型能力、模型服务能力、性能要求、安全性要求五个方面[19]。

综合行业发展需求及企业产品特点，关注医疗健康 AI 大模型的技术要求，应用服务能力要求、合成服务治理要求、安全管理能力要求，搭建形成行业特色的标准体系。（见下图）



2024 年 10 月 25 日，由武汉大学中南医院牵头，联合省内多家大型三甲医疗机构共同编制的《医疗大模型构建与应用标准》（T/HBSEA013—2024）团体标准，由湖北省软件企业协会正式发布，其中对于医疗大模型的构建及应用的整体工作关注两项重要合规内容：

第一，伦理要求：伦理委员会应作为独立的监督机构，确保医疗大模型的开发和应用符合伦理规范和法律要求，不受开发团队和管理层影响。伦理委员会应在数据收集、处理和使用过程中提供决策和伦理指导，确保项目伦理合规性。

[19]参见《中国信通院首批医疗健康行业大模型应用服务能力符合性验证正式启动》，网址为：https://mp.weixin.qq.com/s/TwTt-igtPGszQrZsGAU6zg。

第二，数据合规要求：针对数据处理，应遵循合法性和透明度、最小化原则以及采取适当的技术和组织措施确保数据的保密性和完整性；在数据共享环节，应注意与合作方签订详细的数据共享协议并对第三方资质和合规情况进行审查；跨境传输场景下还要遵守目的地国家或地区的数据保护法律法规。

在模型构建场景下，本标准对数据的全生命周期处理行为提出了具体要求，其中不仅仅包含对数据安全的要求，也包括对数据质量的追求：

序号	类型	要求
1	数据来源	数据来源多渠道且获得合法授权，确保患者的知情同意，进行标准化采集，实时数据采集，保障安全存储和传输。
2	数据质量	对数据质量控制提出要求，确保数据完整性、准确性、一致性。
3	数据预处理和清洗	应去除无效数据，统一数据格式并进行规范化处理。
4	数据标注与分类	制定统一的数据标准，采用专业的数据标注工具，建立标注审核机制。
5	数据分类	利用自动化分类算法，提高数据分类效率和准确性。

③医疗机构本地化部署大模型的合规要点

医疗机构本地化部署通用大模型从而提升辅助诊疗系统、智能决策平台的效率。现行监管框架对此类创新模式并未提出具有针对性的监管指引，主要可关注以下问题：

第一，医疗机构本地化部署后利用以往医疗数据进行训练：在这个过程中，医疗机构会结合以往收集和存储的各类医疗数据进行标注，生成训练样本再进行训练，需要符合《中华人民共和国个人信息保护法》《信息安全技术健康医疗数据安全指南》的相关规定，同时还应符合《医疗机构病历管理规定》的要求。针对患者的个人信息进行训练的，要关注是否属于授权用途范围。如果超出授权范围还需要征得个人信息主体的再次同意，或考虑将病例数据脱敏清洗匿名化处理及标注后，再生成训练样本。

第二，将大模型应用于辅助决策或诊疗活动时，应充分考虑大模型的算法逻辑和数据来源，要求医疗人员独立审核其输出的建议并进行人工校验。

第三，严禁人工智能自动生成处方。《互联网诊疗监管细则（试行）》明确规定，处方应由接诊医师本人开具，严禁使用人工智能等自动生成处方。

（3）人工智能医疗器械合规

①人工智能医用软件管理类别

2021 年 7 月，国家药监局发布《人工智能医用软件产品分类界定指导原则》（以下简称“分类指导原则”），原则中将“人工智能医用软件”界定为基于医疗器械数据，采用人工智能技术实现其医疗用途的独立软件。医疗器械数据是指医疗器械产生的用于医疗用途的客观数据，特殊情形下可包含通用设备产生的用于医疗用途的客观数据。

根据《医疗器械监督管理条例（2024 修订）》第十三条的规定，第一类医疗器械实行产品备案管理，第二类、第三类医疗器械实行产品注册管理。分类指导原则对人工智能医用软件管理类别提出判定方式：

按照第三类医疗器械管理	算法在医疗应用中成熟度低（指未上市或安全有效性尚未得到充分证实）的人工智能医用软件，若用于辅助决策，如提供病灶特征识别、病变性质判定、用药指导、治疗计划制定等临床诊疗建议。
按照第二类医疗器械管理	用于非辅助决策，如进行数据处理和测量等提供临床参考信息

②人工智能医用器械算法合规

2022 年，国家药监局器审中心发布《人工智能医疗器械注册审查指导原则》（以下简称“审查指导原则”）发布，该指导原则适用于人工智能医疗器械的注册申报。根据上述指导原则规定，“人工智能医疗器械”是指基于“医疗器械数据”，采用人工智能技术实现其预期用途（即医疗用途）的医疗器械。[20]医疗器

[20] 参见《人工智能医疗器械注册审查指导原则》，网址为：https://max.book118.com/html/2023/0602/7051015110005114.shtm。

械数据是指医疗器械产生的用于医疗用途的客观数据。

人工智能技术从发展驱动要素角度是基于模型/数据和算力的算法，其中模型/数据是人工智能技术的基础，算力是人工智能技术的保证，算法是人工智能技术的核心。根据审查指导原则的要求，应结合人工智能医疗器械的预期用途、使用场景、核心功能选择与之相适宜的人工智能算法或算法组合，基于算法特性并结合风险管理开展相应验证与确认工作，特别关注算法的合规性及安全性，并对算法研究报告的内容进行说明列示：

序号	项目	内容
1	算法基本信息	明确算法的名称、类型、结构、输入输出、流程图、算法框架、运行环境等基本信息以及算法选用依据。
2	算法风险管理	明确算法的软件安全性级别（轻微、中等、严重）并详述判定理由。
3	算法需求规范	提供算法需求规范文档，若无单独文档可提供软件需求规范，并注明算法需求所在位置。[21]
4	数据质控	数据来源合规性声明、数据采集操作规范文档、数据整理情况，明确数据清洗、数据预处理的质控要求、提供数据标注操作规范文档。
5	算法训练	依据适用人群、数据来源机构、采集设备、样本类型等因素，提供训练集、调优集（若有）关于疾病构成的数据分布情况。
6	算法验证与确认	依据适用人群、数据来源机构、采集设备、样本类型等因素，提供测试集关于疾病构成的数据分布情况。
7	算法可追溯性分析	提供算法可追溯性分析报告，即追溯算法需求、算法设计、源代码（明确软件单元名称即可）、算法测试、算法风险管理的关系表。[22]
8	结论	简述算法性能综合评价结果，明确对产品的适用范围、使用场景、核心功能所做的必要限制，并判定人工智能算法或算法组合的安全有效性是否满足要求。

5.医疗数据出境场景

[21] 参见《病理图像人工智能分析软件性能评价审评要点》，网址为：https://max.book118.com/html/2023/0710/7064060000005132.shtm。

[22] 参见《血液病流式细胞学人工智能分析软件性能评价审评要点》，网址为：https://max.book118.com/html/2023/0710/5141110000010242.shtm。

“COLORIV 国际多中心临床研究跨境平台合作项目”是首都医科大学附属北京友谊医院(简称“北京友谊医院”)牵头并与荷兰阿姆斯特丹大学医学中心(AUMC)联合发起的,中国和欧洲知名医学中心共同参与的国际多中心结直肠外科临床研究项目。项目中涉及我国境内参与项目研究的受试者个人信息的出境合规和安全保障。该项目也是自 2022 年 9 月 1 日《数据出境安全评估办法》（下称《评估办法》）正式施行后的首个通过数据出境安全评估的申报项目。

实务中存在大量的中外合作医疗项目和跨国经营的医疗健康行业的企业机构，不可避免地产生医疗数据跨境传输的合规问题。

（1）数据出境的合规路径

《国家安全法》《网络安全法》《数据安全法》以及《个人信息保护法》从法律层面建立了数据出境的监管规则。从现有法律框架看,目前我国主要规定了三条数据出境途径：

①安全评估：按照《数据出境安全评估办法》及《促进和规范数据跨境流动规定》的相关规定，符合一定条件的需要通过网信部门组织的安全评估才能进行合规的数据出境；[23]

②标准合同：主要适用于个人信息处理者向境外提供个人信息的情况，需按照网信部门制定的标准合同与境外接收方订立合同；

③认证：按照网信部门规定经专业机构进行个人信息保护认证。

其中,安全评估强制适用于关键信息基础设施运营者和处理个人信息达到规定数量的主体的个人信息出境活动;标准合同及认证都仅适用于未达安全评估标准的个人信息出境活动。

[23] 参见魏如连：《上海自贸区数据跨境“一般数据清单”的国际数字经贸规则规范性研究》，载《《法学前沿》集刊 2024 年第 2 卷——航运法治保障研究文集》2024 年。

出境数据类型 主体类型	重要数据	个人信息
关键信息基础设施运营者	出境安全评估	出境安全评估
数据处理者	出境安全评估	出境安全评估:自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）；或者1万人以上敏感个人信息
		认证、标准合同：自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）；或者不满1万人敏感个人信息的
		免于出境安全评估、认证、标准合同：自当年1月1日起累计向境外提供不满10万人个人信息(不含敏感个人信息）的

（2）医疗场景下的个人信息出境

①自由传输

根据《促进和规范数据跨境流动规定》，符合以下条件之一的，原则上可以自由传输出境，即免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

序号	活动
1	国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的。
2	在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的。[24]
3	为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的。
4	按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的。

[24] 参见《多省市出台支持AI的新政从“%2b”到“×”将成为数字经济影响国民经济奇点》，网址为：https://max.book118.com/html/2024/0504/6055050204010124.shtm。

5	紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的。
6	关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。

《促进和规范数据跨境流动规定》第六条明确了负面清单机制，以自贸区为试点，进一步降低数据跨境门槛。在生物医药领域，一些自贸区已经探索出台了相关清单。例如上海临港新片区管委会于2024年5月发布了《中国（上海）自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单（试行）》，为生物医药企业在临床试验和研究、药物警戒、医学问询与产品投诉、供应商管理等生物医药企业日常经营的数据出境场景下的数据跨境流动提供便利，且明确了去标识化技术对受试者个人信息的保护效果，不再一概将患者健康医疗数据纳入敏感个人信息监管范畴。

②医疗场景下的敏感个人信息识别

敏感个人信息的数量也将影响医疗机构采取何种合规出境的方式。

《个人信息保护法》对“敏感个人信息”定义为“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”

综合《信息安全技术个人信息安全规范》（GB/T35273-2020）以及《网络安全标准实践指南——敏感个人信息识别指南》（TC260-PG-20244A）来看，其中涉及医疗行业的敏感个人信息可包括：

◆ 与个人身体或心理的伤害、疾病、残疾、疾病风险或隐私有关的健康状况信息，如病症、既往病史、家族病史、现病史、传染病史、体检报告、生育信息等；

◆ 在疾病预防、诊断、治疗、护理、康复等医疗服务过程中收集和产生的

个人信息，如医疗就诊记录（医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、诊治情况）、检验检查数据（如检验报告、检查报告）等；[25]

◆ 个人生物识别信息：个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

（3）医疗行业的“重要数据”

医疗行业的重要数据识别对于合规路径的选择也具有影响。

根据《网络数据安全管理条例》第六十二条、《数据出境安全评估办法》第十九条的规定，重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

2022 年发布的《信息安全技术重要数据识别指南（征求意见稿）》对重要数据识别的考虑因素包括“h）反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据属于重要数据；”

根据《数据安全技术数据分类分级规则》（GB/T43697-2024），附录 G 重要数据识别指南考虑因素包括：“n）反映生物技术研究、开发和应用情况，反映族群特征、遗传信息，关系重大突发传染病、动植物疫情，关系生物实验室安全，或可能被利用制造生物武器、实施生物恐怖袭击，关系外来物种入侵和生物多样性，如重要生物资源数据、微生物耐药基础研究数据；p）反映国家或地区群体健康生理状况，关系疾病传播与防治，关系食品药品安全，如涉及健康医疗资源、批量人口诊疗与健康管理、疾控防疫、健康救援保障、特定药品实验、食品安全

[25] 参见李伟华;余佳薇：《保险行业敏感个人信息的识别方法与合规实践——《网络安全标准实践指南——敏感个人信息识别指南》解读》，载《上海保险》2024 年。

溯源的数据。”

医疗机构在识别重要数据时应特别关注上述考虑因素。

《健康医疗数据安全指南》（GB/T39725-2020）提到：“涉及人类遗传资源数据（是指利用人类遗传资源材料产生的数据，人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料）等重要数据的，按照相关部门要求执行。”可见人类遗传资源数据可能被认定为重要数据，其跨境传输均需要向国家网信部门申报数据出境安全评估。

此外，在医疗数据使用披露要求中明确关于医疗数据传输的要求：“o）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，否则应提请相关部门审批。p）经主体授权同意，并经数据安全委员会讨论审批同意，不涉及国家秘密且不属于重要数据的，控制者可向境外目的地传送个人健康医疗数据，累计数据量应控制在250条以内，否则应提请相关部门审批。”

《促进和规范数据跨境流动规定》第二条规定：“数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。”

由此可见，医疗机构可自行结合相关国家标准自行识别判断及申报重要数据，如未被认定为重要数据，则可不作为重要数据申报数据出境安全评估。

（4）人类遗传资源信息出境合规

《健康医疗数据安全指南》（GB/T39725-2020）提到人类遗传资源数据等按照相关部门要求执行；同时又规定“健康医疗数据的出境安全管理，按数据出境安全评估相关办法执行。”由此可见，人类遗传资源信息属于重要数据，如涉及人类遗传资源信息数据出境的，应当采取出境安全评估的方式履行相关合规义务。

①出境安全评估：根据《人类遗传资源管理条例（2024 修订）》第二十七条的规定，利用我国人类遗传资源开展国际合作科学研究，或者因其他特殊情况确需将我国人类遗传资源材料运送、邮寄、携带出境的，应当符合下列条件，并取得国务院卫生健康主管部门出具的人类遗传资源材料出境证明：（一）对我国公众健康、国家安全和社会公共利益没有危害；（二）具有法人资格；（三）有明确的境外合作方和合理的出境用途；（四）人类遗传资源材料采集合法或者来自合法的保藏单位；（五）通过伦理审查。

②安全检查：根据《人类遗传资源管理条例（2024 修订）》第二十八条规定，将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院卫生健康主管部门备案并提交信息备份；如上述行为可能影响我国公众健康、国家安全和社会公共利益的，应当通过国务院卫生健康主管部门组织的安全审查。结合《人类遗传资源管理条例实施细则》的规定，应当进行安全审查的情形包括：重要遗传家系的人类遗传资源信息；特定地区的人类遗传资源信息；人数大于 500 例的外显子组测序、基因组测序信息资源；可能影响我国公众健康、国家安全和社会公共利益的其他情形。科技部会同相关部门制定安全审查规则，组织相关领域专家进行安全评估，并根据安全评估意见作出审查决定。人类遗传资源出口过程中如相关物项涉及出口管制范围，须遵守国家出口管制法律法规。

（三）典型场景数据安全

1. 医生调阅数据场景

医生调阅数据场景适用于医疗机构内医生为患者提供诊疗服务时访问相关医疗数据的过程。在此场景中，医疗机构作为控制者负责数据安全管理。调阅行为需遵循最小必要原则，确保数据在合法、合规、安全的前提下支撑诊疗决策。除满足一般性医疗数据合规要点外，要重点关注以下几方面：

（1）数据分级体系构建

根据数据敏感性和隐私风险，医生调阅场景中的数据可划分为三级：

①默认级（可在较大范围内供访问使用的数据）。如检验检查名称、就诊医院、就诊科室等基础诊疗信息。

②告知级（可在中等范围内供访问使用的数据）。如检验检查报告、手术记录、出院小结等小结类资料。

③授权级（在较小范围内供访问使用的数据）。如住院详细病历、特殊病种（如性病、遗传病、恶性肿瘤）及特殊身份（孕产妇、婴幼儿）数据等。但涉及特殊病种、特殊身份的资料均需要授权或告知。

（2）角色权限定义机制

医生权限基于科室归属、职称等级、诊疗组划分动态分配，确保最小化访问原则。

①科室划分。按医院科室（如消化科、心外科）定义数据调阅范围，医生仅可访问本科室患者数据；

②职称分级。住院医师，仅可访问普通病种数据及特殊病种概要级资料（如诊断名称）；主治医师，可访问普通病种数据及特殊病种摘要级资料（如检查报告）；主任医师，可访问所有级别数据，包括详细病历。

③诊疗组划分。科室内部按诊疗组（如肝胆组、胃肠组）细分权限，医生仅能调阅本组患者数据。

（3）数据标注规范

数据需进行分级标注和颗粒度标注，以匹配权限控制。

①分级标注即定义标识符（姓名、身份证号、生物识别信息等）、特殊病种（明确标注 8 类高风险疾病）、特殊就诊身份（标注婴幼儿、孕产妇、罕见病患者等敏感身份）。

②颗粒度分类。概要级：仅含诊疗基础信息（如就诊时间、科室）；摘要级：包含诊疗过程关键结论（如手术小结）；详细级：涵盖完整诊疗记录（如病程记录、用药详情）。

（4）权限分配示例

结合角色权限定义与数据标注规范，形成权限分配的规则。

角色	权限
科室医生	仅可调阅本科室患者数据
住院医师	仅可调阅普通病种资料及概要级特殊病种资料
主治医师	仅可调阅普通病种资料及摘要级特殊病种资料
主任医师	可调阅普通病种资料及详细级特殊病种资料
诊疗组	仅可调阅本诊疗组管辖范围内患者资料，不可调阅本科室其他诊疗组内患者资料

例外：传染性疾病数据默认向接诊医护人员开放，以保障医疗安全。上级医生可查看下级医生管辖患者数据，但不可反向操作。

（5）身份认证与访问控制

①多因素结合身份鉴别。采用账号口令、数字证书、生物识别（指纹/人脸）组合认证等。

②动态权限管理。角色随人事变动（如职称晋升、科室调整）自动更新权限等。

③访问环境限制。仅允许院内 IP 调阅，非工作时间访问视为异常行为。无操作 10 分钟后自动锁屏，防止未授权访问等。

（6）数据调阅过程管理

①患者知情同意。如调阅跨机构数据时，需患者扫码授权等。

②异常行为监控。系统实时监测调阅行为，记录访问轨迹（IP、时间、内容）。触发报警阈值后自动阻断访问，并通过短信、邮件通知管理员等。

③日志审计与留存。调阅日志保存期≥6 个月，定期审核敏感数据访问记录。重点审计特殊病种、高敏感数据及特殊身份患者数据调阅行为等。

2.患者查询数据场景

患者查询数据场景适用于个人通过在线系统（如医院 APP、区域健康平台等）查询自身健康医疗数据的场景。医疗机构或健康服务平台作为控制者，需确保患者查询行为的安全性、隐私性及数据完整性。核心目标包括：防止未授权访问、限制敏感信息披露、保障数据传输安全。

（1）重点安全措施

①身份识别与账户管理。首次注册需绑定实名制手机，通过短信验证码完成身份核验。支持监护人代理查询（如子女代父母、父母代子女），需上传身份证明文件（身份证、户口本）并通过后台审核。强制设置符合复杂度要求的密码（如包含大小写字母、数字及特殊字符），定期提示用户更新密码（建议每 90 天更换一次）等。

②信息查询限制。默认隐藏敏感数据（如 HIV 检测、肝炎结果）等高敏感信息，需患者线下联系医疗机构获取。仅开放三个月内的检查检验报告、用药记录等非敏感数据供在线查询。历史数据需患者提交申请并经医疗机构审核后开放等。

③操作权限控制。

A.功能权限分级：

基础操作：允许查看、浏览数据。

高风险操作：下载、打印、另存为等需二次授权，系统弹出用户须知提示数据泄露风险。

警示标识：下载页面需以红色字体标注“数据安全责任由本人承担”等警示内容。

B.操作日志追踪：

记录患者账户的查询、下载行为（包括时间、设备 IP、操作类型），日志留存≥6 个月。

④数据传输安全保障。默认启用传输层加密，确保数据在传输过程中的保密性。采用哈希校验或数字签名技术，防止数据在传输中被篡改。移动端应用强制开启数据加密功能，禁止通过未授权第三方渠道传输数据等。

（2）风险防控

①异常访问拦截。系统实时监测异常登录行为（如异地 IP、频繁失败尝试），自动触发账户锁定或人工复核流程。

②数据泄露应急响应。发现数据泄露后，立即暂停患者账户功能，通知用户修改密码并追溯泄露源头。

③定期安全审计。医疗机构每季度审查患者查询日志，重点排查敏感数据访问记录及高频下载行为等。

3.临床研究数据场景

临床研究数据安全适用于学术性医学中心、医疗机构、科研机构等开展回顾性研究、前瞻性研究、真实世界研究等场景，涉及患者健康医疗数据的采集、传输、存储及使用。研究过程中，需遵循伦理规范、最小必要原则及数据安全标准，保障受试者隐私与数据完整性。除满足一般性医疗数据合规要点外，要重点关注以下几方面：

（1）核心安全措施

①伦理审查与知情同意。研究开始前，将研究计划报相关医疗机构的伦理委员会审批。涉及人类遗传资源收集的，同时向相关部门申报批准。原则上需受试者签署知情同意书，明确数据使用范围及目的。允许患者授权去标识化数据用于未来研究（需就诊时签署）。与此同时，存在例外与豁免情形，如回顾性研究无法追溯受试者时，经伦理批准可免除同意（数据需去标识化）；真实世界研究在

去标识化前提下，可豁免知情同意。

②数据分级与分类。公用数据集（PUF）：汇总统计级数据（如疾病年度发病率），可公开共享；受限制数据集（LDS）：患者级数据，去标识化处理（如加密姓名、地址），需授权访问；可标识数据集（RIF）：含直接标识符（如身份证号、基因数据），仅限必要场景使用。

③采集、传输、存储与使用。采集阶段，采用双人录入或电子数据采集系统（EDC），确保数据准确性。避免收集非必要标识符（如全名），以代码替代患者身份。传输阶段，机构与申办者间通过如专线/VPN 等加密传输方式，离线数据存储介质需加密且与密钥分离。禁止开放未审批端口，数据存储类服务严禁外网暴露。存储阶段，患者知情同意书与代码索引由医疗机构独立保存（纸质加锁/数字加密）。数据备份≥3 份，定期验证恢复有效性，研究结束 5 年后需匿名化或删除等。使用阶段，数据库锁定后禁止修改，数据变更需记录稽查轨迹（时间、操作人、变更内容等）。多中心研究集中管理数据，统计分析仅开放去标识化数据集。

④权限与审计控制。研究者、数据管理员、统计师等主体分配独立账号，按职责限制操作权限。需全流程审计，记录登录、数据修改、导出等行为。定期审查异常访问（如非工作时间调阅、高频下载），触发自动报警与权限锁定。

⑤数据共享与发布。科研数据平台分级开放，需签署保密协议并注明数据来源。政府资助数据原则上公开共享（涉密除外），商业用途需签订有偿协议。共享数据需附加隐私声明及溯源标识，确保可追溯至原始数据。论文、专利中引用数据需标明来源，禁止泄露患者身份信息。

4.二次利用数据场景

二次利用数据安全适用于第三方（政府部门、科研机构、企业等）出于非营利性目的（如科研、创新竞赛）申请使用已脱敏或去标识化的健康医疗数据，且

无法直接联系数据主体或联系成本过高的场景。控制者（如医疗机构、区域卫生信息平台）负责数据全流程管理，第三方作为使用者需遵循最小必要原则与安全协议，确保数据在二次利用中的隐私性与合规性。二次利用数据安全通过分级管理、动态审批、去标识化强化及全生命周期监控，构建了兼顾科研创新与隐私保护的管理框架。控制者需完善数据资源目录、优化审批机制，第三方应严格遵守安全协议，共同维护健康医疗数据在二次利用中的合法性与安全性。重点关注以下几个方面：

（1）数据分级与资源准备

①分级标准

无标识数据集：群体统计数据（如某疾病年度发病率），无个体标识，可公开共享。

受限制数据集：患者级数据，去除直接标识符（如姓名、身份证号），需授权访问。

可标识数据集：含敏感标识符（如地址、基因组数据），仅限特殊研究需求（如流行病学追踪）。

②资源目录建设：

控制者公开数据资源目录，提供字段说明、样本量、年份及申请条件，提供第三方评估需求。生物组学数据按类型（如基因组、代谢组）封装，明确数据包内容与使用限制。

（2）数据申请与审批机制

控制者对数据申请者的身份进行限制，如限定申请者为科研人员，在其研究领域有丰富经验和相应的职称，社会信用达到A级等。并对申请渠道进行限制。同时规范数据使用目的，仅可用于非营利性目的，申请提取的数据内容与研究主题紧密相关，满足最少必要原则。

控制者成立数据安全专委，建立审批专家库，制定审批规则及流程。制定科学、定性或定量的数据申请审批指标。

维度	**指标**
合法性、正当性	是否符合相关法律规范要求
数据申请与数据需求一致性	数据使用过程中是否会应用申请数据，控制超范围申请，保障最少必要性
数据使用价值	数据本身价值、数据应用价值
数据泄露风险	影响人数、涉及病种、患者损失等
提供数据成本	提取、清洗、去标识化、传递所耗费的人力物力等

（3）数据去标识化处理

标识符定义：明确姓名、住址、联系方式等直接标识符，严格删除或加密。

最小计数原则：同一描述的患者数≥5，否则泛化（如“宫颈癌”患者仅仅4人，则需要将“宫颈癌”泛化处理）。

重标识检测：通过算法验证数据不可逆，防止通过关联信息回溯身份。

（4）安全传输与使用管控。

无标识数据：加密邮件或加密USB设备（需专用电脑解密）等方式传递。受限制/可标识数据：采用虚拟桌面远程分析（仅允许导出统计结果）或数据沙箱环境等方式。签署数据使用协议，明确保密义务、使用期限及泄露追责条款。禁止数据转售、共享或用于训练商业模型。

（5）数据销毁与溯源管理

使用期满后，第三方需书面通知控制者并提交销毁证明（如存储介质消磁记录）。控制者核查销毁结果，违规者列入黑名单并追究法律责任。公开发表的研究需注明数据来源，确保溯源可查等。

5.健康传感数据场景

健康传感数据指通过可穿戴设备、智能医疗设备等传感器采集的与个人健康

状况相关的数据（如心率、血压、血糖、睡眠监测、运动轨迹等）。该场景涉及个人主体、控制者（如医疗机构、健康服务企业等）及处理者（如设备厂商、信息系统服务商等），需确保数据从采集到使用的全流程安全，防止泄露、篡改及未授权访问。

（1）隐私保护与知情同意。设备首次使用时需明确告知数据采集范围、用途及共享对象，用户需主动授权。未经用户同意，不得向第三方披露原始数据；集成多源数据时需二次告知用途。

（2）数据采集安全。设备身份认证需要求用户通过生物识别（指纹、虹膜等）、密码或数字证书验证设备使用权。设备与终端（如手机、云端）通信时启用节点认证，防止非法设备接入。用户可自主开启/关闭传感器数据采集功能，选择上传内容（如屏蔽定位信息）。设备固件需定期更新，修复漏洞，禁用非必要服务端口。

（3）数据传输与存储安全。默认启用如 TLS、IPSec 等协议加密传输链路，保障数据保密性与完整性。公共网络传输时强化加密强度，避免遭受攻击。加强存储防护，本地设备存储数据需加密（如 AES-256），密钥与数据分离保存。云端存储采用分布式加密及访问控制，定期备份并验证可恢复性。设备丢失或被盗时，支持远程擦除数据功能，防止信息泄露。

（4）数据使用与审计。基于角色合理、精细化定义分配访问权限（如医生仅可查看诊疗相关数据），禁止超范围调阅，敏感操作（如批量导出）需二次审批。严格行为审计，记录数据访问、修改及共享行为，日志留存。实时监测异常操作（如高频调阅、非工作时间访问），触发告警并自动阻断等。

6.移动应用数据场景

移动应用指为个人提供在线健康医疗服务（如在线问诊、电子健康档案查询等）或健康数据管理的应用程序，涵盖医疗咨询、健康监测、保险理赔等场景。

移动应用数据安全通过采集合规化、权限最小化、传输加密化及存储冗余化构建防护体系。应用发布者需强化技术防护与第三方监管，用户应主动管理授权权限，共同维护健康医疗数据的隐私与完整性。除参照和满足一般性医疗数据合规要点外，要重点关注：

（1）数据采集合规性。参照《GB/T 35273 信息安全技术 个人信息安全规范》，制定隐私政策，明确数据收集类型、用途及共享范围。严格执行最小必要原则，仅采集与业务直接相关的数据，禁止超范围获取（如健康应用索要通讯录权限）。宜采取动态授权机制，敏感操作（如调阅病历）需实时弹窗获取用户同意，支持随时撤回授权等。

（2）访问控制强化。登录采用“账号密码+短信验证码”或生物识别（指纹、虹膜等），特权操作（如数据导出）需二次认证（如动态令牌）。建立并确保有迹象表明身份可能已经被泄露时还可以利用其他方法或技术进一步验证用户身份的机制。权限精细化管理，按角色（医生、患者、管理员）分配权限，遵循“最小授权”原则。离职员工账号即时冻结，定期清理冗余账户等。

（3）传输加密保障。端到端加密：采用如 TLS 1.3、HTTPS 等协议加密传输链路，防止攻击。敏感数据特殊处理，生物特征信息（如指纹）仅传输摘要值，禁止原始数据网络传输。支付数据符合 PCI DSS 标准，隔离存储与传输通道等。

（4）存储安全防护。提供并使用管理、物理和技术保护等措施，保护用户信息免受未经授权的泄露或访问。可采用每日增量备份、每周全量备份，灾备数据异地存储（≥3 份）等方式定期备份数据。本地数据加密化处理，密钥与数据分离管理；云端数据启用分布式加密，定期轮换密钥。移动介质存储，需对介质上数据进行加密，防止数据受到未经授权的泄露或访问。存储个人生物识别信息时，宜采用技术措施处理后再行存储，如仅存储个人生物识别信息摘要等。

（5）应用安全加固。去标识化展示方面，界面显示患者信息时隐去直接标

识符；报告下载自动添加水印，关联用户账号与时间戳。系统漏洞防护方面，定期更新补丁，禁用高风险端口（如 Telnet、FTP）；集成防病毒引擎，实时监测恶意代码注入。第三方服务监管方面，供应商接入前需通过安全评估（如 ISO 27001 认证）；API 接口限流限频，监控异常调用行为（如每秒超 50 次请求）等。

7.商业保险对接场景

商业保险对接场景适用于医疗机构与商业保险公司系统互联，实现患者医疗费用实时结算、理赔审核等业务。医疗机构作为控制者负责数据源管理，商业保险公司作为使用者需遵循最小必要原则获取数据，双方通过技术与管理协同保障数据在传输、使用、存储环节的安全性，防范数据泄露与滥用风险。

（1）涉及数据类型

个人属性数据，如姓名、性别、证件号、联系方式、住址等；健康状况数据，如诊断结果、检验报告、手术记录、用药史等；医疗应用数据，如诊疗明细中的药品/服务名称、单价、数量、自付比例等；病案信息，如入院诊断、出院小结、手术名称、病理诊断等；医疗支付数据，如住院号、结算金额、医保类型、报销比例等；卫生资源数据，如医院名称、等级、科室信息等。

（2）对接环节安全措施

①对接前准备。医疗机构与保险公司互相验证主体合规性（如经营许可、信用评级、资质等）。签订数据使用协议，明确相关授权、数据范围（如仅限理赔相关字段）、使用期限、保密义务及违约责任等内容。双方系统需通过等保三级认证，接口上线前完成渗透测试与漏洞扫描等技术工作，确保传输的安全性，符合国家、监管机关和对接双方的安全要求。禁止开放非必要端口（如数据库默认端口），关闭冗余服务等。商业保险公司需提交数据使用申请，列明字段用途（如“药品名称”用于理赔范围核验），超范围需求需重新审批等。

②对接中管控。参照医疗数据一般性合规要点，重点把握数据传输安全、数

据使用安全、数据存储安全，并建立访问控制与审计机制。数据同步管理方面，设置数据丢失重传机制，异常中断后自动校验续传，防止数据缺失。禁止直接访问医疗机构生产库，通过中间库隔离并限制查询频次（如每秒≤5 次）等。

③对接后治理。参照医疗数据一般性合规要点，重点把握数据存储安全、数据销毁与介质处理。

（3）风险防控与应急响应

参照医疗数据一般性合规要点内容，建立相关制度、机制，重点把握异常行为的监控机制和手段、第三方供应商的安全管理、数据泄露应急处置机制和方案等。

8.医疗器械数据场景

医疗器械数据安全涵盖具有联网或存储功能的医疗设备（如影像系统、检验设备、AI 辅助诊断软件等）在生产、使用及维护环节中的数据管理。医疗器械厂商负责产品安全设计，医疗机构作为控制者确保临床使用合规性，维护方（厂商或第三方）作为处理者需遵循协议约束，共同保障患者诊疗数据与设备日志信息的保密性、完整性及可用性。医疗器械使用中的数据安全，属于医疗机构内部数据安全范畴，参照本合规要点相关章节内容。本章节重点关注医疗器械产品研发及维护环节。

（1）涉及相关方与数据范围

①相关方角色

厂商：研发生产环节确保设备内置安全能力。

医疗机构：使用环节管理设备数据访问权限。

维护人员：远程或现场维护时处理设备日志、维护记录等数据。

②数据类型

诊疗数据：患者影像、检验结果、诊断报告等。

设备日志：操作记录、故障信息、维护历史（时间、操作人、维护内容）。

维护数据：软件补丁、固件版本、校准参数等。

（2）研发与生产环节

医疗器械厂商在产品研发过程中，参照相关的国际、国家标准和技术报告，进行器械网络安全能力建设，进行系统加固等方面的设计工作。

①传输认证。支持白名单、数字证书或生物识别（如指纹）验证设备使用者身份，并确保传输过程中健康医疗数据保密性手段。

②数据导出控制。若导出含患者信息，需提供去标识化功能（如替换姓名为患者代码）。

③数据完整性保障。产品宜提供相关技术手段使得存储在本地的，在系统故障恢复后、发生故障前的医疗数据可获取，并提供医疗数据的备份、归档、恢复手段。

④审计跟踪。创建审计跟踪来记录和检查用户行为。审计记录确保不被修改或删除。跟踪行为至少应包括：身份认证、医疗数据的查询、建立、删除、修改、导入、导出、网络传输等。

⑤系统加固。器械厂商要对产品实施系统加固，保证用途下确保安全最大化。加固方式至少包括：防火墙设置、关闭非必要端口、禁用未授权服务、操作系统、应用软件漏洞安装维护等。

（3）维护环节数据管理

①数据采集安全。维护人员需通过授权访问认证机制，建立安全连接，仅允许访问指定设备日志，进一步强化控制访问来源（如特定公司的特定维护人员可以访问等）。导出医疗数据时自动去标识化，禁止保留原始患者标识符。通过远程桌面访问时，确保得到医疗器械操作人员或医疗机构工作人员的认证或授权等。

②数据传输与存储。使用如 TLS 或 IPSec 加密维护通道，离线数据存储介质

需采取技术加密措施。通过哈希算法（如 SHA-256）校验数据未被篡改，确保完整性验证，并定期备份日志及异地存储。

③权限与审计。维护人员仅可访问设备日志，无权调阅患者病历；数据导出与密钥管理由不同角色执行。记录维护人员数据访问行为，异常操作（如频繁下载日志）触发告警并锁定账号。

（4）组织管理要求

参照本合规要点相关章节内容，全面建立相关机制。重点建立安全策略、规程和管理流程，定期进行安全风险评估与管理，制定和执行安全运维，制定应急管理策略并定期开展演练，确保安全责任，并对员工进行安全管理、安全培训和考核。厂商与医疗机构签订维护协议，明确数据安全责任及泄露追责条款，定期对医护人员、维护人员开展数据安全与隐私保护培训，制定数据泄露预案，设备丢失或遭攻击时立即断网、擦除数据并上报等。

（5）特殊场景管理

医疗器械数据涉及如基因数据、AI 医疗等特殊模块，需另行依据国家专门法律规范处理，不纳入医疗器械一般性合规范畴，相关内容参照本合规要点“特殊场景下的医疗数据合规”章节。

五、其他商业化应用场景

医疗数据作为医疗行业的核心资产，其潜在价值在技术进步和应用场景拓展中逐渐显现。随着大数据、人工智能等新兴技术的不断成熟，医疗数据的应用已从传统的临床决策支持、疾病监测等领域，逐步扩展到市场调研、行业分析、疾病筛查与防控、医疗器械不良事件监测、医检数据治理以及人工智能辅助医疗健康服务等多个创新领域。这些应用不仅为医疗行业的智能化转型提供了有力支持，也为实现高效的人群健康管理、医院降本增效以及

满足医务工作者的临床与科研需求奠定了坚实基础。

（一）市场调研与行业分析：精准数据赋能产业发展

随着大数据、人工智能等新兴技术的不断成熟，医疗数据的应用已从传统的临床决策支持、疾病监测等领域，逐步扩展到市场调研、行业分析等多个创新领域。据 IDC 报告显示，2023 年中国医疗大数据市场规模达到 34.5 亿元人民币，医疗大数据建设和应用正在进入数据价值的深入挖掘阶段。通过对海量匿名化医疗数据的深度挖掘与分析，医疗数据能够为市场调研和行业分析提供精准的数据支持。例如，某集团自主研发的“某呼吸道病原体检测阳性率分析报告”，通过整合历史数据与实时监测数据，不仅可预测呼吸道感染的流行趋势，助力政府和卫生部门提前部署防控措施，还可解析病原体的传播规律及感染人群特征，为疫苗接种计划和公共卫生政策制定提供科学依据。此外，该数据产品还为医药及医疗器械企业的产品研发和市场布局提供了精准指导，助力企业预测细分市场需求，开发针对性的抗病毒药物、抗生素、多联检试剂盒及快速检测技术，满足临床对于高流行率病原体的快速筛查诊断需求。同时，这一数据产品也为科研机构的医学研究提供了宝贵支撑，推动特定病原体的流行特征、传播规律及变异情况等基础研究的开展。

（二）疾病筛查与防控服务：助力疾病的早发现、早干预

在疾病筛查与防控领域，医疗数据的应用能够显著提升疾病的早发现、早诊断与早治疗能力。以宫颈癌筛查为例，广州金域医学检验集团股份有限公司携手广东省疾病预防控制中心及广州医科大学附属妇女儿童医疗中心，基于超 1 亿例宫颈癌数据积累，建立了涵盖数据采集、治理与应用的整体解决方案，搭建了宫颈癌数据分析平台，提供全国多中心的宫颈癌筛查一站式数据服务。该项目通过合法渠道收集数据，并获得患者的知情同意，同时建立严格的数据质量控制机制，对数据进行清洗、验证和校验，确保数据的真

实性和准确性。此外，通过数据安全评估，采用数据加密、匿名化等技术手段，防止数据在共享过程中被泄露或滥用，确保数据在不同机构之间的安全可靠流通，为公共卫生决策提供有力支持。

（三）医疗器械不良事件监测：保障器械安全与有效性

医疗器械不良事件监测是保障医疗器械安全性和有效性的重要环节。江门市人民医院通过建立完善的数据收集与分析体系，研发了“江门市人民医院医疗器械不良事件报告”的数据产品，旨在通过先进的数据分析技术，为医疗器械的安全性监管提供强有力的支持。该数据产品通过对医疗器械使用过程中产生的患者情况、器械使用情况及不良事件数据进行分析，科学监测医疗器械的安全性和有效性，帮助监管机构、制造商和服务提供者掌握产品实际使用情况，为监管合规、风险管理、产品改进及公众安全等方面发挥关键作用。数据处理主体通过合法渠道收集数据，并获得患者的知情同意，同时建立严格的数据安全管理制度，采用加密存储、访问控制、数据备份等技术手段，保障数据的安全性和保密性。此外，数据仅用于医疗器械的安全性监管、风险管理和产品改进等合法用途，确保数据使用过程的合规性。

（四）医检数据治理与应用：提升医疗数据质量与价值

医检数据的有效治理与应用能够为医疗行业及相关领域提供重要的数据支持。金域医学率先对其积累的神经免疫系统疾病与感染性疾病两大类检测数据进行治理，成功完成了两款数据产品的资产登记。其中，“金域医学神经疾病相关抗体送检情况及阳性率分析报告”可提供不同地域神经免疫系统疾病患者的抗体阳性率分析，为制药企业、医疗机构及科研机构的药品研发工作提供宝贵数据支持；“金域医学结核分枝杆菌耐药地图”则结合网页端地图，直观呈现结核分枝杆菌耐药的地域分布及趋势，为政府及医疗机构的公共卫生监控、防控政策制定及精准治疗提供数据支撑。数据处理主体制定

了详细的数据治理方案，明确数据采集、清洗、转换、存储等环节的操作规范，同时建立数据质量评估指标体系，定期对数据质量进行评估和监控，确保数据的准确性、完整性和一致性。此外，对患者的个人信息进行匿名化处理，仅保留与疾病检测相关的必要数据，明确数据的使用权限和范围，通过合法的授权协议，确保数据仅用于药品研发、科研工作、公共卫生监控、防控政策制定等合法合规的用途。

（五）AI 辅助医疗健康服务：推动医疗服务智能化升级

人工智能技术与医疗数据的结合为医疗健康服务带来了新的突破。例如，深圳罗湖“AI+医疗健康”创新应用场景通过运用人工智能辅助眼底诊断技术，搭建“眼底人工诊断平台”，为糖尿病患者开展眼底筛查，实现糖尿病视网膜病变的早期发现与干预。该项目在国内率先将基于 AI 定量技术的远程辅助诊断系统应用于社区大规模糖尿病视网膜病变筛查及糖尿病患者的常规眼底检查，开创性地将眼底定量化指标用于糖尿病的随访管理，有效破解了医疗资源不足与地域分布不均的困境，提升了糖尿病患者眼底检查覆盖率，推动了糖尿病远程会诊与分级诊疗体系建设。数据处理主体确保所使用的医疗数据符合相关法律法规和政策要求，数据来源合法，且经过患者授权，同时对数据进行严格的隐私保护和安全处理，防止数据泄露和滥用。此外，对 AI 算法的准确性、可靠性和公平性进行评估和验证，避免因算法偏差导致误诊或漏诊，确保模型的可解释性，使医生和患者能够理解 AI 诊断结果的依据，推动医疗服务智能化升级。

附件 1：医疗数据使用授权协议

医疗数据使用授权协议

尊敬的患者（以下简称“您”），_____医院（以下简称“本院”）重视患者的隐私，您在通过手机应用（包括但不限于微信公众号、微信小程序、支付宝生活号、 以及手机 APP）和线下使用本院疾病诊疗服务过程中，本院将按照《医疗数据使用授权协议》（以下简称“本协议”）、《个人信息保护法》《数据安全法》《网络安全法》等法律法规及政策性文件的要求，采集、存储、使用、加工、传输您的个人医疗信息。为了保证对您的个人医疗数据合法、合理、适度地采集、使用，并在安全、可控的情况下进行传输、存储，本院制定了本协议，请您仔细阅读本协议并确认了解本院对您医疗数据的处理规则。阅读及使用过程中，如您有任何疑问、个人信息安全投诉或举报，可联系本院的患者服务、投诉、举报热线进行咨询、投诉、举报，本院将于 15 个工作日内为您进行处理。如您就本协议线上或线下点击或勾选“同意”，并确认提交，即视为您同意本协议，同意本院将按照本协议的相关规定来采集、存储、使用、加工和传输您的相关医疗数据。您不同意以本协议约定的方式处理您医疗数据的，本院不会拒绝向您提供产品或者服务，医疗数据属于提供产品或者服务所必需的除外。

一、授权范围

（一）基础授权范围

您□同意□不同意本院在以下范围内使用其医疗数据：

1.医学研究：对医疗数据进行分析研究，以探索疾病的发生机制、发展规律以及不同治疗方法的效果评估，推动医学知识的进步和创新。

2.临床诊断参考：在临床实践中，为医生提供辅助诊断建议，帮助医生更准确地判断病情，制定更合理的治疗方案，从而提高医疗服务质量和效率。

（二）扩展授权范围

1.（□同意□不同意）第三方合作研究：与国内外其他科研机构、高校、企业等开展合作研究项目，共享医疗数据以实现更广泛的研究目的，但本院应确保第三方遵守与本院相同的保密义务和数据使用规范。

2.（□同意□不同意）商业用途开发：在符合法律法规的前提下，将匿名化后的医疗数据用于与医疗服务相关的商业产品或服务的开发与推广，如开发新型诊断试剂、治疗药物、医疗器械等，但本院应确保商业活动的开展不会损害您的合法权益。

3.（□同意□不同意）公共卫生统计与政策制定：向卫生行政部门等提供脱敏后的医疗数据统计信息，用于公共卫生状况的监测、疾病预防控制策略的制定以及医疗资源的合理配置等公共卫生管理工作。

4.（□同意□不同意）AI 辅助诊断系统训练：将您医疗数据作为训练数据，用于提升 AI 在疾病诊断方面的准确性和可靠性，涵盖但不限于脑卒中、胸痛、肺结节、骨折、骨龄评估、QCT 及下肢血管等疾病的诊断系统训练。

5.（□同意□不同意）专业人员培训：作为教学案例，用于医学专业学生、住院医师、进修医生等的培训教育活动，提升医学人才的专业素养和实践能力。

6.（□同意□不同意）商业保险定价及理赔：将您的医疗数据与相关的商业保险企业进行共享，用于商业保险企业根据您的过往病史、检测结果，依据公平合理的规则进行特定保险产品的价格评测。此外将您的数据向商业保险企业进行提供能够极大地方便您的就医及后续保险结算流程。

（三）医疗数据的数据接收方信息

数据接收方名称	利用用途	患者授权
		□同意□不同意

		□同意□不同意
		□同意□不同意
		□同意□不同意
		□同意□不同意

（四）本院将采取合理的安全手段保护您提供的医疗数据，不会擅自将患者医疗数据超出上述授权范围披露给任何无关的第三方，但涉及下列情形之一的除外：

1.由于患者对自身医疗数据保密不当，从而导致患者医疗数据的泄露、被盗或者患者自行向社会公众公开的医疗数据；

2.与国家安全、国防安全有关的，或与公共安全、公共卫生、重大公共利益有关的，或与政府管制、政策影响有关的；

3.相关司法机关依照法定程序要求提供的，或者有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的；

4.根据与您签订和履行相关协议或其他书面文件所必需的；

5.法律法规规定的其他情形。

二、儿童医疗数据特别授权

（一）未成年人同意本协议，必须在其父母或者其他监护人的监护下进行。本院将根据国家相关法律法规的规定保护未成年人的个人信息的保密性及安全性。

（二）监护人验证机制

14 周岁以下患者需完成双重身份核验，即监护人身份证件扫描件上传（含人脸识别活体验证）和监护关系证明（出生医学证明/户口簿）电子件提交。

（三）撤回授权条款

作为未成年人的法定监护人，您可以通过生物特征验证（人脸识别+身份证件核验）行使撤回权，并需上传监护关系证明文件。您可以行使的撤回方式包括医院

手机应用、官网专用通道及线下窗口办理，撤回后48小时内冻结数据接口，但已用于科研的匿名化数据集不受影响。涉及遗传信息撤回将同步通知伦理委员会备案，监护人可在线查看撤回操作进度。撤回效力不溯及已完成的诊疗数据流处理。

（四）特殊处理机制

出于对未成年人权益的保障，监护人可要求查阅数据使用日志（含访问时间、用途、操作人员）和获取数据脱敏处理技术说明。

三、授权期限

本授权书自您签字之日起生效，有效期为____年。授权期限届满后，若您未以书面形式提出终止授权，本授权自动延续____，延续次数不限。

四、患者权利

根据《个人信息保护法》及相关规范，您就授权的医疗数据享有以下法定权利：

（一）知情权

您有权随时了解其医疗数据的存储情况，知悉其医疗数据存储的位置、存储期限以及存储的安全措施，有权了解其医疗数据被用于何种目的、以何种方式使用，以及使用数据的具体流程，有权知晓其医疗数据在处理过程中的具体情况，包括但不限于数据的收集、整理、分析等环节。

（二）选择权

您可自行决定授权的医疗数据范围，如仅授权特定类型的医疗数据，或仅授权在特定情况下使用其医疗数据，可以选择通过电子签名、点击确认等方式进行授权，也可以选择不进行授权。

（三）撤销权

您可以通过线上或者线下的方式来撤销授权，撤销授权后72小时内完成数据链路清除（含第三方协作单位数据副本销毁），但基于匿名化处理且无法关联个人

身份的科研数据集除外。

（四）更正权

您可以在发现数据标注错误后在线提交医学影像复核申请(需附三甲医院诊断证明），系统应在15个工作日内完成数据校验与修正。

（五）数据可携权

您可要求以结构化格式获取原始医疗数据包，医疗机构应在30日内通过国密算法加密传输。

（六）限制处理权

对AI辅助诊断结论存疑时，患者有权要求建立人工复核隔离区（数据仅限副主任医师及以上权限访问）。

（七）删除权

患者可发起不可逆删除请求，但依法需保留的医疗数据医疗档案除外。门急诊医疗数据存档时长至少为患者上一次就医日期之后的15年，住院医疗数据按30年医学档案标准保存。

四、数据安全保障

本院承诺将采取严格的数据安全保障措施，确保您医疗数据的保密性、完整性和可用性。具体措施包括但不限于：

（一）数据加密

本院将通过存储加密和传输加密对您提供的医疗数据进行加密处理，确保数据在存储、传输和使用过程中的安全性。

（二）访问控制

本院将实施动态权限管理，遵循最小权限原则来建立严格的访问权限管理制度，仅允许经过授权的人员在特定的工作场景下访问和使用您的医疗数据，并对访问行为进行记录和监控。

（三）数据备份与恢复

本院定期对您的医疗数据进行备份，并制定数据恢复计划，以防止数据丢失或损坏。

（四）安全审计与监控

本院将定期对数据使用情况进行安全审计，及时发现和处理潜在的安全隐患。

（五）数据生命周期管理

本院保证门诊医疗数据保留期限为患者末次就诊后 15 年，住院数据保留 30 年，数据销毁采取不可逆擦除技术并经伦理委员会审批。

五、违约责任

（一）若本院违反本授权书的约定，超出授权范围使用您的医疗数据，本院应立即停止违约行为，并承担相应的违约责任，包括但不限于赔偿您因此遭受的全部损失。

（二） 若本院未履行数据安全保障义务，导致您的医疗数据泄露、丢失或损坏，本院应承担相应的赔偿责任，并采取补救措施以减轻对您造成的不利影响。

（三）若您违反本授权书的约定，提供虚假的医疗数据或就同一医疗数据向其他方授予导致本院权益受损的类似授权，您应承担相应的违约责任，包括但不限于赔偿本院因此遭受的全部损失。

六、争议解决

（一）因本协议（含补充协议）引起的或与本合同相关的争议，双方应友好协商解决。若协商不成，任意一方有权向有管辖权的人民法院提起诉讼。

（二）争议处理期间，相关数据须采用区块链存证技术进行保全，确保数据完整性与不可篡改性。

（三）涉及跨境数据争议的，应优先适用中国司法管辖。

（四）本条款与主协议具有同等法律效力，争议解决期间数据控制方不得单方面

变更授权范围。

七、免责声明

本院在国家相关法律法规规定的范围内，按现有状况和诊疗规则提供相应的诊疗服务，发生下列情形之一的，本院不承担责任：

（一）因不可抗力（包括但不限于地震、台风、水灾、火灾、战争及其他不能预见、不能避免且不可克服的客观事件）导致的；

（二）因不可预测或无法控制的系统故障、设备故障、通讯故障、线路故障、停电、黑客攻击、计算机病毒等突发事件或第三方原因给会员造成的损失；

（三）因法律和政策发生变化或政府机关、司法机关采取措施、提出特殊要求的；

（四）患者在本院提供的有关个人信息不真实，或者违反任何保证、承诺或法律规定的；

（五）任何非经患者授权或许可的第三方非法使用患者的名称、手机号码、密码等登录或进行任何形式操作的；

（六）患者有违背协议承诺、保证或相关义务、责任之行为或事由的；

（七）服务中任何非与本院有关第三人的声明或行为；

（八）依据法律规定和本院规则认定的其他免责情形。

八、协议的更新

（一）本院可能会不时更新本《医疗数据使用授权协议》，更新时将在本院醒目位置发布公告，或在手机应用中发布通知，您每次接受本院提供的诊疗服务或登录使用本院手机应用时均视为同意受当时有效的声明条款内容的约束。

（二）《医疗数据使用授权协议》的更新和变化包括但不限于：

1.服务模式发生重大变化，如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；

2.控制权等方面发生重大变化，如并购重组等引起的信息控制者变更等；

3.个人信息共享、转让或公开披露的主要对象发生变化；

4.您参与个人信息处理方面的权利及其行使方式发生重大变化；

5.我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化；

6.个人信息安全影响评估报告表明存在高风险；

7.本院认为应予更新的其他情形。

九、其他

（一）本协议依据的内容包括《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》等现行有效的法律、行政法规和政策性文件。

（二）本协议及其修改权、更新权及最终解释权均属本院所有。

附件 2：交易合同示范文本

第一部分 术语和定义

1. 数据

是指任何以电子或非电子形式对信息所做的记录。

2. 数据交易

《医疗数据交易合同示范文本》（下称“本合同”）所称的“数据交易”是指数据供方和需方之间以本合同约定的数据处理权益为交易对象、以货币为媒介的价 值交换过程。

3. 数据供方

是指通过数据包或者API等方式，向数据需方交付标的数据、转让或共享数据处理权益，并获得相应对价的主体。

4. 数据需方

是指具有特定数据需求，从数据供方接受标的数据、获得标的数据处理权益，并支付对价的主体。

5. 数据处理权益

5.1 本合同所称的“数据处理权益”，是指依据法律、行政法规或地方性法规的规定、当事人的约定或者特定事实行为而享有的、在特定权限范围内对数据进行处理之权利。

5.2 前款所称的“特定权限范围”包括对数据的处理目的权限、处理方式权限及处理期限权限。

5.3 前款所称“处理方式”是指数据处理主体对数据进行的包括但不限于收集、存储、使用、加工、传输、提供、公开等活动。

6. 数据处理权益转让

简称“数据转让”，本合同中指供方向需方提供标的数据的同时，不再对标的数据享有任何数据处理权益的交易方式；但本合同另有约定的除外。

7. 数据处理权益共享

简称“数据共享”，本合同中指供方向需方提供标的数据的同时，各方均独立对标的数据享有数据处理权益的交易方式；需方对标的数据的处理权限依据合同约定予以明确。

8. 概括处理

本合同所称的“概括处理”，是指数据处理主体享有对数据进行收集、存储、使用、加工、传输、提供、公开等全部处理方式之权限，但法律、行政法规禁止的处理方式除外。

9. 独占处理

本合同所称的“独占处理”，是指在数据共享交易中，需方所享有的要求供方不得自行或授权他人就标的数据在一定目的、期限范围内、以一定方式进行处理的权利。

10. 原始数据

本合同所称的“原始数据”，是指供方按照一定方式和规则收集的、用于生成标的数据的、尚未进行额外加工的初始数据或底层数据。

11. 标的数据

本合同所称的“标的数据”，是指对原始数据进行一定加工而形成的用于交付的数据。

12. 衍生数据

本合同所称的“衍生数据”，是指由数据需方对供方提供的标的数据进行进一步加工后形成的区别于标的数据的数据。

13. 重要数据

指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等数据。

14. API交付

即数据供方向需方提供满足约定的应用程序编程接口，以实现需方获取本合同约定的标的数据。

15. 数据安全保护责任

本合同所称的“数据安全保护责任”，是指通过采取必要措施，保障数据得到有效保护并持续处于安全状态之责任。

16. 个人信息

个人信息是指以电子或者其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的信息。“匿名化”是指个人信息经过处理无法识别特定自然人且不能复原的过程。

17. 敏感个人信息

敏感个人信息是指一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

18. 公共数据与公共开放数据

本合同所称的“公共数据”是指行政机关以及具有公共管理和服务职能的单位（以下统称“公共管理和服务机构”）在依法履行职责、提供公共服务过程中获取的数据资源。

“公共开放数据”即指公共管理和服务机构直接或间接面向社会公开的公共数据，包含有条件公开和无条件公开的数据。

19. 合规性要求

本合同所称的“合规性要求”是指法律法规、规章及其他国家、地区及行业规定等规范性法律文件对供需一方或双方就本合同所涉事项所应履行或遵循的 强制性、义务性规定。

20. 涉外或涉港澳台数据

指因原始数据或标的数据的数据处理行为等有关事宜涉及中华人民共和国领域外或港澳台而导致与交易有关的事项可能受到外国或港澳台法律、外国或港澳台司法、仲裁机构所管辖的数据。

第二部分 专用条款

数据需方：

统一社会信用代码：

法定代表人：

送达地址：

指定联系人：　　联系电话：

送达邮箱：　　传真：

数据供方：

统一社会信用代码：

法定代表人：

送达地址：

指定联系人：　　联系电话：

送达邮箱：　　传真：

鉴于：

数据需方（以下简称“需方”）为在中华人民共和国境内（不含港澳台）合法成立的法人或非法人组织，拟将本合同项下约定的标的数据用于合法用途；数据供方（以下简称“供方”）为在中华人民共和国境内（不含港澳台）合法成立的营利性法人或非法人组织，经营范围包含实施本合同约定的数据交易行为。

依据《中华人民共和国民法典》《中华人民共和国网络安全法》及相关规范性法律文件，供需双方经平等、自愿协商，达成如下协议：

第一条　交易标的

1.1 交易方式

□数据转让

□数据共享

1.2 标的数据要求

1.2.1 标的数据名称：

1.2.2 标的数据□是□否根据需方要求制定。

1.2.3 标的数据性质

标的数据□是□否包含或涉及本地区、部门或行业重要数据（以下简称“重要数据”）。

1.2.4 标的数据描述

□标的数据为标准数据的，可见附件《样本数据描述》。

□标的数据为定制数据的，可见附件《标的数据需求表》。

1.3 需方对标的数据之处理权限

1.3.1处理目的权限

需方承诺仅将标的数据用于如下目的：

_____。

1.3.2处理方式权限

需方在标的数据处理目的范围内享有的处理方式权限为第___项：

A.概括处理

B.享有除如下划“×”方式外的其他处理方式权限：

□加工

□传输

□提供

□公开

□其他 _____

1.3.3处理期限权限

□固定期限

处理期限为_____，自如下第___项约定时间起算：

A．自供方交付标的数据之日起计算

B．自标的数据或API接口通过验收之日起计算

C．其他 _____

□不固定期限：

○以标的数据处理目的达成为限

○其他_____

1.4 标的数据到期处理

（□适用□不适用）处理期限到期后，需方应按照以下方式对标的数据进行销毁：

_____。

（□适用□不适用）若标的数据为重要数据的，供方□是□否需要通过销毁数据安全风险评估。

1.5 （□适用□不适用）标的数据独占处理

需方在标的数据的处理目的、期限范围内就标的数据享有如下划“ √”方式的独占处理权 ：

○存储

○加工

○使用

〇传输

〇提供

〇公开

〇其他

第二条　交易价款

2.1 计价方式与价格

_____。

2.2 支付方式与结算

_____。

2.3 （□适用□不适用）质量保证金

需方有权将交易总额的____%作为质量保证金予以扣留。

在专用条款5.2条约定的质量保证期届满后14日内，扣除质量保证期间因标的数据质量瑕疵而导致的赔偿金或违约金（若有）后，需方应按如下第____种方式向供方支付：

A．扣留的质量保证金不计息。

B．以抵扣后最终应付的质量保证金为基数，自标的数据通过验收之日起按照_____的标准计息，与质量保证金一并支付。

第三条　交易安全

3.1 数据交易风险评估与行政审批

3.1.1标的数据属于重要数据的，供方应当对本次数据交易进行安全风险评估，需方应当积极配合供方的安全风险评估。

3.1.2标的数据属于重要数据的，供方□应当/□暂不报有关监管部门批准。

3.2 （□适用□不适用）标的数据分级分类安全保护

3.2.1供方应当至少在本合同签订之日起_____日内向需方出具《标的数据分级分类安全保护说明》。

3.2.2 需方应当按照《标的数据分级分类安全保护说明》采取相应的措施，并确保在标的数据交付_____日前符合《标的数据分级分类安全保护说明》的要求，并向供方出具《标的数据安全保护措施响应承诺书》。

3.3 （□适用□不适用）网络安全等级测评

3.3.1供方应当在本合同签订之日起_____日内向需方提供第〇一〇二〇三〇四级《网络安全等级测评报告》。

3.3.2需方应当在本合同签订之日起_____日内向供方提供第〇一〇二〇三〇四级《网络安全等级测评报告》。

3.4 （□适用□不适用）网络安全审查

若需方为关键信息基础设施运营者，则经需方进一步评估确认本次交易〇是〇否可能影响国家安全；若是，供需双方应当共同配合进行网络安全审查。

第四条　交付与验收

4.1 标的数据交付方式

□ 数据包交付

□ API交付

□ 其他_____

4.2 （□适用□不适用）交付要求

供方应当按照附件《标的数据交付要求》向需方交付标的数据，以保证标的数据的安全、准确、完整传输。

4.3 交付期限

□数据包交付的，供方应在_____前向需方交付；

□API 交付的，供方应在____前提供符合约定的API接口，以实现需方对标的数据的获取需求。

4.4 标的数据验收

双方确认以下列___方式作为需方对供方标的数据合格交付的确认：

A.双方约定以数据包形式交付的，需方应在标的数据交付之日起的_____日内对标的数据是否符合本合同约定进行验收；确认标的数据与本合同约定相符的，应同时向供方出具《验收确认书》。

B.双方约定以API形式交付的，需方应在API接口向其开通之日起_____日内对通过API接口是否能够获取符合本合同约定的标的数据进行确认；确认合格的，应同时向供方出具《验收确认书》；

C. 其他_____。

4.5 验收异议

需方验收时对交付存在异议的，应在4.4条约定的验收期限内通知供方；异议成立的，供方应当积极采取补救措施以确保标的数据符合合同约定。

异议事项消除后，供方应重新交付并提交验收，需方应在___日内予以验收；因此导致迟延交付的，迟延期限在___日内且重新交付验收合格的，供方可免予承担迟延交付责任。

4.6 数据安全保护责任转移

根据交易方式的不同，双方确认本次交易□是□否涉及标的数据之数据安全保护责任转移（如需方通过API接口直接获得计算结果数据的情况下，若供方不对标的数据进行处理，则可不涉及标的数据的安全保护责任转移）。

第五条　标的数据质量保证

5.1 （□适用□不适用）标的数据质量验证

供需双方约定的质量验证方式为：

_____。

5.2 （□适用□不适用）标的数据质量保证期

〇标的数据交付方式为数据包的，质量保证期限为自需方出具《验收确认书》之日起_____。

〇标的数据交付方式为API方式的，质量保证期限按___项确定：

A.自需方出具《验收确认书》之日起_____。

B.与本合同有效期相同。

C.其他

第六条　特别处理约定

6.1 类标的数据处理

6.1.1（□适用□不适用）若交易方式为数据转让的，则供方〇是〇否能够继续处理与本合同约定的“标的数据要求”相同或具有高度相似性的数据（以下简称“类标的数据”）。

若供方有权处理类标的数据，其〇是〇否能够将类标的数据向任何与需方有利益冲突或行业竞争关系的第三方转让、共享或披露。

6.1.2 （□适用□不适用）若交易方式为数据共享，且需方享有本合同约定范围内的独占处理权益的，则供方〇是〇否能够继续处理类标的数据。

若供方有权处理类标的数据，其〇是〇否能够将类标的数据向任何与需方有利益冲突或行业竞争关系的第三方转让、共享或披露。

6.2 供方标的数据销毁

6.2.1若交易方式为数据转让的，则供方应按照第____项的约定对标的数据进行销毁，不得以其他任何方式对标的数据进行处理：

A.应在需方向其出具《验收确认书》之日起三日内

B.应在质量保证期届满之日起的三日内

C.其他_____

6.2.2 （□适用□不适用）若标的数据为重要数据的，供方□是□否需要通过销毁数据之安全风险评估。

第七条　衍生数据处理

7.1 （□适用□不适用）需方对标的数据享有加工权限的，需方对加工形成的衍生数据之处理权限范围按照以下___方式确定：

A.参照本合同对于标的数据的约定执行；

B.其他：_____

7.2 （□适用□不适用）供需双方对于衍生数据的其他约定：_____。

第八条　保密

8.1 保密信息

如下信息应被视为保密信息，供需双方均应按照本合同的约定对相对方的保密信息履行保密义务：

（1）商业秘密，即指一方不愿公开或尚未主动公开的技术秘密、商业情报及信息。

（2）（□适用□不适用）除商业秘密外，各方还应对如下划“√”信息负有保密义务：

〇从相对方获知的可能影响相对方正常经营、管理或第三方合法权益的信息，前述信息不以明示保密为前提。

〇有关本合同的磋商、签订、履行及争议之信息。

〇其他_____。

8.2 保密义务之例外

存在如下划“√”情况，向第三方披露相对方的保密信息的，不视为对保密义务的违反：

□为履行法定义务而向国家机关或有关单位合理披露的。

□为履行上级机关或集团内部管理要求而向前述主体及相关人员披露的，但应保证前述主体及人员参照本合同的约定履行保密义务。

□为融资需求而向银行或有关金融机构及相关人员披露的，但应保证前述主体及人员参照本合同的约定履行保密义务。

□因实施收购、兼并或类似行为而向相关方及相应人员披露的，但应采取合理措施控制披露范围，并保证前述主体及人员参照本合同的约定履行保密义务。

□其他_____。

第九条　合约追踪

9.1 （□适用□不适用）合约追踪方式

供方有权在不干涉需方正常运营的前提下,就需方对标的数据的处理是否符合合同约定进行如下划“ √”方式的合约追踪：

〇 审 计　　〇 定 期 抽 查　　〇 采 样 检 查　　〇 其 他

9.2 （□适用□不适用）合约追踪要求

供需双方对于合约跟踪的具体约定：见附件《合约追踪约定》。

第十条　应急预案与处置

10.1 网络与数据安全应急预案

供需双方□是□否应将相应的应急预案作为本合同附件。

10.2 负面数据事件处理与责任

10.2.1 标的数据属于通用条款 1.3.1 项所列数据的，需方通知供方的同时应当通知相关监管部门；在相关部门进一步指示前，不得采取其他任何处理措施，但为了避免损失进一步不可逆转的扩大而采取合理、必要措施的除外。

10.2.2 标的数据涉及通用条款 1.3.2 项所列数据的，需方应当按照如下第 项方式予以处理：

A.在通知供方的同时应当通知相关监管部门，在相关部门进一步指示前，不得采取其他任何处理措施，但为了避免损失进一步不可逆转地扩大而采取合理、必要措施的除外。

B.应及时通知供方，并按照供方的要求对负面数据予以销毁。

10.2.3 标的数据涉及通用条款 1.3.3 项所列数据的，需方应当按照如下第 项方式予以处理：

A.在通知供方的同时应当通知相关监管部门，在相关部门进一步指示前，不得采取其他任何处理措施，但为了避免损失进一步不可逆转地扩大而采取合理、必要措施的除外。

B.应及时通知供方，并按照供方的要求对负面数据予以销毁。

10.2.4 标的数据属于违反通用条款 1.3.4 项约定、涉及个人信息数据的，供方应当启动应急预案，同时通知受影响的个人信息主体，征求个人信息主体的 事后追认；无法获得事后追认的，需方应当立即销毁相关数据，不得以任何方式 加以利用。

第十一条 违约责任

11.1 交付违约

除本合同另有约定外，供方未按照本合同约定的期限交付标的数据并通过验收的，应当以_____为基数，按照_____的标准计算并向需方支付违约金；前述违约金不足以弥补需方损失的，供方还应当据实承担赔偿责任。

11.2 质量瑕疵

除本合同另有约定外，供方交付的标的数据存在质量瑕疵的，应当以_____的标准计算并向需方支付违约金；前述违约金不足以弥补需方损失的，供方还应当据实承担赔偿责任。

11.3 付款违约

需方未按照本合同约定的期限和金额支付价款的，应当以欠付金额为基数，按照_____的标准计算并向供方支付违约金。

11.4标的数据处理违约

□除本合同另有约定外，需方违反本合同约定处理标的数据或衍生数据，尚未给供方造成损失或者损失难以计算的，应当以_____为基数，按照的标准计算并向供方支付违约金。

□除本合同另有约定外，需方违反本合同约定处理标的数据或衍生数据给供方造成损失的，应当据实承担赔偿责任。

11.5 违反合规性要求

□任意方违反本合同约定的合规性要求，尚未给相对方造成损失或者损失难以计算的，应当以_____为基数，按照_____的标准计算并向相对方支付违约金。

□除本合同另有约定外，违反本合同约定的合规性义务，给相对方造成损失的，应当据实承担赔偿责任。

11.6 违反保密义务

□除本合同另有约定外，一方违反本合同约定的保密义务，尚未给相对方造成损失或者损失难以计算的，应当以_____的标准计算并向相对方支付违约金。

□除本合同另有约定外，一方违反本合同约定的保密义务给相对方造成损失的，应当据实承担赔偿责任。

11.7损失赔偿范围

因违约给相对方造成损失的赔偿责任应相当于因违约所造成的损失，包括合同履行后可以获得的利益。

前述损失□是□否包含守约方为实现债权或追究对方责任所支出的合理费用，如律师费、公证费、财产保全（担保、保险）费用、差旅费等。

11.8 其他约定

双方对违约责任的其他约定：_____。

第十二条　合同解除

12.1　需方单方解除权

出现下列划“√”情形之一的，需方可书面通知供方解除合同，通知到达供方时，本合同解除：

□供方未按照约定期限交付标的数据，延迟交付达____天的。

□供方交付的标的数据不符合本合同的约定，经____日内采取补救措施后仍不符合本合同约定、导致需方无法实现合同目的的。

□供方违反合规性要求，导致需方无法实现合同目的的。

□出现法律、行政法规规定的可单方解除合同的其他情形的。

□其他约定：_____。

12.2 供方单方解除权

出现下列划“√”情形之一的，供方可书面通知需方解除合同，通知到达需方时，本合同解除：

□需方未能按照本合同的约定达到《标的数据分级分类安全保护说明》中的必备要求、经供方书面催告后_____日内，需方仍未达到的。

□需方不具备法律、行政法规规定的适用于标的数据的强制性保护要求、经供方书面催告后____日内，需方仍未达到的。

□出现法律、行政法规规定的可单方解除合同的其他情形的。

□其他约定：_____

12.3 单方合同解除权行使期限及后果

出现本条约定的单方解除事宜的，守约方应在知道或应当知道权利受到侵害或者违约方存在违约情形之日起_____内行使合同解除权；超出该期限的，单方合同解除权消灭。

第十三条　争议解决

因本合同（含补充协议，若有）引起的或与本合同有关的任何争议，双方同意按照下列第____种方式予以解决：

A.任意一方有权提请_____仲裁委员会按照其仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

B.任意一方有权向_____有管辖权的人民法院提起诉讼。

第十四条　合同文件组成与优先解释顺序

14.1本合同文件由以下文件共同组成：

（1）术语与定义

（2）专用条款

（3）通用条款

（4）附件

□《样本数据描述》

□《标的数据需求表》

□《标的数据分级分类安全保护说明》

□《标的数据安全保护措施响应承诺书》

□《网络安全等级测评报告》

□《标的数据交付要求》

□《验收确认书》

□《合约追踪约定》

□《合规承诺》

☐《网络安全审查配合承诺》

☐ 供方《网络与数据安全事件应急预案》

☐ 需方《网络与数据安全事件应急预案》

14.2优先解释顺序

本合同的各组成文件应视为内在统一，能够相互印证或相互解释。

若各文件之间的条款存在不可调和之冲突或矛盾以致无法通过文义确定各方真实意思的，应按照如下顺序进行解释：

（1）合同附件

（2）专用条款

（3）通用条款

（4）术语与定义

（5）其他：_____

第十五条　合同生效与有效期

15.1合同生效

本合同的生效方式采用如下第____种：

A.　自双方签字或盖章之日起生效。

B.　自通过监管部门的重要数据交易行政审批之日起生效。

C.　自通过监管部门的网络安全审查之日起生效。

15.2合同有效期

本合同的有效期采用如下第____种：

A. 自本合同生效之日起至双方权利义务履行完毕之日止。

B. 自_____年__月___日起至 _____年___月___日止。

C.其他_____。

第十六条　其他

16.1（□适用□不适用）行政备案

由□供方□需方按照规定进行备案、□供方□需方予以充分配合；除法律、行政法规的强制性规定外，是否备案不影响本合同的效力。

16.2文本效力

本合同一式__份，需方持有__份，供方持有__份，具有同等法律效力。

16.3 其他特殊约定

_____。

第三部分 通用条款

第一条　交易标的

1.1交易方式与数据处理权限制

1.1.1本合同约定的交易类型为转让的，自标的数据交付之日起至本合同约定的数据销毁之日，供方对标的数据不再享有除存储以外的其他处理权限，不得自行或委托他人再行对标的数据进行任何处理。

经需方同意，在约定的数据销毁之日前，供方基于本合同项下的质量验证或质量保证目的而需对标的数据进行合理且必要的处理的，不受前项约定的限制。

1.1.2本合同约定的交易类型为共享且约定需方对标的数据享有独占处理权益的，供方不得自行或委托他人在需方独占处理权限范围内处理标的数据。

经需方同意，供方基于本合同项下的质量保证或质量保证目的而需对标的数据进行合理且必要的处理的，不受前项约定的限制。

1.2标的数据质量保证承诺

供方对标的数据作出如下质量保证承诺：

1.2.1供需相符保证

A.供方提供标准数据样本的，应当保证标的数据在数据类别、名称、计量单位、质量要求、格式、加工要求等与样本数据相符，不得存在明显背离或差异。

B.需方定制标的数据的，供方应当保证符合需方指定的《标的数据需求表》中关于数据类别、名称、计量单位、质量要求、格式、加工要求等，不得存在明显背离或差异。

1.2.2信息精确度保证

在供方保证原始数据信息精确度的基础上，供方应同时保证标的数据所记载信息的客观、真实与有效性。

1.2.3处理权限与合规保证

供方承诺并保证依据本合同对标的数据进行处理的行为均具有与之相应的完整、清晰、无争议的合法处理权限；不存在无权或超越处理权限的行为；

供方应当向需方出具《合规承诺》并保证需方能够依据本合同约定对标的数据合法享有数据处理权益。

1.3负面数据交易排除

1.3.1供需双方承诺本次交易不得包含或涉及载有以下信息的数据：

（1）反对宪法所确定的基本原则的；

（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（3）损害国家荣誉和利益的；

（4）歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；

（5）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；

（6）煽动民族仇恨、民族歧视，破坏民族团结的；

（7）破坏国家宗教政策，宣扬邪教和封建迷信的；

（8）散布谣言，扰乱经济秩序和社会秩序的；

（9）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（10）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

（11）涉及法律、行政法规予以禁止或要求抵制的其他内容的。

1.3.2供需双方确认本次交易的标的数据不包含或涉及本地区、部门、行业颁布的数据交易禁止或负面清单的数据。

1.3.3供需双方确认本次交易的标的数据不包含涉外或涉港澳台数据。

1.3.4供需双方确认本次交易的标的数据不包含或涉及个人信息。

1.4 需方对标的数据处理的合法、合约、合规承诺

1.4.1需方应保证对标的数据的处理符合法律、行政法规的规定，尊重社会公德和伦理，遵守商业道德，诚实守信，不利用标的数据实施危害国家安全、公共安全或社会公共利益的行为，不利用标的数据进行不正当竞争，不利用标的数据侵犯自然人的人格权益、他人的商业秘密、知识产权及其他合法权益。

1.4.2需方应当秉承诚信、谦抑原则在本合同约定的处理权限范围内合理、正当处理标的数据；除本合同另有约定外，不得超出合同约定处理权限范围处理标的数据。

1.4.3需方在享有约定的数据处理权益的同时，应履行法律法规、规章及其他国家、地区及行业规定等规范性法律文件对其就本合同所涉事项应履行或遵循的强制性、义务性规定（即需方合规性要求）。

第二条　交易价款

2.1按约支付

需方应当按照本合同的约定向供方支付合同价款。

2.2质量保证金的支付

需方应按照专用条款的约定将质量保证金扣除在质量保证期间内因标的数据质量瑕疵而导致的赔偿金或违约金（若有）后，向供方支付。

第三条　交易安全

3.1数据交易风险评估与行政审批

3.1.1供方应对标的数据进行初步评估，若评估标的数据属于重要数据的，应当进行安全风险评估并出具《重要数据交易安全风险评估报告》，需方应当予以积极配合。

重要数据交易安全风险评估未通过的，不得进行交易。

供方组织的安全风险评估通过的，应当按照专用条款的约定报经监管部门批 准。

3.1.2供方依据专用条款约定需要进行安全风险评估并需报批的，可将有关主管部门的批准作为本合同的生效条件。

3.1.3若供方未将有关主管部门批准作为本合同的生效条件的，因主管机关监管导致无法进行交易或者引发任何法律责任的，由供方承担。

3.2标的数据分级分类及对应安全措施

3.2.1供方应依据国家有关规定，按照对标的数据的来源、内容、用途、价值、内容敏感程度、披露影响范围等标准， 将标的数据进行分级分类并采取相应措施保证数据安全。

3.2.2供方应按照专用条款的约定向需方提供《标的数据分级分类安全保护说明》，告知标的数据的分级分类级别，说明为确保标的数据安全所需采取的必要的技术措施和管理措施，以便对需方就标的数据的存储、访问、传输等处理行为提供安全操作标准和说明。

3.2.3《标的数据分级分类安全保护说明》可以包含以下内容：网络安全等级保护级别建议或要求、具体网络与数据安全保护技术措施及员工数据访问权限等网络、数据安全管理措施等。

3.2.4专用条款约定需方应向供方出具《标的数据安全保护措施响应承诺书》方能交付的，在需方出具前述文件前，供方不得交付；否则，标的数据交付后出现数据安全事件的，供方应当承担相应的责任。

3.2.5法律、行政法规对数据安全保护另有强制性规定的，从其规定。

3.3网络安全等级评测

3.3.1供方应当确保其计算机网络系统具备与处理原始数据和/或标的数据相适应的网络安全保护水平。

3.3.2符合下列情形之一的，宜在专用条款中约定供方应向需方提供证明其具备与处理原始数据和标的数据相适应的网络安全等级测评文件：

（1）原始数据涉及个人信息数据

（2）原始数据涉及重要数据

（3）标的数据涉及重要数据

（4）原始数据或标的数据涉及存在其他特殊合规性要求的数据（如原始数据为有条件开放的公共开放数据）

3.3.3需方应当确保其计算机网络系统具备与处理标的数据相适应的网络安全保护水平。

3.3.4符合下列情形之一的，宜在专用条款中约定需方应向供方提供证明其具备与处理标的数据相适应的网络安全等级测评文件：

（1）标的数据涉及重要数据

（2）标的数据涉及存在其他特殊合规性要求的数据

3.3.5按照本合同约定需要提供网络安全等级测评文件的，应按照《信息安全技术　网络安全等级保护基本要求》的要求自行或委托具有相应资质的测评机构进行测评并出具。

3.3.6法律、行政法规对网络安全标准或评测另有强制性规定的，从其规定。

3.4　网络安全审查

3.4.1需方为关键信息基础设施运营者的，应当预判本次交易可能带来的国家安全风险，影响或者可能影响国家安全的，应当向主管机关申报网络安全审查。

3.4.2需方为关键信息基础设施运营者，且预判本次交易可能影响国家安全的，供方应向需方出具《网络安全审查配合承诺》，承诺若本次交易进入网络安全审查程序，将配合网络安全审查，包括承诺无正当理由不中断标的数据供应或必要的技术支持服务等。

3.4.3需方预判本次交易可能影响国家安全的，可将有关主管部门的审查通过作为本合同的生效条件；未通过安全审查导致本合同不生效的，各方自行承担相应的缔约费用与损失。

3.4.4若需方未将有关主管部门审查通过作为本合同的生效要件，因审查机关监管导致无法进行交易或者引发任何法律责任的，由需方承担。

第四条　交付与验收

4.1按约交付

4.1.1供方应当按照本合同的约定向需方交付标的数据。

4.1.2双方约定采用数据包的方式交付标的数据的，宜在《标的数据交付要求》中约定包括但不限于数据传输方式、数据接收频次、访问权限限制等事宜。

4.1.3双方约定采用API界面方式交付标的数据的，宜在《标的数据交付要求》中约定包括但不限于接口开放时间、频次、单次数据下载量、访问权限等级、访问权限人数等事宜。

4.1.4双方约定采用其他方式交付标的数据的，可参考前述约定就相关事宜予以明确。

4.2交付传输安全

供方应在标的数据交付前对数据采取适当的加密等措施，并应当明确告知需方相应的注意事项，双方共同配合以保证传输中的数据安全。

专用条款约定供方应出具《标的数据安全保护级别说明》的，双方应当按照《标的数据安全保护级别说明》及《标的数据安全保护措施响应承诺书》的说明和承诺执行，以保证数据传输安全。

4.3验收

需方应当按照专用条款的约定对标的数据是否符合本合同的约定进行验收并出具《验收确认书》。

需方无正当理由未按照专用条款约定的期限出具《验收确认书》，或者需方在异议事项消除后，无正当理由未在约定期限内响应供方的重新验收请求的，视为标的数据通过验收。

4.4数据安全保护责任转移

4.4.1专用条款确认本次交易涉及数据安全责任转移的，除非双方另有约定，在供方交付标的数据之前，数据安全保护责任由供方承担；标的数据交付后，需方对其处理的标的数据承担数据安全保护责任；但需方能够证明供方对数据安全事件的发生或处置等有过错的，供方承担相应的过错责任。

4.4.2专用条款确认本次交易不涉及数据安全责任转移的，除非双方另有约定，需方应独立承担对标的数据的数据安全保护责任；但需方能够证明供方对数据安全事件的发生或处置等有过错的，供方承担相应的过错责任。

4.4.3标的数据交付后，供方按照本合同约定仍享有标的数据处理权的，供方对其处理的标的数据负有独立的数据安全责任。

第五条　标的数据质量保证

5.1质量验证

需方有权按照专用条款的约定对标的数据进行质量验证，供方应当予以必要的配合。

5.2质量保证责任

5.2.1供方应当承担因标的数据不符合本合同约定即存在质量瑕疵而导致的责任，下称“质量保证责任”。

5.2.2 供方承担质量保证责任的方式有：数据修正、数据再加工、降低价款、赔偿损失、承担违约金等。

5.3质量保证金

5.3.1 质量保证金是指标的数据验收后，需方在总交易金额中预留的一部分用于保证标的数据与合同约定相符的资金；在标的数据在质量保证期中因质量瑕疵而给需方带来损失时，需方可直接将损失从预留的质量保证金中予以扣除。

5.3.2 双方在专用条款中约定质量保证金及质量保证期的，在质量保证期限届满后十四日内，需方应向供方支付扣除相应损失或违约金后的剩余质量保证金。全部质量保证金不足以弥补损失的，供方还应继续承担赔偿责任。

5.4质量保证金责任

5.4.1无论需方是否出具《验收确认书》，若双方约定质量保证期的，供方应在质量保证期限内对标的数据承担质量保证责任。

5.4.2 双方在专用条款中仅约定质量保证金而未约定质量保证期的，自需方出具《验收确认书》之日， 供方的质量保证责任终止；需方应当在出具《验收确认书》之日起十五日内向供方支付扣除相应损失或违约金后的剩余质量保证金。全部质量保证金不足以弥补损失的，供方还应继续承担赔偿责任。

第六条　特别处理约定

6.1禁止再识别

标的数据为个人信息匿名化后数据的，需方不应以任何方式将标的数据单独或结合其他任何数据用于识别个人信息主体。

6.2数据处理后果责任

除法律、行政法规等强制性规定、本合同另有约定或供方确有故意或重大过失外，需方按照本合同约定对标的数据进行处理所产生的一切法律后果，由需方自行承担；需方违反或超出本合同约定进行标的数据处理的，还应同时按照本合同的约定向供方承担违约责任。

6.3供方类标的数据处理限制

本合同约定供方不享有对类标的数据的相应处理权限的，供方不得自行或授权他人再以任何方式对类标的数据进行相应处理。

6.4数据销毁

6.4.1供方数据销毁义务

双方应当依据法律、行政法规或地方性法规的强制性规定对标的数据或/及原始数据进行销毁；没有前述强制性规定的，供方应当按照本合同约定的期限及指定方式对标的数据或/及原始数据进行销毁。

若标的数据或/及原始数据涉及重要数据且约定供方应进行销毁数据安全风险评估的，若安全评估未通过，不得对所涉重要数据进行销毁，对标的数据的处理由双方另行协商。

6.4.2需方数据销毁义务

双方应当依据法律、行政法规或地方性法规的强制性规定对标的数据进行销毁；没有前述强制性规定的，双方可在本合同中约定对标的数据进行销毁。

若标的数据涉及重要数据且约定需方应进行销毁数据之安全风险评估的，若安全评估未通过，不得对所涉重要数据进行销毁，对标的数据的处理由双方另行协商。

第七条　衍生数据处理

7.1 需方对标的数据加工后获得的衍生数据享有专用条款所列处理权限，除非双方另有书面约定，供方对衍生数据不享有任何处理权限。

7.2 除双方另有约定外，需方按照本合同约定对衍生数据进行处理所产生的任何义务或责任与供方无关。

7.3 需方超出本合同约定对标的数据进行处理而形成衍生数据的，供方有权要求需方在合理期限内予以销毁并承担相应的违约责任。

第八条　保密

8.1 保密义务

8.1.1除双方另有约定外，各方仅应出于本合同的磋商、签订、履行及争议解决之目的（简称“合同实施目的”）而合理使用相对方的保密信息。

8.1.2各方对相对方的保密信息负有保密义务,不应以任何方式向任何第三方披露，且负有采取妥善措施以保证保密信息不被与合同实施目的无关的任何单位或个人知悉或使用之义务。

8.1.3超出合同实施目的而使用保密信息，或者未尽妥善管理义务而导致任何与合同实施目的无关的单位或个人知悉或使用保密信息的，即视为对保密义务的违反。

8.2 保密条款效力

本合同对保密事项作出的约定具有独立效力，即便在本合同失效、终止、被撤销、确认无效之后仍继续有效，直至相关保密信息成为公众可无差别的免费获知的信息，或权利人书面通知不再负有保密义务为止。

第九条　合约追踪

9.1专用条款约定供方有权就需方是否按照合同约定处理标的数据进行合约追踪的，需方有义务按照供方或《合约追踪约定》的要求提供其依约处理标的数据之必要、合理、充分的证明材料。

9.2需方不得仅以合同追踪侵犯其商业秘密或保密信息为由拒绝配合。但确实涉及需方保密信息的，供方应当承担保密义务，或根据需方的要求出具相应的保密承诺函。

第十条　应急预案与处置

10.1网络与数据安全应急预案

10.1.1 供需双方均应当按照《中华人民共和国网络安全法》等规定的要求建立网络与数据安全应急预案。

10.1.2 原始数据或标的数据涉及通用条款 3.3.2 项的约定的，供方宜向需方提供前述预案作为本合同附件。

标的数据涉及通用条款3.3.4项的约定的，需方宜向供方提供前述预案作为合同附件。

10.1.3发生数据泄露、毁损、丢失等安全事件，或者发生数据安全事件风险 明显加大时，应当依据“谁处理、谁负责”的原则按照各方应急预案的规定立即采取补救措施，并按要求向有关部门报告。

10.1.4需方滥用合同权利或违反合同约定危及供方原始数据或供方处理的标的数据安全的，需方应当立即按照供方的要求消除安全隐患；造成安全事件，应当承担相应责任。

10.2负面数据事件处理与责任

10.2.1需方收到标的数据后,若发现标的数据存在通用条款 1.3 条所列的负面数据情形的，则应立即告知供方；在依约采取下步补救措施前，需方应当对所涉负面数据采取严格限制访问的技术措施及安全管理措施。

10.2.2供需双方应按照专用条款的约定对负面数据进行妥善处理；相应合规性要求对负面数据的处理另有强制性规定的，可从其规定；其中为法律、行政法规的强制性规定的，应从其规定。

10.2.3负面数据事件责任由供方承担；需方因此承担责任的，有权向供方予以追偿。

需方未能积极履行法律规定及本合同约定的义务导致负面数据事件的影响或造成的损失扩大的，在影响或损失扩大的范围内承担责任；需方因此承担责任后，有权就不属于自身承担责任的范畴向供方予以追偿。

10.2.4除本合同约定外，需方不得以任何方式对负面数据进行处理或予以利用。

第十一条　违约责任

11.1违约责任

违约方应当按照专用条款的约定向守约方承担违约责任。

11.2违约赔偿

除专用条款的明确约定外，一方违反本合同给对方造成损失的，应当承担损失赔偿责任。

第十二条　合同解除

12.1协商一致解除

除专用条款的约定外，供需双方协商一致的，可以书面方式确定本协议的解除，各方应按照书面约定对本合同进行清理结算。

12.2单方合同解除权行使期限

守约方应当按照专用条款的约定行使单方解除权；超出约定期限未行使的，单方合同解除权消灭。

单方合同解除权消灭的，不影响守约方依据本合同向违约方主张除单方解除合同以外的其他权利。

12.3合同解除后果

合同解除后，尚未履行的，中止履行；已经履行的，守约方可以请求恢复原状或者采取其他补救措施。

合同解除的，不影响守约方按照本合同的约定追究违约方的约定或法定责任。

第十三条　处理权限变更

13.1需方因客观情况变化需要变更或增加对标的数据或/及衍生数据的处理权限的，应当事先征求供方的意见，并签署书面的变更协议后依法履行。

13.2下列情况下，需方超出合同约定的范围合理处理数据的，无需事先征求供方意见，但应当及时书面通知供方：

（1）国务院及有关主管部门为履行维护国家安全、公共安全、社会管理、经济调控等职责需要，依照法律、行政法规的规定， 要求需方对标的数据进行超出合同约定范围的数据处理的。

（2）国家监察机关、公安机关等依法侦查犯罪的活动所需，要求需方对标的数据进行超出合同约定范围的数据处理的。

（3）标的数据存在违反通用条款 1.3 条约定之情形，需方为遵守法定义务而对标的数据进行超出合同约定范围的合理且必要的数据处理的。

（4）为履行其他法律、行政法规所规定的强制性法律义务而超出合同约定范围内处理数据的。

第十四条　不可抗力与情势变更

14.1不可抗力

14.1.1不可抗力的定义

本合同所称的不可抗力是指不能预见、不能避免且不能克服的客观情况。

14.1.2不可抗力免责主张的前提与法律后果

一方因不可抗力不能履行合同并按照本合同约定履行通知及减损义务的，根据不可抗力的影响，部分或者全部免除责任，但是法律另有规定的除外。

主张适用不可抗力的一方因不可抗力导致本合同客观上全部或者部分不能履行，应当及时通知对方，以减轻可能给对方造成的损失，并应当在合理期限内 提供证明。

若受不可抗力影响的一方采取可行的合理措施即可避免对方损失不合理扩大的，还应根据对方的要求采取合理措施避免损失的扩大；为避免相对方损失不合理扩大而支出的费用由相对方承担；否则主张不可抗力的一方应就对方不合理 扩大的损失承担相应的责任。当事人对于合同不能履行或者损失扩大有

可归责事由的，应当承担相应责任； 当事人迟延履行后发生不可抗力的，不能免除违约责任。

14.2情势变更

合同成立后，合同的基础条件发生了在订立合同时无法预见的、不属于商业风险的重大变化，继续履行合同对于一方明显不公平，或者继续履行确实存在重大客观困难但尚不构成不可抗力的，受不利影响的一方可以与相对方重新协商；在合理期限内协商不成的，各方均有权请求人民法院或者仲裁机构变更或者解除合同。

第十五条 送达地址与法律后果

15.1送达地址

本合同载明的各方联系方式应被视为各方有效的送达地址。

送达地址适用范围包括双方在合同履行过程中各类通知、协商、请求等文件的送达，以及发生争议时相关文件和诉讼或仲裁法律文书的送达。

15.2送达地址变更

各方送达地址需要变更时，应当按照原送达地址通知对方；在仲裁及诉讼程序中地址变更的，应当同时向仲裁机构或法院履行送达地址变更通知义务。

任何一方未按前述方式履行通知义务，本合同载明的送达地址仍视为有效送达地址。

15.3司法送达与法律后果

仲裁机构、法院进行送达时可直接按照本合同载明或依据本合同变更后的送达地址予以邮寄送达。

因本合同载明的送达地址不准确、变更地址后未及时履行告知义务、法定代表人或联系人拒绝签收等原因导致法律文书未能被实际签收的，邮寄送达的，以

法律文书退回之日视为送达之日；直接送达的，送达人当场在送达回证上记明情况之日视为送达之日；非收件人本人签收而由他人代收的，视为收件人签收。

第十六条　其他

16.1如本合同的任何条款被视作无效，则上述条款可被分离，其余条款仍具有法律效力。

16.2本合同任何条款与法律、行政法规相抵触的，从其规定；与其他强制性规定相抵触的，由各方协商确定；协商无法获得一致的，向约定的争议解决机构提请依法解决。

16.3本合同的各条款标题仅为了便于记忆或用于检索，条款的具体含义应以具体条款的文字表述为准。

（以下无正文）

甲方（数据需方）：	乙方（数据供方）：
法定代表人/授权代表人：	法定代表人/授权代表人：
数据安全负责人：	数据安全负责人：
签约日期：	签约日期：
签约地点：	