競天公誠律師事務所
JINGTIAN & GONGCHENG

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

北京市竞天公诚律师事务所

关于

浙江太美医疗科技股份有限公司香港上市项目中国法项下

数据处理合规事项的

法律意见书

競天公誠律師事務所
JINGTIAN & GONGCHENG

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

目 录

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

释 义

在本法律意见中，除非文义另有所指，下列词语具有下述含义：

竞天公诚或本所	指	北京市竞天公诚律师事务所
公司	指	浙江太美医疗科技股份有限公司及纳入其合并报表的境内控股子公司
《法律意见书》	指	《关于浙江太美医疗科技股份有限公司香港上市项目中国法项下个人信息和重要数据处理合规事项的法律意见书》
《个保法》	指	《中华人民共和国个人信息保护法》
《数安法》	指	《中华人民共和国数据安全法》
《网安审查办法》	指	《网络安全审查办法》
《关基条例》	指	《关键信息基础设施安全保护条例》
《安全评估办法》	指	《数据出境安全评估办法》
《数据跨境规定》	指	国家互联网信息办公室 2024 年 3 月 22 日公布的《促进和规范数据跨境流动规定》

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

《个人信息安全规范》	指	GB/T 35273-2020《信息安全技术 个人信息安全规范》
《数安条例》	指	《网络数据安全管理条例》2021 年 11 月 14 日公布的征求意见稿版本
《数据分类分级规则》	指	GB/T 43697-2024《数据安全技术 数据分类分级规则》
《人遗条例》	指	2024 年 5 月 1 日施行的《人类遗传资源管理条例》
《人遗条例实施细则》	指	2023 年 7 月 1 日施行的《人类遗传资源管理条例实施细则》
《暂行办法》	指	《生成式人工智能服务管理暂行办法》
员工	指	公司以各类用工形式聘用的劳动者，包括签订劳动合同的职工，以及建立劳务关系的外部顾问、劳务派遣人员、实习生。
客户业务数据	指	客户拥有数据处理自主决定权的数据，为本法律意见书之目的，包括客户使用公司提供的各类软件产品过程中所产生的数据，以及公司在为客户提供数字化服务过程中接触到的客户相关数据。
CRM	指	Customer Relationship Management，客户关系管理。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

CRC	指	Clinical Research Coordinator，即临床研究协调员，又称研究协调员／机构协调员，临床试验协调员等。在临床试验中协助研究者进行项目管理与协调等非医学判断相关工作的人员，是临床试验的参与者、协调者。
CRO	指	Contract Research Organization，合同研究组织，通过签订合同授权，执行申办者或者研究者在临床试验中的某些职责和任务的单位。
SMO	指	Site Management Organization，临床资源管理组织或临床试验现场管理组织。协助临床试验机构进行临床试验具体操作的管理良好的专业商业机构及现场管理工作的查核机构。
SDK	指	Software Development Kit，软件开发工具包。
个人信息	指	以电子或者其他方式记录的与已识别或者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。
敏感个人信息	指	是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

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

		周岁未成年人的个人信息。敏感个人信息的类型和示例详见《个人信息安全规范》。
个人信息的处理	指	个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动
重要数据	指	一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。
个人信息出境	指	个人信息处理者将在中国境内运营中收集和产生的个人信息传输、存储至境外；个人信息处理者收集和产生的个人信息存储在中国境内，境外的机构、组织或者个人可以查询、调取、下载、导出；或者国家网信办规定的其他个人信息出境行为。
香港	指	中华人民共和国香港特别行政区
联交所	指	香港联合交易所有限公司
本次上市或香港上市	指	浙江太美医疗科技股份有限公司在联交所主板上市
中国或我国	指	中华人民共和国，为本法律意见之目的，不包括香港特别行政区、澳门特别行政区及台湾地区。

競天公誠律師事務所
JINGTIAN & GONGCHENG

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

北京市竞天公诚律师事务所

关于浙江太美医疗科技股份有限公司香港上市项目中国法项下

个人信息和重要数据处理合规事项的

法律意见书

致：浙江太美医疗科技股份有限公司

北京市竞天公诚律师事务所（“**本所**”）是在中华人民共和国注册并执业的律师事务所。根据浙江太美医疗科技股份有限公司之委托，本所担任浙江太美医疗科技股份有限公司香港上市项目中国法项下个人信息和重要数据处理合规的专项法律顾问，根据《个保法》《数安法》《安全评估办法》等中华人民共和国法律、法规和部门规章，并参照《个人信息安全规范》《数据分类分级规则》等国家推荐性标准的有关规定，及《数安条例》等相关重要文件之征求意见稿，按照律师行业公认的业务标准、道德规范和勤勉尽责精神，出具本法律意见。

为出具本法律意见，本所律师作出如下承诺和声明：

一、本所律师已根据本法律意见出具日以前已发生或存在的事实和我国现行法律、法规和部门规章的有关规定，并根据本所律师对有关事实的了解和对有关法律的理解发表法律意见。鉴于《个人信息保护法》于 2021 年 11 月 1 日正式施行，本所律师核查的合规要求仅针对公司目前业务情况和个人信息保护要求和处理方式是否合规发表意见，无法涵盖之前在《个保法》前已经发生的个

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

人信息处理行为。

二、本所律师已严格履行法定职责，遵循勤勉尽责和诚实信用原则，对公司业务中有关个人信息和重要数据保护事项是否符合中华人民共和国法律法规的要求进行充分的核查验证，保证本法律意见不存在虚假记载、误导性陈述及重大遗漏。鉴于公司业务中个人信息主体数量众多，本所律师主要采取抽查方式进行核验。

三、为出具本法律意见，本所律师对公司业务中有关个人信息和重要数据保护的情况进行了尽职调查，相关方已向本所出具声明和保证：向本所提供了出具本法律意见书所必须的真实、完整、有效的原始书面材料、副本材料或者口头证言；所有书面文件的签字和/或印章均属真实；所有副本材料或复印件均与正本材料或原件一致；不存在任何虚假记载或误导性陈述，亦不存在任何重大遗漏。对上述声明和保证之充分信赖是本所出具本法律意见的基础和前提。

四、在本法律意见中，本所律师仅根据本法律意见出具日现行有效的中国法律、行政法规、部门规章和监管部门适用的有关文件的明确要求，对公司业务中有关个人信息和重要数据保护的合规性发表法律意见。对于对本法律意见至关重要而又无法得到独立的证据支持的事实，本所律师依赖于公司或其他有关单位出具的证明文件就该等事实发表法律意见。

五、本法律意见仅供公司为香港上市之目的使用，该意见可以被本次公司香港上市所聘请的保荐机构及境内外律师合理引用或合理信赖。非经本所书面同意，不得用作任何其他目的。

基于上述，本所律师依据中华人民共和国有关法律、法规、部门规章和规范性文件，在对公司业务中的个人信息和重要数据保护情况进行充分的核查验证的基础上，发表如下法律意见。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

正 文

一、 员工个人信息处理

（一） 个人信息处理范围

根据公司提供的书面说明，截至 2024 年 3 月 31 日公司在职员工 831 人，根据公司介绍，公司员工（含候选人阶段）个人信息的处理目的及所收集的个人信息类型如下：

表一

处理目的	个人信息类型	敏感个人信息	收集来源
招聘与面试（候选人）	个人基本资料（姓名、性别、个人电话号码等）、个人教育工作信息（教育经历、工作经历等）	一般不会涉及	个人主动提供，或经由猎聘等第三方渠道收集。
背景调查（候选人）	个人基本资料、个人教育工作信息、个人财产信息（征信信息）、个人身份信息（身份证等）	个人财产信息（征信信息）、个人身份信息（身份证等）	个人主动提供，政府网站或其他单位/机构等第三方渠道
录用前体检（候选人）	个人基本资料、个人健康生理信息（检验报告）	个人健康生理信息（检验报告）	个人主动提供
办理入职	个人基本资料、个人身份信息（身份证等）、个人教育工作信	个人身份信息（身份证等）、个人健康生理信息（检验报	个人主动提供

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	息、个人健康生理信息、个人财产信息（银行账户）	告）、个人财产信息（银行账户）	
门禁与考勤	个人基本资料、个人位置信息（精准定位信息）	个人位置信息（精准定位信息）	个人主动提供
请休假管理	个人基本资料、个人健康生理信息（相关的诊疗单据、怀孕证明、预产期诊断书、子女出生证明、工伤诊断证明等）、其他信息（婚史）	个人健康生理信息（相关的诊疗单据、怀孕证明、预产期诊断书、子女出生证明、工伤诊断证明等）、其他信息（婚史）	个人主动提供
社会保险缴纳	个人基本资料、个人身份信息（身份证等）、个人财产信息（银行账户、流水记录等）	个人身份信息（身份证等）、个人财产信息（银行账户、流水记录等）	个人主动提供
商业保险投保	个人基本资料、个人身份信息（身份证等）、个人健康生理信息	个人身份信息（身份证等）、个人健康生理信息	个人主动提供
薪酬发放	个人基本资料、个人身份信息（身份证等）、个人财产信息（银行账户、流水记录等）	个人身份信息（身份证等）、个人财产信息（银行账户、流水记录等）	个人主动提供
差旅预订	个人基本资料、个人身份信息（身份证等）、个人位置信息	个人身份信息（身份证等）、个人位置信息	个人主动提供

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	（行踪轨迹、住宿信息）	（行踪轨迹、住宿信息）	
财务报销	个人基本资料、个人财产信息（银行账户、交易和消费记录等）	个人财产信息（银行账户、交易和消费记录等）	个人主动提供
视频监控	视频录像信息	视频录像信息	公司直接收集
员工办公行为监控	个人常用设备信息、个人上网记录（网页浏览记录）	个人上网记录（网页浏览记录）	公司直接收集
员工离职	一般不会新收集员工个人信息	/	个人主动提供

根据本所律师核查，公司处理员工个人信息的目的均合法、正当且处理的个人信息与前述处理目的直接相关，限于实现处理目的的最小范围，符合《个保法》第五条、第六条等条款所述的各项原则。

（二） 个人信息处理活动

1. 个人信息处理的合法性基础及告知义务履行

根据《个保法》第五条的规定，处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。同时，《个保法》第十三条规定必须具备处理个人信息的合法性基础方可处理个人信息。根据该条款，合法性基础包括（一）取得个人的同意；（二）为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）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；（五）为公共利益实施新闻报道、舆论监督等行为，

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律、行政法规规定的其他情形。该条款同时规定，“处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意”。

根据《个保法》第十七条，个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：（一）个人信息处理者的名称或者姓名和联系方式；（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；（三）个人行使本法规定权利的方式和程序；（四）法律、行政法规规定应当告知的其他事项。

根据本所律师的访谈和查证，公司在招聘与面试、背景调查、录用前体检、商业保险投保等需要取得候选人授权同意作为个人信息处理合法性基础的场景中，通过要求候选人/员工阅读并签署《个人信息处理授权同意书》取得了候选人/员工的授权同意。《个人信息授权同意书》涵盖《个保法》第十七条规定的告知事项。在员工办理入职、门禁与考勤、请休假管理、社会保险缴纳、薪酬发放、差旅预定、财务报销、员工办公行为监控等需要援引“为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需”以及“为履行法定职责或者法定义务所必需”作为合法性基础的场景中，公司已通过员工入职时向其提供《员工个人信息保护规则》并要求员工签署，向员工履行《个保法》第十七条所要求的告知义务。

公司亦存在从第三方间接获取职位候选人个人信息的情形，此类第三方包括猎聘、BOSS 直聘、前程无忧、拉勾以及猎头公司。猎聘、BOSS 直聘、前程无忧、拉勾均已通过公示隐私政策并要求用户注册时主动勾选隐私政策的方式告知用户向公司等招聘方提供其个人信息的处理目的等事项并取得其授权同意。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

公司承诺在与猎头公司签署服务合同前已核查其从事人力资源业务所需具备的资质条件。对于第三方提供的候选人个人信息的处理，根据公司的说明，公司仅留存经评估可进入面试阶段的候选人个人信息，且对于候选人个人信息的处理限于与招聘相关的目的，未超出必要范围。

2. 敏感个人信息处理

根据《个保法》第二十八条、第二十九条、第三十条的规定：处理敏感个人信息需具备特定的目的和充分的必要性；除非法律、行政法规另有规定，个人信息处理者处理敏感个人信息应取得个人的单独同意，同时除向个人告知《个保法》第十七条所要求的各类告知事项外，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。

据公司提供的资料文件并经本所律师核查，公司背景调查目的为核实候选人简历信息真实性及信用状况，且仅抽查部分人员；录用前体检意在了解候选人是否具备从事相关岗位的身体条件；公司仅为部分管理层人员投保商业保险。前述涉及敏感个人信息处理并以个人授权同意为个人信息处理的合法性基础的场景中，公司通过候选人/员工阅读并签署《个人信息处理授权同意书》配合具体处理场景下人事部门通知的方式取得了个人单独同意。同时，在《个人信息处理授权同意书》中含有对该等敏感个人信息处理必要性及对个人权益影响的描述。

3. 个人信息委托处理

根据《个保法》第二十一条的规定，个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

公司委托第三方进行候选人背景调查，据本所律师核查，公司已与第三方

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

背景调查公司八方锦程人力资源（惠州市）有限公司签署的《背景调查服务合同》，双方已就委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等进行了约定，同时根据合同约定，由公司直接向候选人提供相关个人信息采集表和授权书，可实现对第三方背景调查公司受托处理行为的有效监督。

公司使用“钉钉”软件进行员工日常管理，根据根据钉钉公布的《钉钉隐私权政策》（生效日期为 2024 年 7 月 3 日），当企业开通钉钉服务并要求员工使用时，视同企业将其员工数据委托钉钉处理，企业则被视为个人信息处理者。《钉钉隐私权政策》对受托处理范围等事项向注册用户进行了充分告知并要求用户注册时进行了阅读和主动勾选同意。

4. 个人信息存储

根据《个保法》第十九条的规定，除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

根据本所律师的访谈和查证，公司员工个人信息存在不同保存期限策略。当相关职位候选人没有最终聘用时，公司将会及时删除其个人信息，具体方式为删除订阅的简历邮件或销毁相应文档；当相关职位候选人确认聘用后，公司会将其简历及应聘文件保存为纸质人事档案进行管理。根据《企业文件材料归档范围和档案保管期限规定》的要求，该档案目前的管理期限为永久。

此外，公司员工个人信息存储于中国境内，不存在个人信息出境行为。

5. 其他个人信息处理活动

根据公司的说明和承诺，公司未对员工个人信息进行公开、汇聚融合、自动化决策等处理活动。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

6. 个人信息保护影响评估

根据《个保法》第五十五条、第五十六条的规定，个人信息处理者在处理敏感个人信息、委托处理个人信息时，应当事前进行个人信息保护影响评估，并就处理情况进行记录。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

公司承诺已按照《个保法》及相关国家标准对法定个人信息处理场景进行个人信息保护影响评估，并将评估报告和处理情况记录至少保存三年。根据公司提供的证明文件，公司已就员工办理入职、背景调查以及委托“钉钉”处理员工个人信息等场景进行事前个人信息保护影响评估并撰写书面报告，且就处理情况进行了记录。

（三） 个人信息主体权利

根据《个保法》，并参考《个人信息安全规范》、《数安条例》的要求，个人信息主体权利包括抽象的知情权、决定权、限制权、拒绝权，也包括具体的查阅权、复制权、更正权、删除权、撤回同意权、可携带权（转移权）和说明权，同时，针对特殊场景下个人信息主体也被赋予了额外权利，如自动化决策场景中个人信息主体对通过自动化决策方式作出对个人权益有重大影响的决定享有释明权，再如，逝者近亲属也被赋予了行使查阅、复制、更正、删除权的权利。

经本所律师查验，结合公司提供的《员工手册》《员工个人信息保护规则》《个人信息授权同意书》《承诺函》等文件资料，公司向员工告知了其享有的各项个人信息主体权利，同时指定人力资源部门专人负责员工的行权事宜，对员工的权利行使要求及时响应和处理。

（四） 法律意见

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

综合上述，本所律师认为公司对员工个人信息的处理符合《个保法》等相关法规的规定，未发现明显违法违规事项。

二、 供应商/客户联系人个人信息处理

（一） 个人信息处理合规现状

根据公司的说明和承诺，截至 2024 年 3 月 31 日，公司处理的供应商/客户联系人数量合计不超 10,000 人。公司基于业务合作中的往来联系目的处理供应商/客户联系人的个人信息，涉及的个人信息字段主要包括姓名、手机号、邮箱、工作单位及职位等个人基本信息，不涉及敏感个人信息。公司对供应商/客户联系人个人信息的处理不存在误导、欺诈、胁迫等情形，且未超出《个保法》所要求的合法、正当及必要的范围。

考虑到供应商/客户联系人个人信息主要来源于联系人在商务往来中主动向公司采购或销售人员提供，其对于公司的处理目的和处理方式存在明确预期，即公司仅会在必要的双方商务合作场景处理其个人信息，其主动提供的行为可视为构成《个保法》第十三条列举的合法性基础之一，即公司“取得个人的同意”。

公司亦自供应商/客户处间接收集联系人个人信息，此时供应商/客户将其基于履行劳动合同所必需而处理的联系人信息向公司提供，供应商/客户无需获取联系人的授权同意。公司承诺其在合同签订过程中会对供应商/客户是否在中国境内合法经营和存续进行审核，并要求供应商/客户承诺其向公司提供的联系人信息已具备《个保法》第十三条列举的合法性基础。本所律师认为公司该等行为可被认定为尽到了审查供应商/客户联系人个人信息来源合法性的合理努力。

公司使用本地化部署的“销帮帮”CRM 系统进行客户联系人个人信息管理。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

公司承诺对供应商/客户联系人个人信息仅在实现处理目的所必要的期限内存储，超出该期限，将对供应商/客户联系人个人信息进行删除或匿名化处理。

公司承诺将响应或协助供应商/客户响应联系人对其个人信息主体权利的各项请求并在法定期限内处理。

根据公司的说明和承诺，公司未对供应商/客户联系人个人信息进行委托处理、对外提供、向境外提供、公开、汇聚融合、自动化决策等处理活动。

（二） 法律意见

综合上述，本所律师认为公司对供应商/客户联系人个人信息的处理符合《个保法》等相关法规的规定，未发现明显违法违规事项。

三、 公司主营业务涉及的个人信息处理

（一） 公司主营业务类型

公司向客户提供临床研究解决方案以及生命科学营销解决方案，包括各类部署于第三方公有云或客户私有化部署的软件产品，以及多样化的数字化服务。主要的软件产品和数字化服务如表二所列：

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

表二

类别	名称	主要功能	数据存储方式	客户业务数据涉及的自然人身份类型	个人信息类型	主要客户
软件	eCooperate/CTMS	临床试验项目的电子化及数据化管理	第三方公有云	临床试验项目团队人员，不涉及受试者/患者	个人基本资料	生命科学企业、临床研究机构、CRO
	eArchives/eTMF	临床研究档案的电子化管理	第三方公有云	受试者/患者	匿名化	
	eCollect/EDC	具有远程数据评估及透明数据标准的电子数据采集系统	第三方公有云	受试者/患者	匿名化	
	eBalance/IWRS	临床试验中的随机选择、入组、药品供应及分配、紧急揭盲等工作	第三方公有云	受试者/患者	匿名化	

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	eImage/IRC	对以影像评估为终点的临床研究进行独立影像评估	第三方公有云	受试者/患者	匿名化	生命科学企业
	eSafety/PVS	自动扫描及下载监管部门的反馈，并自动生成安全报告	第三方公有云	受试者/患者	匿名化	
	ONECEM	ONECEM-SCRM，促进客户关系智能管理	第三方公有云，或私有化部署	医生	个人基本资料	生命科学企业
		ONECEM-SFE，将销售效率管理数字化	第三方公有云，或私有化部署	客户的销售人员	个人基本资料	
		ONECEM-Event 及 ONECEM-Engagement，简化会议管理和现场直播，实现在线互动	第三方公有云，或私有化部署	讲者、医生	个人基本资料	
数字化服务	IRC 服务	协助生命科学企业进行医学影像的独立评估	依托客户购买的软件服务	受试者/患者	匿名化	生命科学企业

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	数字化临床研究服务	数字化 SMO 派发及管理服务、促进临床试验及其他相关流程	依托客户购买的软件服务	CRC 及其他临床试验项目参与人员、受试者/患者	CRC 个人基本资料及受试者/患者的经匿名化处理的数据	

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

（二） 公司运营的涉及个人信息处理的主要网站、App、小程序

根据公司提供的说明和清单，截至 2024 年 3 月 31 日，公司运营的涉及个人信息处理的主要网站、App、小程序如下所列：

1. 官方网站

类型	名称	主要功能	涉及处理的个人信息（角色）	用户数量（人）
网站	圣方（上海）医药研发有限公司官方网站 https://www.ecr-global.com/	品牌展示与推广、业务介绍与咨询等。	在线留言用户的姓名、联系电话、公司名称、邮箱、留言内容等信息；咨询用户的姓名、电话、邮箱、咨询的服务内容等信息。（个人信息处理者）	约1,337
	浙江太美医疗科技股份有限公司官方网站 https://www.taimei.com/		申请试用用户的姓名、手机号码、公司名称、职位、所在区域信息；咨询用户的姓名、电话、邮箱、留言内容等信息。（个人信息处理者）	

2. 医药研发协作平台

类型	名称	主要功能	涉及处理的个人信息（角色）	用户数量（人）
网站	TrialOS 药试圈 https://www.trialos.com/	公司临床试验软件产品的集成平台和统一入口，亦向社会公众开放注册，提供医药资讯信息以及其他相关服务。	姓名、用户名、密码、手机号码、电子邮箱、微信共享账户信息（微信 ID、微信昵称、头像）、企业名称、搜索查询记录、角色、设备信息（设备型	352,596
App	药试圈	网站 TrialOS 药试圈的移动端使用入口，可使用部分临床试验软件产品，频道及功能设置相对 web 端简单。		

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	采集易	eCollect/EDC 的移动端	号、操作系统版本、设备设置、Android ID）、系统权限信息等。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	
	随访易	ePro 的移动端		
	Trial Ops	eCooperate/CTMS 的移动端		
	管培易	eCollege 的移动端		
	远程监查	eMonitor 的移动端		
	eSMS	eSMS 的移动端		
小程序	开心随访 evisit	eVisit 的移动端		

3. 生命科学营销平台

类型	名称	主要功能	涉及处理的个人信息（角色）	用户数量（人）
网站	PharmaOS 平台 https://www.pharmaos.com/	公司生命科学营销软件产品统一入口	姓名、手机号码、密码、电子邮箱、微信 open ID、微信共享信息（昵称、头像）。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	6,175
小程序	销邦会 Plus2	提供给企业用户的员工及其客户使用专业的浏览在线学术资料、医学信息，进行互动的平台	微信 open ID、微信共享信息（昵称、头像），必要的系统权限（麦克风、摄像头等）（个人信息处理者） 客户业务数据。（个人信息受托处理方）	20,568
	销邦会 UAT2			307
	销帮会2			14,315
	销深客	订购销深客 CRM 系统客户远程拜访模块的扩展使用		26,700

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

	母婴营养 e 学界	雀巢 ETMS 项目远程会议模块的拓展功能，使用人均为雀巢 NFO 的员工及客户		148,000
	太美销深客资料库	销深客资料库为销深客 CRM 系统的拓展功能，主要用于资料的分享阅读，使用群体为购买此功能的企业客户员工及其客户	微信 openID，微信共享信息（头像，昵称）（个人信息处理者）	5,227
合计				221,292

4. “无界”产品

类型	名称	主要功能	涉及处理的个人信息（角色）（字体加粗字段为敏感个人信息）	用户数量（人）
网站	无界网站 https://www.wujieos.com/	医院的运营后台，提供无界学术 App 的医生账号权限、医院学术空间、统计分析等后台管理功能	医院管理人员手机号码、**代表的证件信息(身份证、护照)**、代表手机号。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	0

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

App	无界企业	面向医药代表和医生的平台，提供在线沟通、远程会议、学术内容推荐等功能服务。仅向企业授权用户开放。	账户信息（手机号码）。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	0
	无界学术	学术会议、学术直播、学术咨询、企医沟通、新药发布等。	姓名、手机号、**身份证号码**、所在医院、科室、职称、职务、**资格证/医生执业证书/工作证/胸牌/职称证**。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	500
小程序	无界会议	会议直播互动平台	微信 openID，用户信息(头像，昵称)、必要系统权限（麦克风、摄像头、本地相册）。（个人信息处理者） 客户业务数据。（个人信息受托处理方）	569
合计				1,069

5. 药试圈患者招募

公司处理“药试圈患者招募”中各网站、App、小程序涉及的个人信息时，其在数据处理活动中的角色为个人信息处理者。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

类型	名称	主要功能	涉及处理的个人信息（字体加粗字段为敏感个人信息）	用户数量（人）
网站	药试圈患者招募平台 https://trialnet.cn/	患者招募项目申请、患者管理及随访服务、推送医学资讯及临床试验项目受试者招募信息	姓名、电话、年龄、**病症、身体状况、药物治疗情况、病历、病理报告、影像检查报告、最新的检验化验单、用药记录、检查报告、现病史、既往史**	5,604
		商务合作	姓名、联系方式、企业名称或个人工作单位、科室	
小程序	药试圈招募	账户管理	手机号码、微信共享账户信息（昵称、头像）	54,172
		患者招募项目申请	患者称呼、**疾病名称**、患者年龄、**身份证号码、身体状况、病史描述**	
		患者管理及随访服务	**病史资料（病历、病理报告、影像检查报告、最新的检验化验单）**	
		招募先锋申请	称呼、工作单位、部门、科室、职位、工牌、名片	
		/	业务功能试用中必需的设备信息和系统权限	
App	药试圈从业者	账户管理	手机号码、微信共享账户信息（昵称、头像）	6,492
		招募先锋申请	称呼、工作单位、部门、科室、职位、工牌、名片	
		意见反馈	称谓、电话、反馈问题详情	
		管理患者信息	患者姓名、年龄、**疾病信息、用药记录、疾病分期、疾病分型、肿瘤相关的基因突变结果、体征体能、病史资料**	

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

		/	业务功能使用中必需的设备信息和系统权限	
合计				66,268

截至 2024 年 3 月 31 日，公司运营的涉及个人信息处理的网站、App、小程序用户数量累计 642,562 人。

（三） 公司在个人信息处理活动中的角色

1. 个人信息处理者

个人信息处理者有权自主决定个人信息的处理目的和处理方式，同时需履行各项法定义务：

(1) 个人信息处理的合法性基础及告知义务履行

截至 2024 年 3 月 31 日，公司所运营的网站、App、小程序均已配备隐私政策文本，告知用户《个保法》第十七条所列明的事项，并要求用户在提供相关个人信息前阅读并主动同意隐私政策。同时，经本所律师适当核查并根据公司提供的承诺，公司在用户同意隐私政策前不会收集用户个人信息，并且未超出处理目的所必要的范围、隐私政策所声明的范围收集处理用户个人信息。

“无界产品”“药试圈患者招募”服务涉及处理敏感个人信息，根据公司的说明和承诺，此类敏感个人信息是进行用户身份认证、临床试验项目患者招募所必要的个人信息。各网站、App、小程序隐私政策中敏感个人信息以有别于一般个人信息的方式显著标识，内容除涵盖《个保法》第十七条所列明的事项外，同时含有对该等敏感个人信息处理必要性的描述。在用户个人信息填写界面，公司通过文字说明告知用户个人信息处理目的，结合用户的主动填写行为，本所律师认为可构成《个保法》第二十九条所要求的用户对敏感个人信息处理的单独同意。

(2) 个人信息对外提供

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

在“药试圈患者招募”服务中，公司将患者的疾病名称、患者年龄、身体状况、病史描述、病史资料（病历、病理报告、影像检查报告、最新的检验化验单）信息进行脱敏处理后提供给患者所报名的药物临床试验项目申办方和研究者，接收方依此判断患者是否符合临床试验的要求。公司已在隐私政策中对前述个人信息对外提供行为按照《个保法》第二十三条的相关要求进行了披露，并通过在个人信息填写页面说明敏感个人信息的处理目的等方式取得了患者的单独同意。

(3) 个人信息存储

根据公司提供的隐私政策模板，公司声明“我们会采取合理可行的措施，尽力避免收集无关的用户信息。我们只会在达成本政策所述目的所需的期限内保留您的用户信息，除非受到法律的允许。超出上述用户信息保存期限后，我们会对您的个人信息进行删除或匿名化处理。”公司承诺已落实前述存储规则。

此外，公司所运营网站、App、小程序处理的用户个人信息存储于第三方公有云，不存在个人信息出境行为。

(4) 系统权限调用及第三方 SDK 集成

公司所运营的 APP 及小程序涉及对移动设备系统权限的调用，并且集成了第三方 SDK。根据公司出具的承诺并经本所律师适当核查：公司所调用的系统权限均为实现特定处理目的所必需、未提前申请权限、权限申请前已告知用户该权限的调用目的、调用频次未超出实现处理目的必要范围；在 App 集成第三方 SDK 前，公司将针对第三方 SDK 进行全面的安全检测和评估，在通过评估后才允许使用，同时不定期对 SDK 行为进行抽检、监督，如有违规情况立即停止接入该 SDK，并将其列入不合作清单，公司还在相关 APP 及小程序的隐私政策中对所集成的第三方 SDK 的名称、厂商、处理个人信息范围及目的、数据安全保障能力等事项进行了披露。

(5) 其他个人信息处理活动

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

根据公司的说明和承诺，公司未对用户个人信息进行公开、汇聚融合、自动化决策等处理活动。

(6) 个人信息保护影响评估

根据公司提供的《个人信息保护影响评估报告》，公司已针对“药试圈招募”小程序涉及的敏感个人信息处理场景按照《个保法》第五十五条、第五十六条的要求进行个人信息保护影响评估。

(7) 个人信息主体权利

公司面向用户的隐私政策均就用户的各项个人信息主体权利进行了描述，用户可通过隐私政策说明的路径行使权利，公司承诺并可在 15 个工作日内完成响应。

(8) 法律意见

综合上述，本所律师认为公司对所运营网站、App、小程序用户个人信息的处理符合《个保法》等相关法规的规定，未发现明显违法违规事项。

2. 个人信息受托处理方

在提供本法律意见书“表二”所列的各类软件产品和数字化服务处理客户业务数据时，以及在运营网站、App、小程序处理客户业务数据时，公司在数据处理活动中的身份为个人信息处理受托处理方。作为个人信息受托处理方，公司需按照客户的指示在受托范围内处理数据，无权自主决定个人信息的处理目的和处理方式。

根据《个保法》第二十一条以及《个人信息安全规范》第 9.1 条的相关规定，个人信息受托方应当按照与委托处理的个人信息处理者约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

同时，受托方应协助个人信息处理者响应个人信息主体的权利请求。

在提供软件产品服务，运营网站、App、小程序过程中，根据公司的说明和承诺，公司对客户业务数据无访问权限，仅提供服务必要范围内的数据云存储服务且涉及存储的受试者/患者个人信息已进行匿名化处理，从而不再属于《个保法》定义的个人信息范畴。公司承诺仅在客户提出故障排除等服务需求的特殊场景下，公司有访问到客户业务数据的可能，该等数据可能包含个人信息，但是公司的访问权限在事前得到了客户的授权，且客户会对公司的访问行为进行记录和审计。

与提供软件产品服务不同，公司在提供数字化服务过程中会接触到客户业务数据。但公司乃基于客户委托受托处理数据，对数据的使用方式不具有自主决定权。数字化 SMO 派发及管理服务中公司负责向客户提供 CRC 服务，CRC 简历信息来源于供应商 SMO 公司的自主上传且简历信息为公司定义，未超出为客户提供 CRC 推送服务的必要范围，公司在 SMO 公司入驻前已要求其提供并审核其具备的相关资质。公司依托客户自行购买的软件服务提供数字化服务，仅在受托范围内处理和存储客户业务数据。

在提供上述服务时，当委托合同不生效、无效、被撤销或者终止时，公司会将所存储的包括个人信息在内的全部业务数据返还个人信息处理者或者予以删除，不会私自留存，除非已经过匿名化处理。

公司承诺对于客户提出的协助响应个人信息主体权利的请求，公司会在能力与权限所及的范围内予以协助。

同时，公司说明未有客户提出签订补充的数据委托处理协议的要求，经查阅公司与客户签署的服务合同，公司已与相关客户签署《保密协议》《信息安全保密协议》，就包括客户业务数据在内的保密义务进行承诺和约定。公司未超出为客户提供服务的目的超范围使用客户业务数据。

(9) 法律意见

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

综合上述，本所律师认为公司在提供各类软件产品和数字化服务，运营网站、App、小程序时的个人信息受托处理活动符合《个保法》《个人信息安全规范》等相关法规的规定，未发现明显违法违规事项。

四、 数据安全保护义务的履行

根据《个保法》《数安法》等相关法规的规定，数据处理者应建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。

（一） 数据安全管理制度和操作规程

公司制定了涵盖人员管理和培训、数据安全技术措施、身份管理和访问控制、风险预警和处置以及信息安全事件预防和响应等在内的数据安全管理制度和操作规程，包括但不限于《员工信息安全行为规范》《信息安全违规处罚规范》《员工入离职管理流程》《数据分类分级安全规范》《数据分类分级指南》《信息安全管理策略》《数据安全管理策略》《数据泄露防护管理流程》《数据备份及恢复程序》《信息安全密钥管理办法》《数据使用安全规范》《敏感数据使用规范》《数据存储安全规范》《数据传输安全规范》《数据销毁安全规范》《对外数据披露管理规范》《个人信息保护管理规定》《信息系统账号和密码管理流程》《信息安全风险评估和处置流程》《信息安全事件管理规范》《信息系统灾难恢复计划》，形成了一整套覆盖数据全生命周期的内部管理体系。

据公司说明，为了强化公司内部建设，公司质量部每半年对内部管理制度进行复核，以评估现有流程规范是否满足公司内部控制要求以及外部监管环境变化，并按需进行更新。

（二） 人员管理和培训

公司任命运营保障部负责人（公司副总裁）为个人信息保护负责人，对个

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

人信息保护工作负全面领导责任，并独立向管理层汇报。公司信息安全管理部门负责统筹实施个人信息安全保护工作，业务部门参照信息安全管理部门编制的各类个人信息保护政策进行个人信息安全保护工作并配合进行个人信息安全事件处置。

公司通过《员工手册》《员工信息安全行为规范》等规范员工的行为准则、奖惩措施及培训活动要求，明确员工在员工纪律和信息安全方面所承担的责任和义务。同时，规范员工培训相关计划、实施、督导以及考评等相关流程。新员工在入职时须签署劳动合同和保密协议，以确保员工在入职前知悉其在信息安全方面应承担的责任和义务。

公司构建了一系列培训体系及考核流程要求，包括但不限于以下方面：

- 新员工须在入职后一个月内完成入职培训并通过相关考核，培训内容涉及公司企业文化、业务概况、规章制度及信息安全等领域；
- 在职员工每年须参加公司组织的信息安全培训并通过相关考核，以维持自身的信息安全意识及信息安全保护能力；及
- 信息安全中心设计并实施了多种安全意识宣贯手段，会不定期通过邮件、宣传画等形式将安全意识向员工进行宣导。

此外，为了进一步巩固公司信息安全管理体系，公司建立了专用邮箱，内外部人员均可通过该渠道及时上报信息安全事件，公司信息安全中心每月对员工信息安全违规事件进行评估，评估结果及相关处理决定依据事件影响程度通过内部渠道进行公告。

员工电脑标配安装商业版杀毒软件确保自身电脑环境的安全可控；标配安装数据防泄密产品确保数据外泄的可控与审计。员工在正式离职前，须完成基于钉钉的离职申请流程，确保员工账号得以被及时清理，相关办公设备得以被及时交接。公司域控管理员与各内部支撑系统的管理员须在离职员工直属上级及人力资源部负责人审批通过后在离职申请流程内对账号清理结果予以确认。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

离职员工仅能在离职申请流程处理完毕、账号已完成清理后离岗。

（三） 安全技术措施

客户端与服务器的通信基于 HTTPS 进行加密传输，密码信息会先在客户端进行 MD5 加密再进行传输，密码密文在服务端进行二次单向不可逆加密存储。针对个人身份信息与敏感个人信息使用国密 SM4 算法进行加密存储，且 SM4 算法选取了最长密钥长度 128 位。

公司中国境内提供的软件产品服务依托于阿里云与腾讯云提供的云计算服务，公司每年获取并审阅由阿里云与腾讯云提供的体系和机构控制报告，对其在安全性、保密性以及可用性方面能否满足公司要求进行评估，评估结果由公司信息安全中心负责人统筹进行潜在风险识别，制定风险应对方案并完成风险处置跟进。公司在公有云上购买了安全增值服务，包括“WEB 应用防火墙企业版”“云防火墙高级版”“云安全中心（态势感知）高级版”等，同时根据业务的具体需求，在以上安全功能中进行了具体的策略配置，可对网络攻击等行为进行告警、阻断，同时配备了安全管理员对产生的日志告警进行分析，能及时地发现安全事件并启动应急响应程序，有效地确保了生产业务的安全性。

在数据备份管理方面，公司针对关键业务数据采取了每周执行本地全量备份的策略，同时构建了异地备份策略，将本地备份数据自动同步至异地备份服务器中。本地备份文件与异地备份文件均默认保留 90 天。同时，为保障所存储备份数据的可用性，公司建立了数据恢复性测试机制，每月由运维工程师对备份文件进行测试恢复以检测其数据可用性，检测结果记录在《备份文件验证报告》中。

为了保障公司业务的持续稳定运营，公司每年进行一次业务影响分析和风险评估，基于评估结果对各类潜在威胁评估最大可容忍中断时间、恢复时间目标和最小服务水平等指标并相应制定响应策略，评估结果记录在《业务影响分析、风险评估及策略报告》中。根据风险评估的结果，运营保障部每年组织相

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

关业务部门针对不同的业务场景进行业务连续性演练，记录演练结果。

公司持续在安全建设中进行投入，并积极参与行业安全建设，以下是目前公司在安全方面取得的认证：

- 公司运营的主要信息系统通过了等级保护（三级）测评并已向公安部门备案；
- 公司通过了 ISO27001、ISO27701、ISO27017、ISO27018、ISO9001、ISO20000 认证；
- 公司取得 SOC2 Type1 以及 SOC2 Type2（安全性、可用性、保密性、隐私性）鉴证报告。

（四） 身份管理和访问控制

公司制定了《信息系统账号和密码管理流程》和《员工入离职管理流程》制度，对公司各内部支撑系统进行了规范。

公司建立了网络准入要求，员工仅在办公网环境才可登录与使用各内部支撑系统，以实现对关键业务数据的安全防护。员工若需通过互联网发起对各内部支撑系统的访问，须通过 VPN 发起访问申请并通过基于域账号和密码的身份校验。此外，公司限制员工直接访问云上的生产环境服务器和数据库，相关的生产环境服务器和数据库访问请求均须通过堡垒机或数据库运维平台跳转实现。公司在堡垒机层面同步开启了命令执行黑名单和访问日志记录功能，可以在对高危操作命令进行阻断的同时保留 24 个月的登录、访问及操作记录（包括：登录 IP、登录方式、登录时间及操作内容等信息）。仅堡垒机管理员可以对黑名单内的命令进行调整。在数据库运维平台层面，公司禁止写入操作并永久保留登录、访问及操作记录（包括：操作名称、操作人、操作时间及操作内容等信息），从而实现对服务器和数据库访问请求的跟踪和统一化管理，保障访问的安全性。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

公司生产数据存储于境内第三方云环境，通过管理和技术手段严格控制员工对数据的访问。在产品、研发、运营方面，无任何授权途径和方式可以访问生产环境。在运维方面，根据权限最小化原则进行分配，相关人员连接服务器、数据库仅允许通过堡垒机进行访问，访问与操作行为受控，以确保在满足基础工作的需求下实现安全管控。

基于严格的安全管控策略，公司对相关权限管理、行为规范等方面进行审计。在内部支持系统权限管理方面，运营保障部会定期针对域控权限进行回顾，确保权限与访问受控。在行为规范方面，由于运维人员访问服务器仅允许通过堡垒机进行访问，堡垒机有录屏审计与敏感命令、下载上传等行为审计，故由信息安全管理部门负责监督与审计。同时公司还部署了数据库操作行为审计设备，针对异常的操作语句进行审计，确保数据库被安全访问。

公司通过 ITSM 系统、钉钉及 JIRA 系统对员工在入职、转岗、离职以及日常运营过程中出于业务需要产生的账号权限变更需求予以管理。

为保障员工在发生岗位调整时冗余权限得以被及时回收，公司建立了转岗权限梳理机制。

公司搭建了网络共享盘用于存放公司内部文件材料。为保障内部数据的安全性，公司默认未面向全体员工开放 VPN 和网络共享盘访问权限。员工若需访问，须通过钉钉或 ITSM 系统提交申请，经申请人所在部门负责人审批通过后，由运维工程师赋予员工对应权限。

（五） 风险检测和信息安全事件

公司为确保漏洞、安全事件及故障能够被及时地识别、响应和处理，制定《软件测试管理标准流程》，以规范各类产品须遵循的漏洞定级标准、漏洞处理及响应修复流程要求；制定《安全配置加固管理流程》，以规范产品相关服务器和网络设备须遵循的安全配置基线要求；制定《信息安全事件管理规范》为保障漏洞和故障得以被及时识别和应对，公司建立了一系列上报和检查机制，

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

以实现对潜在漏洞和故障的持续性检测，力求漏洞与故障在造成巨大损失前被修复。

公司制定了《信息安全风险评估和处置流程》，对公司须遵循的风险评估流程及要求进行了规范，包含风险识别、风险定级、风险分析以及对于超出可接受水平的风险须采取的响应处置措施等内容。

公司对在业务运营过程中可能涉及的各类安全事件进行了分析并依照严重程度由重至轻区分为一级事件、二级事件、三级事件和四级事件四个等级。公司设立了信息安全管理委员会，负责对可能发生的各类安全事件应采取的沟通和响应处理机制进行制定、评估并监督，确保响应机制的有效执行。

公司指派信息安全中心每年开展一次风险评估工作，基于不同的风险场景以及对公司内、外部环境变化的考量，对公司涉及人员、数据、软件等方面的风险敞口进行识别并评估其重要性水平，评估结果会形成风险评估控制矩阵。此外，信息安全中心协同相关业务部门制定整改措施并通过风险评估控制矩阵完成整改跟进。

根据公司的说明、承诺并经本所律师适当核查，截至 2024 年 3 月 31 日，公司未发生数据泄露、篡改、丢失等信息安全事件。

（六） 个人信息保护合规审计

《个保法》第五十四条规定，个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

作为个人信息处理者，公司每年针对其个人信息处理活动会进行梳理评估，并针对其合规性进行审计。作为受托方，公司按照客户要求配合进行合规审计。

（七） 法律意见

综上，本所律师认为公司已适当履行《个保法》《数安法》等相关法规要求的数据安全保护义务，未发现明显违法违规情形。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

五、 公司不涉及处理重要数据

根据国家互联网信息办公室发布的《安全评估办法》的定义，重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

据本所律师所知的范围，医疗领域尚未公布重要数据具体目录。基于《数据安全法》第二十一条之规定，对“重要数据”的识别，应先遵循特定的重要数据具体目录；在没有目录的情形下，可参考通用规范，分析出通用规范中重要数据定义、范围、识别要素等的关键要点，通过对关键要点进行比对分析，判断是否落入重要数据范畴。

根据公司提供给本所的资料、说明并经本所律师核查，公司作为个人信息处理者处理的数据类型不具备重要数据高度敏感的特性。

截至 2024 年 3 月 31 日，未曾有客户向公司声明其处理重要数据或运营关键信息基础设施。

法律意见：综上，本所律师认为公司业务不涉及《数安法》《安全评估办法》《数安条例》《数据分类分级规则》所述“重要数据”，公司非重要数据处理者。

六、 公司不涉及作为个人信息处理者处理人类遗传资源信息

根据《人遗条例》和《生物安全法》，人类遗传资源包括材料和信息两大类：材料指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料；信息指利用人类遗传资源材料产生的数据等信息资料。《人遗条例实施细则》进一步明确了人类遗传资源信息的范围，从正反两面以列举的方式明确：包括利用人类遗传资源材料产生的人类基因、基因组数据等信息资料，不包括临床数据、影像数据、蛋白质数据和代谢数据。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

根据《人遗条例》《人遗条例实施细则》，为取得相关药品和医疗器械在我国上市许可，在临床医疗卫生机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的，不需要批准，但应当在开展临床试验前将拟使用的人类遗传资源种类、数量及其用途向科技部备案。为取得相关药品和医疗器械在我国上市许可的临床试验涉及的探索性研究部分，应当申请人类遗传资源国际科学研究合作行政许可。国际科学研究合作行政许可、国际合作临床试验备案应当由中方单位和外方单位共同申请，申请应由临床试验申办方或医疗机构（组长单位）进行。

根据公司提供的说明，部分客户的临床试验项目涉及利用我国人类遗传资源信息，需要履行国际科学研究合作行政许可或国际合作临床试验备案程序，对于此类项目公司已作为共同申请方配合客户履行前述程序，但公司作为临床试验项目的软件和数字服务提供商，对客户处理的人类遗传资源信息无自主处理权限，仅在客户委托范围内按照客户的指示进行数据处理活动。

法律意见：综上，本所律师认为公司不涉及作为个人信息处理者处理人类遗传资源信息，并且已按照《人遗条例》《人遗条例实施细则》的要求配合相关客户履行临床试验项目的行政许可或备案程序。

七、 公司无需申请网络安全审查

（一） 公司业务涉及的个人信息处理规模未达 100 万人且未开展赴国外上市活动

根据《网安审查办法》第七条，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。截至 2024 年 3 月 31 日，根据公司统计，在尚未进行严格去重计算的情况下，公司作为个人信息处理者处理的个人信息主体数量未达 100 万人。而且，公司递交上市申请的证券交易所为位于香港的联交所，不属于赴国外上市情形。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

法律意见：综上，公司不涉及《网安审查办法》第七条规定的需申报网络安全审查情形。

（二） 公司非关键信息基础设施运营者且个人信息处理活动不会影响或者可能影响国家安全

根据《网络安全审查办法》第二条，关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当进行网络安全审查。

1. 公司非关键信息基础设施运营者

根据《关基条例》第二条、第八条、第十条的有关规定，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。其认定机制为由涉及的重要行业和领域的主管部门、监督管理部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，并负责及时将认定结果通知运营者。

根据公司出具的《承诺函》：公司业务并不涉及运营关键信息基础设施；公司未曾被行业主管部门、监督管理部门通知被认定为关键信息基础设施运营者。

2. 公司个人信息处理活动不会影响或者可能影响国家安全

如本法律意见书第五部分所述，公司业务不涉及处理重要数据。

3. 法律意见

综合上述，本所律师认为，公司非关键信息基础设施运营者，且数据处理类别及数据处理活动不会影响或者可能影响国家安全，不属于《网安审查办法》第二条规定的需申报网络安全审查情形。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

此外，本所律师就公司是否需申报网络安全审查问题专门致电中国网络安全审查认证和市场监管大数据中心，答复意见为无需申报。

八、 公司无需申报数据出境安全评估

（一） 个人信息出境情况

根据《个保法》第三十八条、第三十九条之规定，个人信息处理者向中国境外提供个人信息的，应告知个人并获取单独同意。同时还应当具备下列条件之一：通过国家网信部门组织的安全评估；按照国家网信部门的规定经专业机构进行个人信息保护认证；按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；法律、行政法规或者国家网信部门规定的其他条件。个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到《个保法》规定的个人信息保护标准。

根据《数据跨境规定》，关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 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，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。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 1 万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

公司本次上市筹备中涉及到向位于香港的境外中介机构、联交所提供个人信息和敏感个人信息，但仅限于公司申请上市必需的目的，且仅限于高级管理人员等部分人员，数量极少，公司已通过《个人信息出境授权同意书》获得了前述人员对于其个人信息出境的单独同意。同时，公司已针对此个人信息出境场景进行个人信息保护影响评估，评估从个人信息出境活动的目的、方式、对个人权益的影响及安全风险，以及所采取的保护措施是否合法、有效、与风险程度的适应性等维度展开，评估结论为本次上市筹备涉及的个人信息出境活动风险较低，可以实施。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

综上，本所律师认为：公司不符合《数据跨境规定》规定的需申报数据出境安全评估情形，无需申报数据出境安全评估。由于个人信息出境数量极少，且公司已完成个人信息保护影响评估程序、取得了个人信息主体单独同意，并已采取措施保障出境个人信息的安全，个人信息出境行为不会造成个人信息主体权益的明显损害。因此，公司的数据出境活动对本次上市不构成重大法律障碍。

九、 人工智能技术的应用

根据《暂行办法》，生成式人工智能技术是指具有文本、图片、音频、视频等内容生成能力的模型及相关技术，同时，企业等组织研发、应用生成式人工智能技术，未向境内公众提供生成式人工智能服务的，不适用《暂行办法》的规定。根据公司提供的说明，公司集成的开源大语言模型主要是用来执行序列标注，文本分类等文本预处理任务的“预训练基础模型”（PFM，Pretrained Foundation Model），预处理生成的结果并没有应用在面向客户的商业化产品或服务中，而是用来研发公司的算法技术。

综上，《暂行办法》并没有定义“应用”的具体所指，本所律师认为仅用于公司内部的非商业化使用开源大模型并非《暂行办法》所规定的“应用”，且公司未向境内公众提供生成式人工智能服务，因此公司不适用《暂行办法》。

十、 《数安条例》对公司业务运营及本次上市的影响

《数安条例》根据《个保法》《数安法》等上位法制定，在数据处理活动、数据安全管理等方面作出了更为细化的规定。

假设《数安条例》以目前的形式实施，本所律师认为公司可以在所有重大方面遵守《数安条例》的规定，不会对公司的业务运营或本次上市产生重大不利影响。

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

十一、 关于违法违规事项

根据公司访谈确认，并结合公司书面承诺，公司在个人信息和重要数据处理方面未受到中国监管部门的通报或查处，未收到个人信息主体的投诉、举报。本所律师进行了网络公开查询，未核查到公司发生个人信息和重要数据处理方面的违法违规事项。

十二、 结论性意见

本所律师认为公司的个人信息和重要数据处理在所有重大方面符合中国相关现行法律法规的要求，未发现明显违法违规事项，不会对本次上市构成重大法律障碍。

（以下无正文）

北京市朝阳区建国路 77 号华贸中心 3 号写字楼 34 层 邮编：100025
34/F, Tower 3, China Central Place, 77 Jianguo Road, Beijing 100025, China
T: (86-10) 5809 1000 F: (86-10) 5809 1100

（此页无正文，为《浙江太美医疗科技股份有限公司香港上市项目中国法项下个人信息和重要数据处理合规事项的法律意见书》之签署页）

北京市竞天公诚律师事务所

北京市竞天公诚律师事务所

2024 年 9 月 27 日