索引号	3212000007/2025-336976	分类	部门文件 市场监管 通知
发布机构	市市场监督管理局	发文日期	2025-08-25
文号	泰市监发[202541号]	时效	

泰州市市场监督管理局关于印发《泰州市生物医药企业商业秘密保护指南》的通知

信息来源：市市场监管局 发布日期：2025-08-27 10:38 浏览次数：188

各市（区）市场监管局、各有关单位：

《泰州市生物医药企业商业秘密保护指南》已由泰州市知识产权保护中心编撰完成，现印发你们，请结合工作实际，加强企业宣传引导，积极帮助企业完善商业秘密保护制度。

泰州市市场监督管理局

2025年8月25日

泰州市生物医药企业商业秘密保护指南

1.商业秘密管理体系

1.1 组织架构

1.1.1 商业秘密保护部门架构。生物医药企业可搭建决策层、管理部门及业务部门三级管控体系，强化商业秘密保护力度。

决策层负责确定商业秘密保护的战略方向与重大决策，为保护工作提供顶层规划。

管理部门承担具体管理职责，负责制定和执行保护制度，监督各部门执行情况。

业务部门在日常工作中落实保护措施，保障本部门涉及的商业秘密安全。

1.1.2 商业秘密保护内控内审。企业应明确各部门的商业秘密保护职责，划分保护部门与其他部门的分工及责任边界。各部门间需建立常态化沟通协作机制。

研发部门掌握企业核心技术与创新成果，法务部门具备专业法律知识与风险防控能力。两者需紧密协作，在研发过程中及时识别商业秘密，制定保护策略，确保成果有效保护；遭遇侵权纠纷时，法务部门能快速介入提供专业支持。同时配备专职商业秘密保护专员，明确岗位职责，负责日常管理与监督工作。

1.2 商业秘密的识别

1.2.1 依据《中华人民共和国反不正当竞争法》第九条规定，商业秘密是指不为公众所知悉、具有商业价值且经权利人采取保密措施的技术信息、经营信息等商业信息。商业秘密分为经营信息、技术信息、其他商业信息。

1.2.1.1 涉密技术信息是指涉及科学技术领域的结构、原料、组分、配方、材料、样式、工艺、方法或步骤、算法、数据、计算机程序及相关文档等信息。

1.2.1.2 涉密经营信息是指与经营活动相关的创意、管理、营销、财务、计划、样本、招投标材料、数据、客户信息等，以及对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息整理加工后形成的客户资料。其中“客户信息”是指除客户名称、地址、联系方式外，与之交易的意向合同内容、谈判进度、履行准备，以及通过特定客户保持长期稳定交易关系或通过付出一定的劳动、金钱和努力客户自有的交易习惯、独特需求、交易周期、价格数量、利润空间等特定信息。

1.2.1.3 其他商业信息是指符合商业秘密“不为公众所知悉、具有商业价值，并经权利人采取相应保密措施”的构成要件，除技术信息、经营信息以外的商业信息。

1.2.2 商业信息需具备秘密性、价值性、保密性三大特性方可被认定为商业秘密。秘密性指在被诉侵权行为发生时，该信息未被所属领域相关人员普遍知晓且不易获取；价值性指具有现实或潜在商业价值，能为权利人带来商业利益或竞争优势；保密性指权利人已对相关信息采取必要保密措施。

1.2.2.1 “不为公众所知悉”是指权利人请求保护的信息在侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得。

（1）将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合不为公众所知悉标准与条件的，应当认定该新信息不为公众所知悉。

（2）专利审查员、药品审查机构人员等政府职能部门工作人员在履行专利、药品等审批而知悉商业秘密的，不视为丧失秘密性。

1.2.2.2 “具有商业价值”是指权利人请求保护的信息包括生产经营活动中形成的阶段性成果，因不为公众所知悉而具有现实或者潜在的商业价值，形成市场竞争优势。

1.2.2.3 “保密措施”是指权利人根据商业秘密及其载体的性质、存在形态、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，采取的具有有效性、可识别性、适当性的防止商业秘密泄露的措施。

（1）签订保密协议或者在合同中约定保密义务的；

（2）通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；

（3）对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；

（4）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；

（5）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；

（6）要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；

（7）采取其他合理保密措施的。

1.2.2.4 不属于商业秘密的商业信息：

（1）在所属领域属于一般常识或者行业惯例的信息；

（2）涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的信息；

（3）该信息已经在公开出版物或者其他媒体上公开披露的信息；

（4）该信息已通过公开的报告会、展览等方式公开的信息；

（5）所属领域的相关人员从其他公开渠道可以获得的信息。

1.2.3 结合生物医药行业特性，其商业秘密具有高度技术性、复杂性与时效性，涉及巨额投资与长期研发成果，贯穿产品从概念到上市的全生命周期。准确识别和保护这些商业秘密，对企业长期发展与市场竞争力至关重要。

1.2.4 商业秘密保护部门应评估识别商业秘密信息，建立清单，明确信息内容、级别、保存期限、涉密人员范围、商业秘密信息流传方式。

1.3 信息分级管理

为提升保护效能，企业可建立核心级、重要级、普通级三级分类规范。

1.3.1 核心商业秘密对企业生存发展起决定性作用，如中药独特炮制工艺、中药秘方、处方、化学药关键分子结构等，可采用物理隔绝、双人双锁等严格保护方式；

1.3.2 重要商业秘密关系企业核心利益与竞争优势，如临床研究数据、客户信息等，可实施加密存储、权限管控；

1.3.3 普通商业秘密对企业运营有一定影响，但泄露风险较低，如常规项目计划、内部流程文档等，可通过基础保密协议保护。

1.4 人员全周期管理

1.4.1 人员全周期管理是商业秘密保护的关键环节，建议覆盖招聘背景调查、竞业限制协议、离职审计全流程。招聘环节中，对关键岗位人员开展充分背景调查，包括学历真实性核查、职业经历验证等，确保其具备良好职业道德与保密意识。与入职员工签订保密协议，明确保密范围与责任，实现入职即保密。

1.4.2 针对核心涉密人员，建议签订竞业禁止协议，限制其离职后一定期限内从事与本企业竞争的业务。离职环节需进行严格审计，强制清退涉密载体，注销系统访问权限，防止员工离职时带走商业秘密。

设置脱密期是人员管理的重要举措。脱密期内，员工需遵守保密协议，不得对外泄露企业商业秘密。

1.4.3 此外，企业可运用指纹识别、人脸识别等生物识别技术手段，强化涉密区域与设备的访问控制，提升商业秘密保护安全性。

1.4.4 中药传承人作为企业特殊人才，需采取特殊管理措施。与其签订专门保密协议，明确对中药秘方、炮制工艺等商业秘密的保护责任；同时提供良好工作环境与待遇，激励其积极传承创新中医药技术。

2.核心业务环节保护

新药从研发到上市需经历研发、生产、经营等多个阶段，每个阶段都有独特的商业秘密保护需求。

2.1 研发环节保护

研发环节是生物医药企业商业秘密的关键产生阶段，分项目立项、临床试验、申报审批三阶段。

2.1.1 立项阶段。企业可组建专业评估团队，对研发项目的商业秘密价值进行评估，确定保密级别。与 CRO 机构、高校等外部合作机构合作时，签订详细保密协议，明确双方权利义务。针对化合物筛选数据，采用云端存储加密技术方案，通过先进加密算法对数据加密处理，保障存储传输安全；同时设置严格访问权限，仅授权人员可访问相关数据。

2.1.2 临床阶段。加强临床试验方案及结果保护，对临床试验的人员、内部及外部CRO人员开展保密培训并签订保密承诺书。实验室管理中应用指纹识别、人脸识别等门禁生物识别技术，限制非授权人员进入；定期检查维护实验室设备与数据，确保数据完整安全。

2.1.3 报批阶段。严格审查申报文件内容，避免泄露商业秘密；与监管部门沟通时采取加密文件传输等保密措施。对中医药秘方进行数字化存证，利用区块链技术加密存储相关信息，确保不可篡改与可追溯；同时建立备份机制，防止数据丢失。

2.2 生产环节保护

生产环节是商业秘密保护的重要领域，建议企业建立车间物理隔离与参数实时监控双重机制。

2.2.1 车间物理隔离。设置门禁系统，限制人员车辆进出；核心生产区域如原料药车间、中药饮片加工车间等，采用人脸识别门禁、监控摄像头等设备全方位监控；定期维护检查生产设备，保障设备安全。

2.2.2 参数监控。建立生产参数监控系统，实时监测生产过程各项参数；对关键参数加密存储传输，防止数据泄露；设置预警机制，及时处理参数异常。

2.2.3 原料药生产。严格控制原材料采购渠道，防止信息泄露；对生产过程中的化学反应参数严格保密，避免竞争对手模仿生产工艺。

2.2.4 中药饮片加工。保护中药炮制工艺，防止工艺泄露；对道地药材来源与种植技术保密，保障药材质量与独特性。

2.2.5 废料处理。制定严格废弃物料处置规程，分类处理废料；对含商业秘密信息的废料进行粉碎、销毁等处理，防止信息泄露。

2.2.6 代工厂审计。定期审计代工厂，检查保密措施执行情况；与其签订保密协议，明确保密责任；对代工厂员工开展保密培训，增强保密意识。

2.3 市场经营保护

市场经营环节涉及客户信息与市场策略等商业秘密，企业可设计客户信息虚拟号段外呼管理系统与营销方案分级查阅制度。

2.3.1 客户信息虚拟号段外呼系统。通过虚拟号段与客户沟通，避免直接暴露真实电话号码；数据采集过程中获得客户授权，确保合法性；加强系统安全防护，防止遭攻击导致数据泄露。

2.3.2 营销方案分级查阅制度。将营销方案分为绝密级、机密级、内部级：绝密级涉及企业战略级营销规划、未公开重大市场行动等，仅限核心决策层查阅；机密级包括区域性/产品线营销计划、重要客户开发策略等，供部门负责人及以上级别访问，禁止非授权复制；内部级如常规营销执行方案、已公开活动详细计划等，相关岗位员工可查阅，基础数据禁止转发无关人员。

2.3.3 招投标文件动态水印技术。在招投标文件中添加含使用人、使用时间等信息的动态水印，文件被非法传播时可追踪泄露源。

2.3.4 学术会议信息披露红线。明确学术会议信息披露范围与标准，禁止披露化合物分子结构、中药秘方等核心商业秘密；发布会议报告和论文时严格审核，确保不含商业秘密信息。

3.差异化企业保护

3.1 小微企业防护

小微企业商业秘密保护资源有限，需管理的商业秘密数量较少，保护核心思路应立足可用性，聚焦保密协议签订与访问权限管控。

3.1.1 保护措施建议

3.1.1.1 签订保密协议。与可能接触商业秘密的员工签订全面保密协议，明确保密范围、违约责任等，增强员工保密意识。将安全意识培训纳入新员工试用期转正与周期性工作考核，实现全员覆盖。

3.1.1.2 实施访问控制。设置简单有效的权限管理机制，限制员工对敏感信息的访问；确保员工使用独立账号而非共用账号，启用登录日志与行为日志功能。

3.1.1.3 加强云备份。对关键数据实时备份，其他数据每日备份；确保办公计算机杀毒软件有效启用并及时更新，有效应对勒索病毒威胁，保障客户信息等商业秘密实时可用。采购专业云计算服务供应商产品，获取成熟的备份、访问控制等管理方案，避免因员工离职未有效交接导致客户流失。

3.1.2 主要风险点及检查措施

小微企业商业秘密保护的主要风险点包括：未签订保密协议、安全意识培训不足、备份策略不完善、杀毒软件未完全部署或未启用、系统账号共享等。

针对上述风险点，可采取以下检查措施：

3.1.2.1 确保新入职员工签署保密协议，重点核查关键岗位人员是否签订有效保密条款。

3.1.2.2 定期组织安全意识培训，留存培训材料与签到表；不定期抽检关键岗位人员进行安全意识考核。

3.1.2.3 定期检查备份机制运行状况，包括审阅备份日志、抽样检查备份文件完整性与可读性、不定期执行备份文件恢复测试。集中部署防病毒软件，通过服务端定期查看设备部署情况，检查安装情况及即时防护、定期扫描设置。

3.1.2.4 定期核查系统账号权限，与员工名单匹配，确保账号数量及所有者与员工一致，严格执行 “一人一账号”；重点检查已离职员工账号是否删除或禁用。

3.2 中型企业防护

中型企业需管理的商业秘密数量较多，涉及员工范围广，需设立独立部门负责保护工作。保护核心思路为全面风险识别与重点风险管控相结合。

3.2.1 保护措施建议

3.2.1.1 信息安全管理体系建设。按《中华人民共和国网络安全法》要求开展网络安全信息等级评估，或通过国际认可的 ISO27001 认证、行业特有的 PCI-DSS 支付卡安全认证等；借助第三方测评机构对照体系建设要求查找差距，通过技术与管理手段重点防护。

3.2.1.2 关键岗位背景调查。对数据库管理员、研发人员等接触大量商业秘密的岗位，入职前开展背景调查，防止不法分子以合法身份入职盗取信息。

3.2.1.3 网络隔离。对涉及大量商业秘密的信息系统实施网络隔离，避免直接连接互联网，如部署网络层防火墙。部署网络准入系统，限定有效账号方可接入企业网络，筑牢办公网第一道防线。

3.2.1.4 统一账号管理。建议建立微软 AD 域等统一账号管理系统，将所有登录系统纳入管理，有效管控员工账号。对涉及大量商业秘密的信息系统启用双因子鉴别，如手机短信验证码、动态数字口令等，防止关键岗位员工账号被盗导致商业秘密被第三方窃取。同时避免离职后账号关闭不及时不全面导致的商业秘密持续泄漏风险。

3.2.1.5 数据防泄密系统。对涉及大量商业秘密的信息系统启用加强版访问控制，通过在办公计算机部署管理终端、办公网出口部署网络探针，识别拦截含商业秘密的敏感数据外发行为，减轻内部员工有意或无意外传导致的第三方窃取风险。

3.2.2 主要风险点及检查措施

中型企业商业秘密保护的主要风险点包括：信息安全管理体系不完善、关键岗位候选人背景调查缺失、网络隔离策略未生效、统一账号管理不完善、数据库异常访问、敏感数据泄露等。

除采用小微企业检查措施外，还可采取以下措施：

3.2.2.1 参与第三方机构对信息安全管理体系的认证审核或复核，及时掌握体系建设情况。

3.2.2.2 定期复核关键岗位新入职员工背景调查情况，确保调查执行到位。

3.2.2.3 留存防火墙配置书面策略，调整策略需有正式书面申请与审批；定期审计生产环境防火墙配置，检查与书面策略一致性及内外网隔离有效性。

3.2.2.4 定期从服务端检查终端准入软件登录情况，与员工 / 资产清单匹配，核查是否有未认证设备入网；不定期用非公司设备测试接入，确认终端准入限制有效性。

3.2.2.5 定期检查数据防泄漏软件安装情况，与员工名单匹配确保部署完整；定期审计拦截和警告日志，及时发现员工数据传输异常操作并追因溯源。

3.3 大型企业防范

大型企业需管理海量商业秘密，商业秘密识别与保护存在盲区。保护核心思路为全面风险管控。

3.3.1 保护措施建议

3.3.1.1 组织保障。建议设立独立部门统筹商业秘密保护工作，牵头负责识别、保护、审计等职责。

3.3.1.2 数据分类分级。依据国家和行业要求建立数据分类分级体系，对含商业秘密的数据全面识别分类，以此为基础实施分级保护。

3.3.1.3 数据不落地。对含商业秘密的敏感场景启用云终端等模式，在保障员工使用的前提下，实现商业秘密仅可查看不可下载，无有效审批无法批量导出，防范内外部窃取行为。

3.3.1.4 数字水印。在关键应用系统启用明水印等数字水印技术警示规范员工操作，禁止截屏拍照；或使用暗水印，在商业秘密流失后追溯来源。

3.3.1.5 代理技术。采用代理模式以虚拟号统一外呼，防止客服人员恶意获取注册用户手机等联系方式，保护客户信息。

3.3.1.6 最小授权。通过统一身份验证+安全网关+微隔离模式，授予员工工作必需的最小权限，降低内部员工恶意嗅探窃取风险，提高第三方窃取难度。

3.3.2 主要风险点及检查措施

除中型企业风险外，大型企业还存在数据分类分级体系缺失、未经授权数据落地、数字识别技术缺失、员工账号权限过大等风险。

除采用小微企业和中型企业检查措施外，可增加以下措施：

3.3.2.1 定期检查数据分类分级体系是否随业务变化及时更新，各分类数据是否明确指定所有者。

3.3.2.2 通过 VDI 等虚拟桌面工具限制数据落地访问；定期审查 VDI 操作日志，确保无异常数据交互行为。

3.3.2.3 定期随机选取关键系统进行截屏操作，验证数字水印技术启用效果。

3.3.2.4 定期抽样检查关键系统，查看用户个人数据等敏感信息是否已脱敏处理。

3.3.2.5 依据员工岗位职能制定系统权限标准角色，形成书面岗位角色矩阵表；随业务变化及时更新矩阵表；岗位新增权限需有书面审批记录；定期检查系统账号权限，确保与工作岗位一致，额外权限均有正式申请审批，严格遵循最小授权原则。

3.3.2.6 强化跨国研发中心安全网关配置。采用先进防火墙技术、入侵检测系统等防护网络；设置严格访问控制策略，仅允许授权人员设备访问；对数据传输加密处理，保障跨国传输安全。

3.3.2.7 关注中药生产基地信息监测。中药生产基地涉及种植、加工等环节，存在商业秘密泄露风险。安装监测设备实时监控周边空域，防止无人机等窃取商业秘密。

4.商业秘密行政保护

4.1 查处部门与管辖

4.1.1 查处部门

市场监管部门是侵犯商业秘密行为的查处主体。省市场监管部门负责指导协调本省商业秘密侵权行为的预防与查处工作，处理重大、跨区域侵权案件；各地市场监管部门负责本行政区域内的预防与查处工作。

4.1.2 管辖

侵犯商业秘密行为由违法活动实施地的县级以上市场监管部门管辖，违法活动实施地包括行为着手地、进行地、经过地、结果地。

4.2 投诉举报

4.2.1 权利人可通过以下渠道向市场监管部门投诉举报：

4.2.1.1 实名注册登录全国 12315 网络投诉举报平台（网址：www.12315.cn）举报；

4.2.1.2 拨打市场监管部门投诉举报热线 12315 或市民热线 12345 举报；

4.2.1.3 向辖区市场监管部门现场举报。

4.2.2 权利人请求查处涉嫌侵权行为时，需提供商业秘密具体内容、已采取的保密措施、被侵权事实等初步材料。合理表明商业秘密被侵犯的，可提供以下证据之一：

4.2.2.1 有证据证明涉嫌侵权人有获取商业秘密的渠道或机会，且其使用信息与该商业秘密实质相同；

4.2.2.2 有证据显示商业秘密已被涉嫌侵权人披露、使用或存在被披露、使用的风险；

4.2.2.3 其他能证明商业秘密被涉嫌侵权人侵犯的证据。

4.3 立案与调查

4.3.1 立案

市场监管部门可通过监督检查职权、投诉举报、其他部门移送、上级交办等途径发现涉嫌侵权线索，其中举报是实践中较常见的途径。

经核查，符合以下条件的违法线索应当立案：

4.3.1.1 有明确的违法嫌疑人；

4.3.1.2 有初步证据证明存在侵犯商业秘密行为；

4.3.1.3 属于本部门管辖范围；

4.3.1.4 在行政处罚法定期限内。

注：《中华人民共和国行政处罚法》第三十六条规定，违法行为在二年内未被发现的，不再给予行政处罚。涉及公民生命健康安全、金融安全且有危害后果的，上述期限延长至五年。法律另有规定的除外。前款规定的期限，从违法行为发生之日起计算；违法行为有连续或者继续状态的，从行为终了之日起计算。

4.3.2 案件调查

市场监管部门调查涉嫌侵权行为时，可采取现场检查、询问、查询复制资料、查封扣押财物、查询经营者银行账户等措施。

4.3.2.1 现场检查

执法人员进入涉嫌侵权经营者的经营场所检查，制作载明时间、地点、事件等内容的现场笔录。

4.3.2.2 查封和扣押

经权利人申请并提供初步证明，市场监管部门可对调查中发现的与涉嫌侵权行为相关的场所、设施或财物实施查封扣押。对涉案合同、票据、账簿、凭证等资料，执法人员通过信息化手段或影印、复印等方式可及时有效固定证据的，不实施查封扣押；涉及计算机存储信息的，可能需查封扣押相关服务器、主机、硬盘等存储设备。查封扣押后需及时通过复制、镜像、摄像、截屏、数据恢复等方式固定证据。

查封扣押需符合《中华人民共和国行政强制法》规定。

4.3.2.3 委托鉴定

权利人、涉嫌侵权人可委托有法定资质的鉴定机构，对权利人信息是否为公众所知悉、涉嫌侵权人使用信息与权利人信息是否实质相同等专门性问题进行鉴定。双方可就鉴定结论向市场监管部门提出意见并说明理由，由市场监管部门审查决定是否采纳。

4.4 行政处罚

市场监管部门对确需行政处罚的商业秘密侵权行为，根据情节轻重及具体情况作出处罚决定。

4.4.1 行为类型

4.4.1.1 侵犯商业秘密行为主要包括违法获取、违法披露、违法使用、合法获取违法使用、第三人侵权、教唆帮助类侵权等类型。

4.4.1.2 依据《中华人民共和国反不正当竞争法》第九条，经营者不得实施下列侵权行为：

（1）以盗窃、贿赂、欺诈、胁迫、电子侵入或其他不正当手段获取权利人商业秘密；

（2）披露、使用或允许他人使用以前款手段获取的权利人商业秘密；

（3）违反保密义务或权利人有关保守商业秘密的要求，披露、使用或允许他人使用其所掌握的商业秘密；

（4）教唆、引诱、帮助他人违反保密义务或权利人有关保守商业秘密的要求，获取、披露、使用或允许他人使用权利人商业秘密。

（5）经营者以外的其他自然人、法人和非法人组织实施前款行为的，视为侵犯商业秘密。

（6）第三人明知或应知商业秘密权利人的员工、前员工或其他单位、个人实施第（1）项行为，仍获取、披露、使用或允许他人使用该商业秘密的，视为侵犯商业秘密。

4.4.2 保密义务主体

保密义务主体是指根据法律规定或者合同约定负有保密义务的单位和个人。

（1）根据法律规定或者劳动合同负有保密义务的员工、前员工；

（2）根据交易合同约定或交易合同附随义务负有保密义务的交易相对人；

（3）其他有渠道或机会获取商业秘密的其他单位或个人。

4.4.2 违法行为认定

4.4.2.1权利人能证明涉嫌侵权人使用的信息与自己主张的商业秘密实质相同，且能证明涉嫌侵权人有获取该商业秘密的条件，而涉嫌侵权人无法提供或拒不提供其信息合法获得或使用的证据的，市场监管部门可依据相关证据认定存在侵权行为。

4.4.2.2 实质性相同的构成因素

（1）被诉侵权信息与商业秘密的异同程度；

（2）所属领域的相关人员在被诉侵权行为发生时是否容易想到被诉侵权信息与商业秘密的区别；

（3）被诉侵权信息与商业秘密的用途、使用方式、目的、效果等是否具有实质性差异；

（4）公有领域中与商业秘密相关信息的情况；

（5）需要考虑的其他因素。

4.4.3 行政责任

4.4.3.1 责令停止违法行为

根据当事人侵权行为具体情形，可责令其返还或销毁载有商业秘密的图纸、软件或其他载体，不得继续披露、使用或允许他人使用商业秘密。

当事人利用权利人商业秘密生产的未销售产品，应监督销毁，除非权利人同意收购或继续销售。

4.4.3.2 没收违法所得

依据《中华人民共和国反不正当竞争法》第二十六条规定，没收违法所得。

4.4.3.3 罚款

按照《中华人民共和国反不正当竞争法》第二十一条，对侵权行为处十万元以上一百万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款。

“情节严重”的认定按法律规定或有权解释，综合考虑侵犯商业秘密行为的手段、次数、性质、侵权行为的持续时间、地域范围、规模、后果，侵权人在诉讼中的行为等因素。

行为人有下列情形的，可以认定为情节严重：

（1）因侵犯商业秘密被行政处罚或者法院裁判其承担责任后，再次实施相同或者类似侵权行为；

（2）以侵权为业；

（3）伪造、毁坏或者隐匿侵权证据；

（4）拒不履行保全裁定；

（5）侵权获利或者权利人受损巨大；

（6）侵权行为可能危害国家安全、公共利益或者人身健康；

（7）其他可以认定为情节严重的情形。

4.4.4 民事责任

4.4.4.1 民事责任主要包括停止侵权即不得披露、使用或允许他人使用其接触或获取的商业秘密，赔偿损失，以及销毁或返还侵权载体等。

4.4.4.1 停止侵权应当持续到该商业秘密已为公众所知悉时为止，或者在依法保护权利人商业秘密竞争优势的情况下行为人在一定合理期限或者范围内停止侵权行为。

4.4.4.2 权利人请求判决侵权人返还或者销毁商业秘密载体，清除其控制的商业秘密信息的，一般应当予以准许。但销毁侵权载体会损害社会公共利益，或者销毁侵权载体不具有可执行性等情形的除外。

4.4.4.3 赔偿损失确定方法

（1）按照权利人因被侵权所受到的实际损失确定，实际损失难以计算的，按照行为人因侵权所获得的利益确定。

（2）根据研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素，确定商业价值损失。

（3）权利人实际损失额或者行为人侵权获利额难以确定，有商业秘密许可使用费参照的，可以参照该许可使用费的合理倍数确定赔偿数额。

（4）侵权人在审计报告、上市公司年报、招股说明书、财务账簿、会计凭证、销售合同、进出货单据、知识产权许可使用合同、设备系统存储的交易数据、公司网站、产品宣传册或其他媒体上公开的经营信息，以及第三方平台统计的商品流通数据，评估报告，市场监管、税务、金融部门的记录等，可以证明权利人损失赔偿数额。

4.4.4.4 根据商业秘密的性质、商业价值、研究开发成本、创新程度、能带来的竞争优势以及侵权人的主观过错、侵权行为的性质、情节、后果等因素判决给予权利人500万元以下的法定赔偿。

4.4.4.5 行为人故意侵犯商业秘密，情节严重的，可以在按照上述方法确定数额的1-5倍确定惩罚性赔偿数额。

确定惩罚性赔偿数额时，应当以权利人实际损失数额或者行为人因侵权所获得的利益作为基数。权利人的实际损失数额或者行为人因侵权所获得的利益均难以计算的，法院依法参照许可使用费的合理倍数确定计算基数。该基数不包括权利人为制止侵权所支付的合理开支。

确定惩罚性赔偿数额的倍数时，应当综合考虑行为人主观过错程度、侵权行为的情节严重程度等因素。因同一侵权行为已经被处以行政罚款或者刑事罚金且执行完毕，在确定倍数时可以降低。

4.4.4.6 权利人主张为制止侵权行为所支付的合理开支的，可以在确定的赔偿额之外要求行为人承担。合理开支一般包括以下费用：

（1）公证费；

（2）因调查取证或出庭而发生的交通费、食宿费、误工费等；

（3）档案查询费、材料印制费；

（4）翻译费；

（5）律师代理费；

（6）权利人为制止侵权行为支付的其他合理费用。

4.4.5 移送追究刑事责任

当事人涉嫌构成犯罪的，市场监管部门应移送公安机关追究刑事责任。经公安机关侦查、检察院公诉、法院判决构成侵犯商业秘密罪并判处罚金的，市场监管部门已给予的罚款应折抵相应罚金。

4.4.6 列入严重违法失信名单

根据《市场监督管理严重违法失信名单管理办法》，对侵犯商业秘密这类严重破坏公平竞争秩序的不正当竞争行为，当事人违反法律、行政法规，性质恶劣、情节严重、社会危害较大，受到市场监督管理部门较重行政处罚的，由市场监督管理部门依照本办法规定列入严重违法失信名单，通过国家企业信用信息公示系统公示，并实施相应管理措施。

市场监管部门收到法院生效法律文书要求对相关经营者、人员实施严重违法失信名单管理的，参照该办法执行。

4.5 调解与和解

发现商业秘密侵权行为后，权利人和当事人可在双方自愿的基础上自行和解。认定侵犯商业秘密的，市场监督管理部门在行政处罚的同时，可以应当事人的请求，就侵犯商业秘密的赔偿数额进行调解。和解不影响案件是否构成侵犯商业秘密的定性，但可作为处罚裁量的因素加以考虑。

4.6 监管合作

生物医药企业建议与行业监管部门建立长期良好的沟通渠道，可通过定期参加行业研讨会、主动提交行业报告等方式实现。企业可及时反馈行业商业秘密保护问题，如新型侵权手段、跨境技术转移风险等；同时提出完善政策措施的建议，如加强生物样本管理监管、完善临床试验数据保护机制等。通过积极监管合作，企业可提升合规水平，推动改善行业保护环境，在纠纷发生时获得更有效的行政支持。

5.商业秘密涉外保护

中国生物医药企业在海外经营或国际贸易中需高度关注商业秘密纠纷风险，了解各国保护环境，落实保护措施，做好风险防控与维权策略制定。

5.1 熟悉各国法律规范

对于计划走出国门的中国企业，即便主要生产经营在国内，只要有开拓海外市场的初步规划，就应将海外涉诉风险纳入考量，主动学习了解目标国家法律，明确哪些信息可能构成受保护的商业秘密，以及如何合规处理这些信息。

5.2 开展自查评估工作

若中国企业在国外法院被指控侵犯商业秘密，应首先明确涉及信息是否符合商业秘密法定条件。能证明以下事实将有助于应对：

5.2.1 不具有秘密性。若涉及信息在被指控行为发生时已为公众所知，如可在互联网、学术期刊公开检索到，则不构成商业秘密。企业也可尝试证明对方未对信息采取保密措施或信息无商业价值。

5.2.2 有合法来源。若能证明信息通过合法途径取得，如从第三方善意获取、自行研发或反向工程获得，则可证明无侵权行为。

5.3 跨境信息传输管控

全球研发生产网络中，跨境信息传输不可避免。企业应建立严格的跨境信息传输管理制度，包括加密传输、访问控制、数据本地化存储等措施。对新药配方、关键生产工艺等高度敏感信息，可采用分散存储策略，避免关键信息集中存储。

5.4 知识产权战略协同

在不同国家和地区采取协调一致的知识产权保护策略，包括在关键市场同步申请专利、商标等知识产权保护。对无法通过专利保护的商业秘密，如特定生产工艺或配方，在全球范围采取统一保密措施。同时密切关注各国知识产权法律变化，及时调整保护策略。

5.5 委任专业律师团队

企业应成立由法务部门、业务部门及相关部门组成的内部专项小组，同时聘请具备涉外应诉能力与经验的律师，配合律师开展应诉工作。律师受保密义务约束，企业无需过度担心商业秘密泄露，应如实告知律师所需事实。

5.6 谨慎开展招聘工作

招聘曾就职于外国企业的员工时需保持审慎，先确认其无竞业限制或其他约束，避免携带前公司商业秘密入职。

5.6.1 详尽背景调查

对招聘候选人开展详尽背景调查，核实履历真实性、离职原因、是否与原单位签订保密协议和竞业限制协议，以及是否有涉嫌窃取商业秘密等不当行为的调查或起诉记录。

5.6.2 关注竞争对手员工

从国内外竞争对手公司招聘可能持有保密信息的员工时，需更审慎评估排除风险。劳动协议中明确约定员工不得违反与第三方的保密协议，要求其承担前/现雇主要求的保密义务，不得向前/现雇主泄露商业秘密。

5.7 寻求外部支持力量

接到国外法院或执法机构应诉或配合调查通知后，企业可联系负有经济发展支持职责的行政机关或社会团体共同应对。我国商务部（贸易救济调查局）、地方商务部门、行会商会等可能提供必要支持。

上一篇：泰州市市场监督管理局办公室关于做好2025年度电梯维保单位星级评定工作的通知

下一篇：泰州市市场监督管理局办公室关于开展2025年度泰州市知识产权服务能力提升资助项目申报的通知