医药行业商业秘密保护规范

1 范围

本文件规定了医药行业商业秘密保护的术语和定义、总体要求、组织领导、商业秘密的管理、涉密事项的管理、应急准备与响应、检查与改进等内容。

本文件适用于医药行业商业秘密的保护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DB34/T 4317 商业秘密保护规范

DB34/T 4533 企业商业秘密管理体系 要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

商业秘密 trade secrets

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技术信息、经营信息等商业信息。

3.2

涉密载体 secret-related carriers

用于记载或存储商业秘密的各类介质，如纸质介质、存储介质（U盘、硬盘、光盘、服务器等）和其他介质。

3.3

涉密物品 secret-related items

含有商业秘密的设备、原材料、半成品和样品等。

3.4

涉密区域 secret-related area

产生和存储商业秘密的场所，包括但不限于企业园区、厂房、车间、实验室、办公室、保密室、档案室、机房、用户现场等。

1 总体要求

1.1 企业应坚持“企业自主、预防为先、依法维权”的商业秘密保护原则。

1.2 企业应建立商业秘密保护机制，建立商业秘密保护机构，配备专（兼）职保密人员。

1.3 企业应配备满足商业秘密保护所需的资源（如人员、设施、设备、财务等）。

1.4 企业应建立健全商业秘密保护管理制度，并按制度要求实施管理工作。

1.5 企业应组织开展商业秘密保护相关法律法规、制度等知识的学习培训，不断提高人员的保密意识和商业秘密的保护能力。

1.6 企业宜按照DB34/T 4533的要求，建立、实施并持续改进商业秘密管理体系，将商业秘密管理贯彻到企业的全部经营活动过程。

2 组织领导

2） 对企业生产经营的重要程度；
3） 企业的投入研发、经营以及其他成本；
4） 为企业带来竞争优势；
5） 竞争对手获取商业信息后产生的价值；
6） 因信息泄露后产生或可能产生的经济损失；
7） 因信息泄露后可能承担的法律责任。

3.2.2.3 领导小组在定密的同时，应根据商业秘密的重要性程度和商业价值高低，确定商业秘密的密级，一般划分为核心商业秘密、重要商业秘密、一般商业秘密和定向商业秘密。各密级划分标准如下：

a） 核心商业秘密是指公开或泄露后，会给权利人带来致命的、毁灭性的、长久性极大伤害或即时性持续重大伤害或极大经济损失的商业秘密。
b） 重要商业秘密是指公开或泄露后，会给权利人带来相对滞后的持续性重大伤害或短期性即时重大伤害或重大经济损失的商业秘密。
c） 一般商业秘密是指较难采取技术和物理防护措施，且公开或泄露后会给权利人带来相对滞后的持续性较大伤害或即时性一般伤害或一般经济损失的商业秘密。
d） 定向商业秘密是指无法采取技术和物理防护措施，且被竞争对手、同业人员或特定的利益相关者知悉后，给权利人带来伤害、经济损失、竞争威胁、潜在负面影响的商业秘密。

3.2.2.4 经论证确定的商业秘密及其相关文件，应由保密职能部门统一登记备案，并明确其密级、保密期限、知悉范围、保密事项、保护措施、存放地点及保存方式等内容。

3.2.2.5 企业宜通过公证、第三方存证、电子存证等证据保全方式实现对商业秘密权属的初步确认。

3.3 隐密

3.3.1 下列情形涉及商业秘密的，应由保密职能部门对相关信息予以隐藏：

a） 与供应商、客户、合作方等的沟通和信息往来中；
b） 信息公开、发布、流转时；
c） 协助其他单位尽职调查时；
d） 其他情形。

3.3.2 可采取的隐密方式包括但不限于：

a） 隐藏或删除涉密信息；
b） 对涉密信息进行模糊化处理；
c） 其他方式。

3.4 解密

3.4.1 满足下列要求之一的商业秘密，应由保密职能部门对其进行解密：

a） 企业认为商业秘密事项已不再具有保护价值的；
b） 保密期限届满；
c） 其它特定因素导致商业秘密被公开的。

3.4.2 可采取的解密方式包括但不限于：

a） 移出涉密区域；
b） 消除密级标识、提示；
c） 电子文档解密；
d） 其他方式。

3.5 销密

3.5.1 销毁涉及商业秘密的文件(含复制文件)、资料、电子信息、载体和物品，应列出销毁清单，经保密领导小组审批后，由保密职能部门实施。可采取的销毁方式包括但不限于：

a） 文件、资料应粉碎成颗粒状或焚烧处置；
b） 电子信息应利用彻底删除软件永久删除；
c） 涉密载体应做销毁处理；
d） 其他合适的方式。

3.5.2 可采取下列方式对销毁过程进行监督管理：

e） 涉密载体应保存在涉密区域的专用设备中，并由专人负责保管；涉密载体的维修，应指定专人全程现场监督；

f） 涉密载体的维修和销毁应履行审批和登记手续，按照规定的程序和方法，并在专人监督下进行。

应保留涉密载体管理的成文信息。

4.3 涉密物品管理

企业应对涉密物品进行保密管理：

a） 应制定涉密物品管理制度，明确涉密物品的识别和确定、生产和加工、使用、保存、维修和销毁等环节的管理要求；

b） 应识别和认定企业所有涉密物品，建立涉密物品台账，宜实行分级管理，并在醒目位置粘贴（悬挂）涉密指示标识和禁止行为的警示标识；应定期对涉密物品进行清点和核查，确定涉密物品的数量、位置、状况等信息；

c） 应在涉密区域内进行涉密物品的生产和加工，宜根据涉密物品生产和加工流程，安排不同的人员负责不同的环节；

d） 应在涉密区域内使用涉密物品，并履行使用登记程序；对外销售的涉密物品，应与客户签订保密协议或在销售合同中增加保密义务条款，宜采取足以对抗不特定第三人通过反向工程获取其技术秘密的保护措施；

e） 应在指定的涉密区域存放涉密物品，并指定专人负责管理；

f） 涉密物品的维修、报废应履行审批和登记手续，按照规定的程序和方法，并在保密人员监督下进行。

应保留涉密物品管理的成文信息。

4.4 涉密区域管理

企业应对涉密区域进行保密管理：

a） 应制定涉密区域管理制度，明确涉密区域的识别和确定、安全防护、日常管理、检修和维护等环节的管理要求；

b） 应识别企业所有涉密区域，确定涉密区域的范围，并在醒目位置粘贴（悬挂）涉密区域指示标识和禁止行为的警示标识；宜根据区域内涉密物品、涉密信息及其载体的密级和性质，划分涉密区域的保密级别，实施分级管理；

c） 应对涉密区域进行物理隔离，并根据其保密级别，选择安装安全防范设施设备，配备专职安保人员和管理人员；

d） 涉密区域内部使用的通信、网络、计算机、信息系统、办公设备等应符合国家相关保密规定和技术标准的要求；

e） 应对涉密区域人员、物资进出实行登记管理，未经审批或授权严禁人员进入和物资离开；涉密区域如需接待外来人员，应指派保密人员全程陪同，并告知保密注意事项和要求；必要时，应进行安全检查，限制携带或使用具有录音、摄像、拍照、信息存储等功能的设备；

f） 应定期对涉密区域的设施设备进行检修和维护，并履行审批和登记手续，按照规定的程序和方法，并在保密人员监督下进行；必要时，应开展不定期巡查工作。

应保留涉密区域管理的成文信息。

4.5 涉密商务活动管理

企业应对涉密商务活动进行管理：

a） 应制定涉密商务活动管理制度，明确涉密商务活动中信息发布、涉密会议、商业活动、对外合作、产权交易等活动的管理要求；

b） 应对信息发布实施保密审查，明确人员职责权限，对新闻稿件、展览展会宣传资料、著作论文、申请专利等信息实施对外发布前审查、发布后检查，以及对涉密信息的追踪；

c） 应对涉密会议实施商业秘密管理，选择具有保密条件的场所，限定参会人员范围，签订保密协议或承诺书；涉密文件资料应有明显保密和会后回收标识，会后应及时收回、清点和登记。

d） 应对涉密的采购、销售、委托开发、委托生产、参展等商业活动实施商业秘密管理，开展相关方的保密能力评价，签订保密协议，定期或不定期对相关方进行保密监督检查；

6.2　商业秘密保护办公室负责定期组织对商业秘密保护情况进行检查，对发现的问题提出整改要求，并监督落实。

6.3　商业秘密泄露事件发生后，商业秘密保护领导小组应当组织对泄密事件进行专门评估，并根据评估结果对商业秘密保护体系进行改进。

6.4　企业应强化监督检查结果运用，建立完善商业秘密保护奖惩激励、应急处置等日常工作机制。