

泰格医药隐私政策总则

更新日期:

生效日期:

【引言】

泰格医药（以下简称“泰格”或“我们”）非常重视用户隐私，并深知个人信息对您的重要性，并承诺会按法律法规要求、参考业界成熟的安全标准，尽全力保护您的个人信息安全可控。鉴于此，我们特制定本《泰格医药隐私政策总则》（以下简称“本政策”），以便您详细了解我们将如何收集、使用、传输、保存和披露您的个人信息及您享有何种权利。

本政策适用于泰格医药系统平台和服务（以下简称“系统平台”，范围详见“定义”）。如某一系统平台有单独的隐私政策则该系统平台的隐私政策将优先适用。**该系统平台隐私在政策未涵盖的内容，以本政策内容为准，该系统平台隐私政策与本政策有冲突的内容，以系统平台隐私政策为准。**

我们深知个人信息对您的重要性，也深知为您的信息提供有效保护是公司健康、可持续发展的基石。您的信任对我们非常重要！我们致力于维持您对我们的信任，恪守法律和我们对我们的承诺，尽全力保证您的个人信息安全和合理使用。同时，**我们郑重承诺，我们将按业界成熟的安全标准，采取相应的安全保护措施来保护您的个人信息。**

在您使用泰格系统平台前，请您务必仔细阅读并透彻理解本政策，在确认充分理解并同意后使用相关系统平台。一旦您开始使用泰格系统平台服务，即表示您已充分理解并同意本政策。

【定义】

1. “泰格医药”，指杭州泰格医药科技股份有限公司及其全资和控股子公司。
2. “您”，指使用泰格系统平台及其服务的人员，包括但不限于泰格员工、与泰格合作的第三方人员等。
3. “泰格医药系统平台和服务”，指用于支持泰格医药日常工作和业务开展的各类系统和平台（包括但不限于泰格医药客户管理平台（BDS），临床试验管理系统（CTMS），临床协调管理系统（CCMS），培训管理系统（Training），泰格办公自动化系统（OA）等web端、程序、服务、工具及客户端）。
4. “个人信息”，指以电子或者其他方式记录的与已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。个人信息包括个人基本信息、个人身份信息、个人生物识别信息、网络身份标识信息、个人健康生理信息、个人财产信息、个人通信信息、个人常用设备信息、个人位置信息等。
5. “个人信息主体”，指个人信息所标识的自然人。
6. “敏感个人信息”，指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。
7. “去标识化”，指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。
8. “匿名化”，指通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的

信息不能被复原的过程。

【正文】

本政策将帮助您了解以下内容：

- 一、我们如何收集和使用您的个人信息
- 二、我们如何使用 Cookie 和同类技术
- 三、我们如何共享、转让、公开披露您的个人信息
- 四、我们如何保存及保护您的个人信息
- 五、您的权利
- 六、本政策的修订
- 七、如何联系我们

一、我们如何收集和使用您的个人信息

我们会基于如下的目的收集和使用您的个人信息：

目的	个人信息类别	详细说明
为注册系统平台账号、登录系统平台所需的个人信息处理活动	泰格集团邮箱、个人工作邮箱、私人邮箱、姓名、手机号、验证码、密码	用于验证登录人员的身份并进行实名认证，不提供上述信息您将无法使用泰格系统平台服务。
	头像、英文名	不提供上述信息不会影响您使用泰格系统平台服务。
	设备信息以及与登录环境相关的信息（包括国际移动设备身份码 IMEI、广告标识符 IDFA，集成电路卡识别码 ICCID、设备名称、设备型号、操作系统版本、WIFI 信息 BSSID、SSID、IP 地址信息）。	确保您的账户安全，进行风险控制和防御。
为提供系统平台服务所需的个人信息处理活动	您在使用泰格系统平台时主动提供、留存的信息。例如您主动发布、反馈、评论、上传的文字图片、音频视频等。	各系统平台在向您提供服务的过程中所需的个人信息有所差异，您可以通过点击下方各系统平台的隐私政策进行了解。
	您所使用的设备信息，可能包括您终端设备的设备属性信息（例如最终用户的硬件型号、操作系统版本，设备配置，国际移动设备身份码 IMEI、国际移动用户识别码 IMSI，网络设备硬件地址 MAC、广告标识符 IDFA、供应商标识符 IDFV，移动设备识别码 MEID，匿名设备标识符 OAID，集成电路卡识别码 ICCID，Android ID，硬件序列号等设备标识符）、设备连接信息（例如浏览器的类型、电信运营商、使用的语言、WIFI 信息）以及设备状态信息（例如设备应用安装列表、设备传感器信息）。	
	日志信息	您在使用系统平台服务过程中，我们会记录您使用的日志信息，包括登录时间，登录时长，点击、添加、编辑等操作记录。系统可能通过 cookies、网站信标方式自动采集的上述信息，用于我们进行数据统

		计。
改善我们的平台及服务	您的反馈意见、邮箱地址、姓名	当您向我们反馈意见，提供建议时，我们可能会收集您的姓名、邮箱地址。如拒绝提供信息，您将无法向我们进行反馈，但不影响您正常使用其他功能。
其他处理目的	我们可能出于提供不同的系统平台所需，为实现其他特定处理目的而开展个人信息处理活动，您可以通过点击下方具体系统产品的隐私政策进行了解。 客户管理平台（BDS）隐私政策 临床协调管理系统（CCMS）隐私政策 工时管理系统（Timesheet）	

二、我们如何使用 Cookie 和同类技术

2.1 Cookie

为确保网站正常运转、为您获得更轻松的访问体验、向您推荐与您相关的内容，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符，借助于 Cookie 网站能够记住您的选择，提供个性化增强服务等。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 [AboutCookies.org](#)。您可以清除计算机上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要每一次访问泰格系统平台时更改用户设置。如需详细了解如何更改浏览器设置，请访问您使用的浏览器的相关设置页面。

2.2 网站信标和像素标签

除 Cookie 外，我们还会在网站使用网站信标和像素标签等其他同类技术。例如，我们向您发送的电子邮件可能含有链接至我们网站内容的地址链接，如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品或服务偏好以便于我们主动改善客户服务体验，网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。

三、我们如何共享、转让、公开披露您的个人信息

1. 共享

我们会以高度的勤勉义务对待您的信息。除法律法规明确规定的其他情形外，未经您单独同意，我们不会向除泰格医药外的任何公司、组织和个人共享您的信息。

除此之外，我们可能会委托授权合作伙伴为您提供某些服务或代表我们履行职能，包括为我们的服务提供基础设施技术服务、短信服务、数据处理服务。我们仅会出于本政策声明的合法、正当、必要、特定、明确的目的共享您的信息，授权合作伙伴只能接触到其履行职能所需信息，且不得将此信息用于其他任何目的。

基于不同系统平台的服务略有差异，你看可以详细参阅每一系统平台的隐私政策了解我们会与哪些授权合作伙伴共享您的个人信息。

2. 转让

我们不会将您的信息转让给任何公司、组织和个人，但以下情况除外：

- (1) 获得您的明确同意；

- (2) 满足法律法规、法律程序的要求或强制性的政府要求或司法裁定；
- (3) 在涉及合并、收购或破产清算时，如涉及到信息转让，我们会要求新的持有您的信息的公司、组织继续受本政策的约束，否则我们将要求该公司、组织重新向您征求授权同意。

3. 公开披露

我们仅会在以下情形下，公开披露您的个人信息：

- (1) 获得您的单独同意；
- (2) 基于法律法规、法律程序、诉讼或政府主管部门强制性要求下。

4. 共享、转让、公开披露个人信息时事先征得授权同意的例外

在以下情形中，我们共享、转让、公开披露您的个人信息无需征得您的授权同意：

- (1) 为履行法定职责或者法定义务所必需（例如国家安全、国防安全、刑事侦查、起诉、审判和判决执行等直接相关的法定义务）；
- (2) 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；
- (3) 在合理的范围内处理您自行公开或者其他已经合法公开的您个人信息（如合法的新闻报道、政府信息公开渠道）；
- (4) 根据个人信息主体要求签订和履行合同所必需的；
- (5) 为公共利益实施新闻报道、舆论监督等行为，在合理范围内处理个人信息；
- (6) 法律法规及国家标准规定的其他情形。

根据法律规定，共享、转让经匿名化处理的个人信息，且确保数据接收方无法复原并重新识别个人信息主体的，不属于个人信息的对外共享、转让及公开披露行为，对此类数据的保存及处理将无需另行向您通知并征得您的同意。

四、我们如何保存及保护您的个人信息

1. 保存期限

您在使用泰格系统平台服务期间，我们将持续为您保存您的信息。**若您与泰格终止合作或解除劳动合同关系，基于公司员工管理的需要或日后可能发生的诉讼、法律程序或政府主管部门的强制性要求，我们将继续保存您的个人信息，除了法律法规或强制性规定需要立即删除您的个人信息。**

2. 保存地域

您的个人信息一般储存于中华人民共和国境内。如涉及到跨境传输的，我们会严格按照法律法规的规定执行，并保证您的个人信息安全。

3. 安全措施

- (1) 泰格医药非常重视您的信息安全。我们努力采取各种合理的物理、电子和管理方面的安全措施来保护您的用户信息。防止用户信息遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会使用加密技术提高用户信息的安全性；我们会使用受信赖的保护机制防止用户信息遭到恶意攻击；我们会部署访问控制机制，尽力确保只有授权人员才可访问用户信息；以及我们会举办安全和隐私保护培训课程，加强员工对于保护用户信息重要性的认识。
- (2) 在不幸发生用户信息安全事件（泄露、丢失等）后，我们将按照法律法规的要求，

及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知用户信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，上报用户信息安全事件的处置情况。

- (3) 互联网环境并非绝对安全，我们将基于正常的商业努力尽力确保您发送给我们的任何信息的安全性。

五、您的权利

按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利：

1. 查阅和复制您的个人信息

您有权访问和复制您的个人信息，法律法规规定的例外情况除外。具体查阅和复制您个人信息的方式，您可以通过查阅各系统平台隐私政策进行知悉。

2. 更正或补充您的个人信息

您发现我们处理的关于您的个人信息有不准确或不完整时，您有权对不准确或不完整的信息作出更正或补充。您可以联系公司系统平台管理员进行更正或补充。

3. 删除您的个人信息

在以下情形中，您可以通过具体系统平台的管理员与我们联系，向我们提出删除个人信息的请求：

- (1) 若我们收集您的个人信息是基于您的同意，当您撤回同意时，您有权要求我们删除您的个人信息；
- (2) 我们违反法律、行政法规或者违反约定处理个人信息；
- (3) 法律、行政法规规定的其他情形。

4. 撤回同意

每个系统功能需要一些基本的个人信息才能得以完成，对于我们基于您的同意处理的个人信息，您可以随时给予或收回您的授权同意。您可以详细参阅各系统平台隐私政策进行了解。

5. 注销您的账号

您知悉并同意，基于您与泰格的特殊关系（劳动合同关系、业务合作关系），我们无法立即删除或注销您的账号，除非法律法规有另行规定。您可以通过联系各系统平台管理员了解详细信息。

六、本政策的修订

我们可能随时修订本政策或各系统平台隐私政策。如该等变更会导致您在本隐私政策项下权利的实质减损，我们将在变更生效前，通过在页面显著位置提示、向您发送电子邮件等方式通知您。我们会在本页面上发布对隐私政策所作的任何变更。

本隐私政策所指的重大变更包括但不限于：

- (1) 我们的系统平台服务发生重大变化，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) 个人信息共享、转让或公开披露的主要对象发生变化；

- (3) 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;
- (4) 其他可能对您的个人信息权益产生重大影响的变化时。

七、如何联系我们

如您对本隐私政策有任何意见或建议，[您可以直接联系系统管理员或通过DPO@tigermedgrp.com](mailto:DPO@tigermedgrp.com)联系我们。

工时管理系统隐私政策

更新日期：20231001

生效日期：20231001

感谢您使用泰格医药工时管理系统！

本《公司管理系统隐私政策》（以下简称“本政策”）在基于《泰格医药隐私政策总则》（以下简称“总则”）的基础上，详尽描述了您在使用泰格医药工时管理系统（Timesheet）的过程中我们如何收集、使用、传输、保存及披露您的个人信息。**本政策未提及的内容，以总则部分为准，若本政策与总则有冲突的内容，以本政策为准。**

本政策适用于泰格医药工时管理系统（Timesheet）（包括但不限于网页端、手机客户端）及服务、程序等。

在使用客户管理平台前，请您务必仔细阅读并透彻理解本政策，在确认充分理解并同意使用相关产品和服务。一旦您开始使用客户管理平台，即表示您已充分理解并同意本政策。

本政策将帮助您了解以下内容：

- 一、我们如何收集和使用您的个人信息
- 二、我们如何共享、转让、公开披露您的个人信息
- 三、我们如何保存及保护您的个人信息
- 四、您的权利
- 五、本政策的修订
- 六、如何联系我们

一、我们如何收集和使用您的个人信息

1) 基本个人信息

基本个人信息请详细参阅《泰格医药隐私政策总则》。

2) 额外个人信息（如适用）

除总则中提及的基本个人信息外，我们还会收集如下您的个人信息以为你更好的提供服务。

目的	个人信息类别	详细说明
/	/	/

2) 权限开启

您理解并同意，您在使用工时管理系统（Timesheet）的过程中可能需要您在您的设备中开启特定的访问权限，以实现这些权限所涉及个人信息的收集和使用：

权限名称	权限功能说明	使用场景或目的
摄像头	允许应用拍摄照片和录制视频	使用摄像头进行扫描、拍摄，用于实现名片信息收集、财务报销、上传/更换头像功能。
相册	允许应用读取相册中的照片和文件	如我们访问您的相册，是为了使您可以实现您设备中的照片、图片或视频的取用与上传，便于您实现名片上传、进行财务报销、上传/更换头像。
日历信息	允许应用设备系统的日历权限	用于提醒用户记录工时

当您需要关闭该功能时，大多数移动设备都会支持您的这项需求，具体方法请参考或联系您移动设备的服务商或生产商。请您注意，您开启任一权限即代表您授权我们可以收集和使用的个人信息来为您提供对应服务，您一旦关闭任一权限即代表您取消了授权，我们将不再基于对应权限继续收集和使用个人信息，也无法为您提供该权限所对应的服务。但是，您关闭权限的决定不会影响此前基于您的授权所进行的个人信息收集及使用。

二、我们如何共享、转让、公开披露您的个人信息

除在《总则》中提及我们如何共享、转让、公开披露您的个人信息外，基于特定系统软件服务，我们还会与如下第三方合作伙伴共享您的个人信息：

为了您能够使用我们的服务，我们的软件中会嵌入授权合作伙伴的 SDK 或其他类似的应用程序。我们会对授权合作伙伴获取的有关信息的应用程序接口（API）、软件工具开发包（SDK）进行严格的安全监测，并与授权合作伙伴约定严格的数据保护措施，令其按照我们的委托目的、服务说明及本政策来处理个人信息。

针对 BDS、CCMS 应用程序，我们讲通过本政策为您列举说明我们接入的第三方 SDK 名称及其隐私政策链接，便于您更清楚地了解您的个人信息使用、保护情况。具体信息如下：

第三方 SDK 收集个人信息频度说明

- 百度移动统计 SDK

使用目的：用于统计及分析客户端产品数据或服务数据

数据类型：最终用户的硬件型号及基本信息，操作系统版本及系统情况，设备配置，国际移动设备身份码 IMEI、国际移动用户识别码 IMSI、网络设备硬件地址 MAC、广告标识符 IDFA、匿名设备标识符 OAID、硬件序列号等设备标识符、终端品牌、终端制造厂商）、设备连接信息（例如浏览器的类型、电信运营商、使用的语言、WIFI 信息）以及设备状态信息（例如设备应用安装列表）。

官网链接：<https://tongji.baidu.com/web/help/article?id=330&type=0>

- 个推 SDK

使用目的：用于消息推送。

个推用户隐私协议：<https://docs.getui.com/privacy/>