

隐私政策

(V02/20210101)

本隐私政策适用于成都赛美斯医疗技术有限公司旗下的所有软件。本应用尊重并保护所有使用服务用户的个人隐私权。为了给您提供更准确、更有个性化的服务，本应用会按照本隐私权政策的规定使用和披露您的个人信息。但本应用将以高度的勤勉、审慎义务对待这些信息。除本隐私权政策另有规定外，在未征得您事先许可的情况下，本应用不会将这些信息对外披露或向第三方提供。本应用会不时更新本隐私权政策。您在同意本应用服务用户协议之时，即视为您已经同意本隐私权政策全部内容。本隐私权政策属于本应用服务用户协议不可分割的一部分。

1. 我们获取您的信息

在您使用 CIMS 平台服务时，我们可能收集如下信息：

(a) 日志信息，指您使用我们的服务时，系统可能通过 **cookies**、**web beacon** 或其他方式自动采集的技术信息，包括：

设备或软件信息，例如您的移动设备、网页浏览器或用于接入我们服务的其他程序所提供的配置信息、您的 IP 地址和移动设备所用的版本和设备识别码、

Android ID、**IMSI** 信息；

在使用我们服务时搜索或浏览的信息，例如您使用的网页搜索词语，以及您在使用我们服务时浏览或要求提供的其他信息和内容详情；

您通过我们的服务进行通讯的信息，例如通讯的账号，以及通讯时间、数据和时长；

您通过我们的服务上传的内容所包含的信息（元数据），例如拍摄或上传的照片或录像的日期、时间或地点等。

(b) **mac** 地址，指您使用我们产品时，收集设备中的 **mac** 地址信息，主要用于：定位异常网络请求，确保网络服务稳定与安全；

(c) 用户自行上传的文件，包括照片、视频、电子文档等。在使用上传功能时，需要您进行授权确认。

在您使用 CIMS 平台的 **app** 软件服务的过程中，我们会按照如下方式采集您在使用服务时主动提供的或因为使用服务而产生的信息，用以向您提供服务或优化我们的服务。

(a) 为帮助您进行手机号码、邮箱或账号登录，我们会收集您的手机号码或邮箱地址和移动网络标识信息。其中，手机号码或邮箱地址是敏感信息，如您拒绝提供，则将无法使用 **app** 软件的主要功能，但不影响您使用我们提供的其他功能；

(b) 我们可能通过 **cookie**、标识符及相关技术收集您的信息，包括您的设备信息、浏览信息、点击信息，并将该等信息储存为日志信息，为您提供个性化的用户体验、保障服务安全。您可以通过浏览器设置拒绝或管理 **cookie**、标识符或相关技术的使用在您使用本应用网络服务时。

另外，根据相关法律法规及国家标准，以下情形中，我们可能会采集、使用您的相关个人信息无需征求您的授权同意：

- (a) 与国家安全、国防安全等国家利益直接相关的；与公共安全、公共卫生、公共知情等重大公共利益直接相关的；
- (b) 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- (c) 出于维护您或其他个人的生命、财产、声誉等重大合法权益但又很难得到本人同意的；
- (d) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；
- (e) 根据您的要求签订和履行合同所必需的；
- (f) 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；
- (g) 为开展合法的新闻报道所必需的；
- (h) 出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的；
- (i) 法律法规规定的其他情形。

请您理解，我们向您提供的功能和服务是不断更新和发展的，如果某一功能或服务未在前述说明中且收集了您的信息，我们会通过页面提示、交互流程、网站公告等方式另行向您说明信息收集的内容、范围和目的，以征得您的同意。

2. 我们可能如何使用信息

我们可能将在向您提供服务的过程之中所收集的信息用作下列用途：

- (a) 向您提供服务；

- (b) 在我们提供服务时，用于身份验证、客户服务、安全防范、存档和备份用途，确保我们向您提供的产品和服务的安全性；
- (c) 帮助我们设计新服务，改善我们现有服务；
- (d) 软件认证或管理软件升级；
- (e) 让您参与有关我们产品和服务的调查。

3. 信息安全

(a) 信息的存储与交换。一般情况下，我们只会为实现服务目的所必需的时间内或法律法规规定的条件下存储您的个人信息。我们会按照法律法规规定，将境内收集的用户个人信息存储于中国境内。目前我们不会跨境传输或存储您的个人信息。

(b) 安全保护措施。我们努力为用户的信息安全提供保障，以防止信息的泄露、丢失、不当使用、未经授权访问和披露等。我们使用全方位的安全保护措施，以确保用户的个人信息保护处于合理的安全水平，包括技术保护手段、管理制度控制、安全体系保障等诸多方面。

我们采用业界领先的技术保护措施。我们使用的技术手段包括但不限于防火墙、加密（例如 SSL）、去标识化或匿名化处理、访问控制措施等。此外，我们还会不断加强安装在您设备端的软件的安全能力。例如，我们会在您的设备本地完成部分信息加密工作，以巩固安全传输；我们会了解您设备安装的应用信息和运行的进程信息，以预防病毒、木马等恶意程序。

我们建立了保障个人信息安全专门的管理制度、流程和组织。例如，我们严格限制访问信息的人员范围，要求他们遵守保密义务并进行审计，违反义务的人员会根据规定进行处罚。我们也会审查该管理制度、流程和组织，以防未经授权的人员擅自访问、使用或披露用户的信息。

我们建议您在使用产品和服务时充分注意对个人信息的保护，我们也会提供多种安全功能来协助您保护自己的个人信息安全。

(c) 安全事件处置措施

若发生个人信息泄露、损毁、丢失等安全事件，我们会启动应急预案，阻止安全事件扩大。安全事件发生后，我们会及时以推送通知、邮件等形式告知您安全事件的基本情况、我们即将或已经采取的处置措施和补救措施，以及我们对您的应对建议。如果难以实现逐一告知，我们将通过公告等方式发布警示。

(d) 产品或服务停止运营时的通知

当我们的产品或服务发生停止运营的情况时，我们将以推送通知、公告等形式通知您，并在合理期限内删除您的个人信息或进行匿名化处理，法律法规另有规定的除外。

4. 我们可能如何收集信息

我们可能通过 **cookies**、**web beacon**、标识符及相关技术收集和使用您的信息，包括您的设备信息、浏览信息、点击信息，并将该等信息储存为日志信息，为您提供个性化的用户体验、保障服务安全，并用于以下用途：

(a) 记住您的身份。例如：**cookies** 和 **web beacon** 有助于我们辨认您作为我们的注册用户的身份，或保存您向我们提供的有关您的喜好或其他信息；

(b) 分析您使用我们服务的情况。例如，我们可利用 **cookies** 和 **web beacon** 来了解您使用我们的服务进行什么活动；

您可以通过浏览器设置拒绝或管理 **cookies**、**web beacon**、标识符或相关技术。但请注意，如果停用 **cookies**、**web beacon**、标识符或相关技术，您有可能无法享受最佳的服务体验，某些服务也可能无法正常使用。

5. 我们可能分享的信息

根据相关法律法规及国家标准，以下情形中，我们可能会共享、转让、公开披露个人信息无需事先征得您的授权同意：

(a) 与国家安全、国防安全直接相关的；

- (b)与公共安全、公共卫生、重大公共利益直接相关的；
- (c)与犯罪侦查、起诉、审判和判决执行等直接相关的；
- (d)出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的；
- (e)个人信息主体自行向社会公众公开个人信息的；
- (f)从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道。

除此之外，未经您同意，我们不会与任何第三方分享您的个人信息。

如您发现自己的个人信息泄密，请您联系客服邮箱：

service@cims-medtech.com