

## 隐私政策

本政策仅适用于平安健康保险股份有限公司（以下简称“我们”或者“平安健康险”）向就医理赔管家平台用户提供的就医理赔管家软件系统（以下简称“就医理赔管家”或“APP”）及（或）附随的相关服务（以下简称“附随服务”，与“就医理赔管家”合称为“就医理赔管家及附随服务”）。

发布日期： 2025-06-05

生效日期： 2025-06-05

如果您有任何疑问、意见或建议，请通过以下联系方式与我们联系：

客服电话： 400-1143-837 转 2

个人信息保护负责人：李季

邮箱：LIJI164@pingan.com.cn

公司地址：上海市徐汇区凯滨路 166 号上海平安大厦 B 座 16 楼

### 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、 我们如何保护您的个人信息
- 五、 您的权利
- 六、 我们如何处理儿童的个人信息
- 七、 您的个人信息如何在全球范围转移
- 八、 本政策如何更新
- 九、 如何联系我们

个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。我们深知个人信息对您的重要性，并会尽全力保护您的个人信息安全可靠。我们致力于维持您对我们的信任，恪守以下原则，保护您的个人信息：权责一致原则、目的明确原则、选择同意原则、最少够用原则、确保安全原则、主体参与原则、公开透明原则等。同时，我们承诺，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。

请在使用就医理赔管家平台前，仔细阅读并了解本《隐私政策》。

## **一、我们如何收集和使用您的个人信息**

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

- 1、就医理赔管家平台仅会出于本政策所述的以下目的，收集和使用您的个人信息，当您关闭或者停止相关功能或服务的使用，便会停止对您个人信息的收集。
- 2、为实现本政策中声明的目的，以及为您提供更好的客户服务和用户体验，我们会接入第三方 SDK 服务。当您使用这些服务时，收集您的信息，当您关闭或者停止相关功能或服务的使用，便会停止对您个人信息的收集。
- 3、用户入驻平台需要完成登录注册--实名认证--审核的注册认证流程，审核通过后方可使用就医理赔管家平台进行服务处理。为了确保注册人员信息的真实性及服务的可追溯性，我们在实名认证环节需要收集获取您的生物信息（活体检测、人脸信息），进行验证核对，如果拒绝提供人脸信息则无法完成认证。

### **(一) 用户账号服务**

1、为了使您能够成为就医理赔管家平台用户，我们为您提供用户账号服务，包括账户注册、账户登录、密码修改、实名认证、人脸识别认证（人脸影像数据委托平安科技（深圳）有限公司 存储，联系方式： pub\_pat@pingan.com.cn ），在您注销账号时，我们将停止使用并删除人脸影像数据、消息服务、意见反馈等。

2、为您提供账号服务需要您提供以下信息：**您的手机号、登录密码、用户名称、用户类型、行业名称、部门名称、单位名称、所在城市、位置信息、身份证信息，及您的人脸信息。**

3、在人脸识别登录，face ID 本人认证，二次识别等功能场景中需要获取您的生物信息（**人脸信息、声纹信息、指纹信息**）以及收集您在使用我们的服务过程中产生相应的记录。同时为了验证信息的准确性，我们会将您的信息，**姓名、身份证号码、生物信息（人脸信息、声纹信息、指纹信息）**与合法存有您信息的平安科技（深圳）有限公司进行验证核对；我们会对该验证机构提供的信息来源合法性进行验证。同意本政策后即视为您同意并授权我们获取、使用您的上述信息并用于本服务，并授权我们用于验证身份功能。如您不同意认证或授权，请选择不同意，同时您将无法继续使用人脸识别功能，但这并不影响您使用其他的服  
务。您可点击我们的《人脸识别服务协议》查看我们的人脸识别服务政策。

4、在您使用本平台账号进行业务操作时，为给您提供更好的操作体验及必要的信息传输，我们会根据您的操作**收集您相关的 Android\_id、Mac 地址、应用列表、位置信息、照片信息、视频信息以及读取相册或存储的个人文件信息。**如您不同意认证或授权，请选择不同意，同时您将无法继续使用人脸识别功能，但这并不影响您使用其他的服  
务。您同意我们可以基于验证上述信息准确性的目的，将您的上述信息向合法存有您上述信息的机构进行验证核对。我们仅在您使用用户账号服务时，才收集如上个人信息，当关闭或者停止该功能的使用时，便停止个人信息的收集。您提供的上述信息，将在您使用本服务期间持续授权我们

使用。在您注销账号时，我们将停止使用并删除上述信息。如您不提供前述信息，无法使用用户账户服务，不影响您使用我们提供的其他服务。

在服务过程中基于硬件绑定和加固的目的（保障安全），经客户允许，我们将会收集手机设备信息（包括当前设备的型号；当前系统版本号；安卓系统唯一标识符： Android ID、IMEI），如您拒绝授权，将不会影响使用本服务的基本业务功能。

## **(二) 权限收集及服务信息展示**

为了让您快速找到您所需要处理的任务或提供服务，我们可能会收集您使用我们的产品与/或服务的设备信息（包括当前设备的型号当前系统版本号安卓系统唯一标识符：Android ID、IMEI）来为您提供服务信息的最优方式，为您推送消息提醒，提供知识库的学习。我们也会为了不断改进和优化上述的功能来使用您的上述个人信息。

我们也收集设备的基本信息权限（**手机 MAC 地址、网络参数、设备电量状态、状态栏、底层日志、锁屏、蓝牙、已安装应用程序、查看系统运行进程、获取当前运行的任务列表、获取任务信息权限 GET TASKS**）用于 APP 的基本功能的运行、安装及更新 APP 所必需的权限。其中查看系统运行进程的权限，用于唤醒 APP；获取已安装应用信息的权限，用于使用微信分享功能的时候判断微信 APP 是否存在。

任务作业的时候，我们会根据弹窗申请获得您的定位权限，以便根据您的定位来展示您所在位置信息。你也可以拒绝授权定位权限，这不会影响您继续任务作业的操作。

同时根据监管的可回溯要求，我们需要记录您的相关操作行为，以便监管查验，其中包括您的 WIFI 状态、内网 IP、MAC 地址、Andriod\_ID、IMEI 信息。

## **(三) 向您提供的服务**

### **1、您向我们提供的信息**

为完成服务的作业反馈，您需要提供本人的**真实姓名、证件类型、证件号码、性别、出生日期、人脸认证，以完成实名注册**。如果您拒绝提供此类信息，我们将无法完成人员的审核流程。

为了支持二维码扫描，我们需要开启您拍照、获取图片文件、相册的权限，权限开启前，我们将弹窗提示，由您来选择是否开启相应的权限。

如果您需要使用微信分享功能，我们将使用您的剪贴板，以确保功能正常使用。

如果涉及到了理赔代办、人伤探视服务，您需要提供客户的基本信息**（被保险人的姓名、被保险人的关系、证件类型、证件号码、性别、个人电话号码、电子邮箱地址）及个人就医信息（病症、以往病史、诊治记录、检查报告）**并将其上传。如果您拒绝提供此类信息，我们将无法完成相关保险/医疗健康产品的履约服务。由于涉及到上传图片信息，我们需要开启您拍照、获取图片文件、相册的权限，权限开启前，我们将弹窗提示，由您来选择是否开启相应的权限。

## 2、改进我们的产品与/或服务所必须的功能

我们可能为了提供服务及改进服务质量的合理需要而获得的您的其他信息，包括您与客户/客服联系时您提供的相关信息以及通话内容，您参与问卷调查时向我们发送的问卷答复信息，问题及建议反馈信息。对于从您的各种设备上收集到的信息，我们必要时会将它们进行关联，以便我们能在这些设备上为您提供一致的服务。为了给您更全面、丰富、性能更好的服务，我们可能会变更服务入口、升级服务功能，以便为您持续提供服务、内容、功能等。

## 3、为了使您便捷的进行复制粘贴操作

我们会访问您的手机剪切板，但不会将剪切板信息进行缓存保留。

#### 4、 基于摄像头（相机）和图片（相册）上传的服务

当您使用文件上传、实名认证、意见反馈、录音频（人伤探视作业，同时还需要您设备的麦克风权限）服务时，您可以使用摄像头（相机）来进行拍摄，或读取相册，上传您的作业材料、单据相关的照片、图像、视频资料。对于安卓手机，当您在就医理赔管家 APP 内进行截屏或录屏操作时，我们会需要您授权我们访问您的设备存储权限，以便存入截屏或录屏资料。

#### 5、电子签名技术

当您提交人伤探视材料时，我们会收集一次您及客户的电子签名，以便完成材料及报告的准备。

#### 6、保障服务安全所必需的功能

为提高您使用我们的产品与/或服务时系统的安全性，更准确地预防钓鱼网站欺诈和保护账户安全，我们必要时会通过了解您的浏览信息、工单信息、位置信息、设备信息（当前设备的型号；当前系统版本号；安卓系统唯一标识符： Android ID、IMEI）来判断您的账号风险，并可能会记录一些我们认为有风险的链接（" URL"）；我们也会收集您的设备信息对于系统问题进行分析、统计流量并排查可能存在的风险、在您选择向我们发送异常信息查询请求时予以排查、基于您的设备信息对未注册就医理赔管家账号时，您的信息的汇总。我们只在每次启动 App 时收集一次您的设备信息。

我们可能通过人脸识别功能，在获取您同意的情况下，将您的人脸图像信息传递至公安部进行身份验证和身份识别，但我们不会存储您的人脸图像信息。身份验证为摄像头通过拍摄照片或视频进行核查识别您是否为本人办理业务；身份识别为识别您在平安健康保险身份，

并根据身份提供对应的服务。如您不提供前述信息，我们将无法为您提供身份验证和身份识别相关服务，但不影响您使用我们提供的其他服务。

为保障您的账户安全，如果您使用的是安卓系统的手机设备，我们还需要您授权我们访问外部存储的权限。

#### **(四) 您可选择是否授权我们收集和使用您的个人信息的情形**

1、为使您的使用更方便，提升您在就医理赔管家 APP 的使用体验，我们的以下附加功能中可能会收集和使用您的个人信息。如果您不提供下面描述的个人信息，您将无法使用对应的服务，但并不影响基本功能及其他附加功能的使用。以下场景中，我们仅在您开启功能，主动提供或明确授权时采集您相应的个人信息。这些服务包括：

\*账号风险：某些不法组织、个人，利用非法手机号注册，用来薅羊毛获取利益、破坏平台公平性、扰乱正常交易秩序。我们通过手机号、设备号、用户行为等信息，大数据分析确定账号是否存在风险

**(1) 人伤探视，如果使用该服务，您需要提供录音、个人签名、与伤者/家属合影照片。**

**仅业务发生时收集。**

**(2) 陪诊协助，如果使用该服务，您需要提供地图定位、签到/签退照片、院内导航。仅**

**业务发生时收集。**

**(3) 院内陪护，如果使用这项服务，您需要提供地图定位、签到/签退照片。仅业务发生**

**时收集。**

**(4) 探视慰问/理赔代办/材料收集，如果使用该服务，您需要提供地图定位、签到照片。**

**仅业务发生时收集。**

**(5) 交通安排**, 如果使用该服务, 您需要提供陪护人员姓名、联系方式。仅业务发生时收集。

**(6) 入院探视**, 如果使用该服务, 您需要提供探访人姓名、联系方式、合影。仅业务发生时收集。

**(7) 购买意外保险**, 为了给您作业期间提供更多的保障, 您同意我们根据服务场景需要为您购买商业保险, 并基于购买商业保险的目的, 向商业保险公司提供您的姓名及身份证号码。

**2、上述附加功能可能需要您在您的设备中向我们开启您的地理位置 (位置信息)、相机 (摄像头)、相册 (图片库), 以实现这些功能所涉及的信息的收集和使用。位置权限开启后, 我们使用高德地图的 SDK 高德定位 (精准定位) 获取您的位置信息, 用于签到/签退打卡, 院内导航。如果您想禁用位置权限, 可在系统->设置->安全->应用权限中找到“读取位置信息”的权限, 点开找到“就医理赔管家”APP 来关闭位置权限。位置权限关闭后, 我们将无法获取您的位置信息。**

**3、除此之外, 我们还会使用平安集团插件天眼 SDK, 收集您的设备信息 (包括当前设备的型号; 当前系统版本号; 安卓系统唯一标识符: Android ID、IMEI) 及定位信息, 用于用户行为统计分析, 以上信息仅在弹窗获取您授权后获取。**

#### **(五) 设备权限调用**

为向您提供便捷、优质的服务, 我们会调用您设备的一些权限, 以下是我们调用的设备权限列表及对应的使用目的说明, 您有权随时选择关闭下列权限的授权, 会影响您正常使用我们互联网电子服务或商品的部分或全部功能。



- 1、设备信息：针对核心业务功能，为了完成安全风控及设备加固的目的，需要读取您的设备识别信息、设备状态信息以及设备环境信息、收集 IMEI/MEID 信息，当用户首次打开 APP 时会弹窗询问，如您选择不开启此权限，则无法完成安全风控验证及设备加固。
- 2、相机：针对核心业务功能，需要使用 **OCR 人脸识别**，拍摄照片时，用户首次使用相应服务时会进行弹窗询问。
- 3、相册：用户进行图片上传、保存时，首次使用相应服务前会弹窗询问。
- 4、通知：用户可以接收系统消息提醒，首次打开手机客户端时会弹窗询问。
- 5、无线数据、WLAN：连接网络时，用户首次打开手机客户端会弹窗询问，若关闭则无法正常使用 APP。
- 6、位置：为准确定位，优化用户搜索信息，首次打开 APP 时会弹窗询问，若关闭则无法准确使用基于位置的信息展示。
- 7、存储：为写入存储用户、存储日志等信息，首次打开 APP 时会弹窗询问，若关闭则无法正常使用。

设备权限	对应业务功能	调用权限的目的	是否询问	可否关闭权限	如果关闭权限会影响用户什么功能
设备信息	核心业务功能	为了完成安全风控及设备加固的目的，需要读取您的设备识别信息，设备	用户首次打开移动端时会弹窗询问	是	如您选择不开启此权限，则无法完成安全风控验证及设备加固

		状态信息以及设备环境信息			
位置	用于基于位置的城市服务、药店、医院信息展示、推送	通过用户当前位置,优化用户搜索等信息展示推荐	用户首次打开移动客户端时会弹窗询问	是	用户将无法准确使用基于位置的城市服务及医疗信息展示推荐
相机	核心业务功能	使用扫描二维码、OCR、人脸识别、拍摄照片	用户首次使用相应服务前会弹窗询问	是	用户无法正常使用二维码扫描、电子社保卡领卡等服务
相册	核心业务功能	图片上传、图片保存	用户首次使用相应服务前会弹窗询问	是	无法在业务中使用本地图片或保存图片到本地
通知	全部功能	接收系统消息提醒、支付结果、签约随	用户首次打开手机客户端时	是	用户无法正常接收各类消息,无法及时获知预约挂号、在线咨询等

		访消息	会弹窗询问		提醒
无线数据	全部功能	连接网络	用户首次打开手机客户端时会弹窗询问	是	移动客户端无法正常使用
WLAN	全部功能	连接网络	用户首次打开手机客户端时会弹窗询问	是	移动客户端无法正常使用
存储	全部功能	写入存储用户信息,存储日志信息	用户首次打开手机客户端时会弹窗询问	是	移动客户端无法正常使用
麦克风、录音	核心业务功能	人伤业务,理赔调查作业业务	用户使用相应服务前会弹窗	是	用户在使用互联网电子服务或商品时无法正常交流

			询问		
拨打电话	快捷拨号	方便您在功能页面直接拨打医院、人社或医保服务网点电话	用户使用相应服务前会弹窗询问	是	需自己到拨号页面拨打电话
读取应用列表	消息推送	获取就医理赔管家是否在运行状态	用户首次打开移动客户端时会弹窗询问	是 ( oppo 部分机型不支持)	点击通知栏消息无法跳转详情页面或无法打开 app

## (六) 扩展业务功能及所需要的信息

不涉及拓展业务。

## 二、我们如何使用 Cookie 和同类技术

### (一) Cookie

为确保网站正常运转，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，网站能够存储您的偏好或购物篮内的商品等数据。

我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。有关详情，请参见 [AboutCookies.org](http://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，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置。

## **(二) Do Not Track (请勿追踪)**

很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我们的所有网站都会尊重您的选择。

## **(三) 网络 Beacon**

我们网站上会包含一些电子图像（称为“单像素 GIF 文件”或者“网络 beacon”），使用网络 beacon 可以帮助网站计算浏览网页的用户或者访问某些 cookie，我们会通过网络 beacon 收集您浏览网页活动的信息，您访问的页面地址、您先前访问的援引页面的位置、您的浏览环境以及显示设定。

## **(四) 网络代理**

如您通过我们的网站或者客户端，访问第三方服务，我们无法保证这些第三方会按照我们的要求采取保护措施。为了尽力保证您的账号安全，我们会使用专用的网络协议及代理技术（称为“专用网络通道”“网络代理”）。通过这种方式，我们可以帮您识别已知的高风险站点，减少由此引起的钓鱼、账号泄露等风险，同时更有利于保障您和第三方的共同利益。

## **(五) 关于 SDK 服务部分描述**

为保障就医理赔管家的稳定运行或实现相关功能，我们可能会接入由第三方提供的软件开发包（SDK）实现前述目的。我们会尽到审核义务，对合作方获取信息的软件工具开发包

(SDK) 进行严格的安全监测，以保证数据安全，保证您的个人信息安全。我们接入的第三方 SDK 主要服务于您以及其他用户的需求，因此在满足新的服务需求及业务功能变更时，我们有可能调整接入的第三方 SDK。对此情况，我们会及时在本说明中向您公开说明接入的第三方 SDK 的最新情况。目前就医理赔管家接入的 [《第三方 SDK 收集使用信息说明》](#)，  
明细如下：

### **高德定位（精准定位） SDK**

**公司名称：**高德软件有限公司

**联系方式：**4008100080

**收集信息：**定位权限、读写 SD 卡、手机状态、网络、运营商、当前已连接上的 wifi 信息、OAID、SSID、BSSID、周围的 wifi 信息、传感器

**收集方式：**本机采集

**收集权限：**地理位置权限

**使用目的与场景：**地图定位与签到截图

**隐私政策：**[点击查看](#)

### **人脸识别 SDK**

**公司名称：**深圳壹账通智能科技有限公司

**联系方式：**pub\_jryzt\_ekycserv@pingan.com.cn

**收集信息：**人脸信息

**收集方式：**本机采集

**收集权限：**摄像头权限

**使用目的与场景：**人脸识别、每日打卡

隐私政策: [点击查看](#)

## 平安天眼 SDK

公司名称: 平安科技(深圳)有限公司

联系方式: MAWEISEN329@pingan.com.cn

收集信息: WIFI MAC、BSSID、通过基站获取经纬度、本地局域网 IP、  
ANDROID\_ID、IMEI、SerialNo、IMSI、蓝牙 MAC、运营商信息、OAID

收集方式: 本机采集

收集权限: 手机终端标识信息权限

使用目的与场景: 当您使用 APP 时, SDK 将获取权限生成设备唯一码已追踪标  
记唯一用户记录用户行为

隐私政策: [点击查看](#)

## 平安 PUSH SDK +厂商通道 SDK(含小米、华为、魔推、vivo)

公司名称: 平安科技(深圳)有限公司

联系方式: pub\_pat@pingan.com.cn

收集信息: 手机状态权限、IMEI、设备号、ANDROID\_ID、设备 MAC、运行  
进程信息、已安装应用程序列表、开放匿名设备标识符

收集方式: 本机采集

收集权限: 手机终端标识信息权限、读写手机存储权限

使用目的与场景: 用于 APP 推送、通知

隐私政策: [点击查看](#)

## 平安看云 SDK

**公司名称：**平安科技(深圳)有限公司

**联系方式：**pub\_pat@pingan.com.cn

**收集信息：**设备 ID 信息、设备 IMEI 信息、IP 地址、网络状态、用户操作信息、Android id、开放匿名设备标识符

**收集方式：**本机采集

**收集权限：**手机终端标识信息权限

**使用目的与场景：**当您首次启动 App 时，授予 READ PHONE STATE 权限时，读取 deviceId，当发现如无权限，则会使用其他信息替代；用于 APP 性能管理平台系统，达到 APP 性能优化的目的

**隐私政策：**[点击查看](#)

## 平安 Sparta SDK

**公司名称：**平安科技(深圳)有限公司

**联系方式：**pub\_pat@pingan.com.cn

**收集信息：**传感器、运营商、AndroidID 信息、SSID 信息、BSSID 信息、ICCID、IMSI 信息、IMEI 信息、MAC 地址

**收集方式：**本机采集

**收集权限：**手机终端标识信息权限

**使用目的与场景：**应用安全风控，用于反欺诈渠道监控、行为预警

**隐私政策：**[点击查看](#)



## 华为 HMS SDK

**公司名称：**华为技术有限公司

**联系方式：**developer@huawei.com

**收集信息：**读取手机状态和身份信息、IMEI 信息、MAC 地址

**收集方式：**本机采集

**收集权限：**手机终端标识信息权限

**使用目的与场景：**用于华为 HMS 更新服务

**隐私政策：**[点击查看](#)

## 图片验证码风控 SDK（极验 geetest）

**公司名称：**武汉极意网络科技有限公司

**联系方式：**service@geetest.com

**收集信息：**读取网络状态、传感器信息

**收集方式：**本机采集

**收集权限：**手机终端标识信息权限

**使用目的与场景：**用户滑块验证码验证

**隐私政策：**[点击查看](#)

## 众寻 3D 室内导航 SDK

**公司名称：**众虎物联网（广州）有限公司

**联系方式：**ssales@locnavi.com

**收集信息：**位置信息（经纬度、精确位置、粗略位置）【通过 IP 地址、GNSS 信息、WiFi 状态、WiFi 参数、WiFi 列表、基站信息、信号强度的信息、蓝牙信息、传感器信息（矢量、加速度、压力）、设备信号强度信息获取】

**收集方式：**本机采集

**收集权限：**地理位置权限

**使用目的与场景：**用于医院内导航

**隐私政策：**[点击查看](#)

## **腾讯会议 SDK**

**公司名称：**深圳市腾讯计算机系统有限公司

**联系方式：**Dataprivacy@tencent.com

**收集信息：**姓名、手机号、名称、头像、所属企业、IP 地址、会议音频和视频信息、会议的开始和结束时间、会议主题、会议 ID，以及各参与者加入会议的开始时间、结束时间和参加会议的时长、加速度传感器、距离传感器、方向传感器、设备运动数据（仅 iOS 版，用于采集陀螺仪数据）、已安装应用列表

**收集方式：**本机采集

**收集权限：**获取摄像头、麦克风、相册权限

**使用目的与场景：**使用音视频会议

**隐私政策：**[点击查看](#)

## **神策数据 SDK**

**公司名称：**神策网络科技（北京）有限公司

**联系方式：**400-650-9827

**收集信息：**设备属性信息（Android ID/OAID/IDFA/IDFV/UUID）、位置信息（GPS 位置信息）、网络信息（网络信息）、设备硬件信息（设备型号、屏幕分辨率、硬件制造商、产品名称）、操作系统信息（系统名称、系统版本、系统语言）、应用信息（时区、应用 app\_id、应用名称、应用版本号）

**收集方式：**本机采集

**收集权限：**获取摄像头、麦克风、相册权限

**使用目的与场景：**用于行为统计分析及应用安全风控

**隐私政策：**[点击查看](#)

## **PictureSelector SDK**

**公司名称：**开源工具

**收集信息：**图片

**收集方式：**本机采集

**收集权限：**获取摄像头、相册权限、存储权限

**使用目的与场景：**图片选择

**隐私政策：**不涉及

## **三、我们如何共享、转让、公开披露您的个人信息**

### **(一) 共享**

我们不会与平安健康保险股份有限公司以外的任何公司、组织和个人分享您的个人信息，但以下情况除外：

1、在获取明确同意的情况下共享：获得您的明确同意后，我们会与其他方共享您的个人信息。

2、我们会根据法律法规规定，或按政府主管部门的强制性要求，对外共享您的个人信息。

3、与授权合作伙伴共享：仅为实现本政策中声明的目的，我们的某些服务将由授权合作伙伴提供。我们会与合作伙伴共享您的某些个人信息，以委托授权合作伙伴为您提供更好的客户服务和用户体验。在您上网购买我们的产品时，我们必须与物流服务提供商共享您的个人信息才能安排送货，或者安排合作伙伴提供服务。我们仅会出于合法、正当、必要、特定、明确的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。我们的合作伙伴无权将共享的个人信息用于任何其他用途，如果授权合作伙伴将您的信息用于我们未委托的用途，其将单独征得您的同意。

目前，我们的授权合作伙伴包括以下两大类型：

1、广告、分析服务类的授权合作伙伴。除非得到您的许可，否则我们不会将您的个人身份信息（指可以识别您身份的信息，**姓名**或**电子邮箱**，通过这些信息可以联系到您或识别您的身份）与提供广告、分析服务的合作伙伴分享。我们会向这些合作伙伴提供有关其广告覆盖面和有效性的信息，而不会提供您的个人身份信息，或者我们将这些信息进行处理，以便它不会识别您个人。只有在广告主同意遵守我们的广告发布准则后，我们才会告诉广告主他们广告的效果如何，或者有多少人看了他们广告或在看到广告后安装了应用，或者向这些合作伙伴提供不能识别个人身份的统计信息（“位于北京的 25 岁男性，喜欢软件开发”），帮助他们了解其受众或顾客。

2、供应商、服务提供商和其他合作伙伴。我们将信息委托给支持我们业务的供应商、服务提供商和其他合作伙伴，这些支持包括受我们委托提供技术基础设施服务、分析我们服务的使用方式、衡量广告和服务的有效性、提供客户服务、支付便利或进行学术研究和调查。

对我们与之共享个人信息的公司、组织和个人，我们会与其签署严格的保密协定，要求他们按照我们的说明、本隐私政策以及其他任何相关的保密和安全措施来处理个人信息。

## **(二) 转让**

我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外：

- 1、在获取明确同意的情况下转让：获得您的明确同意后，我们会向其他方转让您的个人信息；
- 2、在涉及合并、分立、解散、收购或破产清算时，如涉及到个人信息转让，我们会再要求新的持有您个人信息的公司、组织继续受此隐私政策的约束，否则我们将要求该公司、组织重新向您征求授权同意。

## **(三) 公开披露**

我们仅会在以下情况下，公开披露您的个人信息：

- 1、获得您明确同意后；
- 2、基于法律的披露：在法律、法律程序、诉讼或政府主管部门强制性要求的情况下，我们会公开披露您的个人信息。

## **(四) 根据国家相关法律法规及国家标准，以下情形中，收集、使用个人信息无需征得您的授权同意：**

- 1、与国家安全、国防安全有关的；
- 2、与公共安全、公共卫生、重大公共利益有关的；
- 3、与犯罪侦查、起诉、审判和判决执行等有关的；
- 4、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；
- 5、所收集的个人信息是个人信息主体自行向社会公众公开的；

- 6、从合法公开披露的信息中收集的您的个人信息的，如合法的新闻报道、政府信息公开等渠道；
- 7、根据您的要求签订合同所必需的；
- 8、用于维护所提供的产品与/或服务的安全稳定运行所必需的，例如发现、处置产品与/或服务的故障；
- 9、法律法规规定的其他情形。

#### **四、我们如何保护您的个人信息**

（一）我们已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权访问、公开披露、使用、修改、损坏或丢失。我们会采取一切合理可行的措施，保护您的个人信息。在您的浏览器与“服务”之间交换数据（如信用卡信息）时受 SSL 加密保护；我们同时对就医理赔管家网站提供 https 安全浏览方式；我们会使用加密技术确保数据的保密性；我们会使用受信赖的保护机制防止数据遭到恶意攻击；我们会部署访问控制机制，确保只有授权人员才可访问个人信息；以及我们会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。

（二）我们会采取一切合理可行的措施，确保未收集无关的个人信息。 **我们只会在达成本政策所述目的所需的期限内保留您的个人信息，除非需要延长保留期或受到法律的允许。**

（三）互联网并非绝对安全的环境，而且电子邮件、即时通讯、及与其他平台用户的交流方式并未加密，我们强烈建议您不要通过此类方式发送个人信息。请使用复杂密码，协助我们保证您的账号安全。

（四）我们将定期更新并公开安全风险、个人信息安全影响评估等报告的有关内容。您可通过就医理赔管家平台推送的消息获得。

(五) 互联网环境并非百分之百安全，我们将尽力确保或担保您发送给我们的任何信息的安全性。如果我们的物理、技术、或管理防护设施遭到破坏，导致信息被非授权访问、公开披露、篡改、或毁坏，导致您的合法权益受损，我们将承担相应的法律责任。

(六) 在不幸发生个人信息安全事件后，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、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、推送通知方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。

(七) 当我们的产品或服务发生停止运营的情形时，我们将以推送通知、公告形式通知你，在合理的期限内删除你的个人信息或进行匿名化处理，并立即停止收集个人信息，如：在人脸识别登录，face ID 本人认证，二次识别等功能场景中的活动，以及关闭第三方应用服务接口，避免第三方服务收集及继续使用个人信息。

(八) 平安健康险会依照个人信息的不同等级存储不同期限，存储期限严格按照法律及相关法规规定，最低期限不少于 6 个月。超出必要期限后，我们将对您的个人信息进行删除或匿名化处理，但法律另有规定的除外。

同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。

## **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：

### **(一) 访问您的个人信息**

您有权访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问：

**账户信息** ——如果您希望访问或编辑您的账户中的个人资料信息和支付信息、更改您的密码、添加安全信息等，您可以在就医理赔管家平台“个人-个人信息管理”中行此类操作。

**搜索信息** ——您可以在就医理赔管家平台已完成任务列表中访问您的历史记录、查看以及管理其他数据。

如果您无法通过上述方式访问这些个人信息，您可以随时使用我们的 Web 表单联系，或通过拨打 400-1143-837 转 2。我们将在 15 天内回复您的访问请求。

对于您在使用我们的平台服务过程中产生的其他个人信息，只要我們不需要过多投入，我们会向您提供。如果您想行使数据访问权， 请通过拨打 400-1143-837 转 2。

## **(二) 更正您的个人信息**

当您发现我们处理的关于您的个人信息有错误时，您有权要求我们做出更正。您可以在就医理赔管家平台“个人-个人信息管理”中行此类操作。

如果您无法通过上述链接更正这些个人信息，您可以随时使用我们的 Web 表单联系，或通过拨打 400-1143-837 转 2。我们将在 15 天内回复您的更正请求。

## **(三) 查阅、复制和转移个人信息的权力**

您有权查阅、复制您的个人信息以及转移您的个人信息到您指定的个人信息处理者，请参阅“九、如何联系我们”一节中的方式与我们联系，实现上述权利。

## **(四) 删除您的个人信息**

在以下情形中， 您可以联系我们的客服电话 400-1143-837 转 2 向我们提出删除个人信息的请求：

- 1、如果我们处理个人信息的行为违反法律法规；
- 2、如果我们收集、使用您的个人信息，却未征得您的同意；



- 3、如果我们处理个人信息的行为违反了与您的约定；
- 4、如果您不再使用我们的产品或服务，或您注销了账号；
- 5、如果我们不再为您提供产品或服务。

若我们决定响应您的删除请求，我们还将同时通知从我们获得您的个人信息的实体，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。您可以在前往【个人】页面，点击【删除账户】进行处理。

当您从我们的服务中删除信息后，我们不会立即备份系统中删除相应的信息，但会在备份更新时删除这些信息。

#### **(五) 改变您授权同意的范围**

每个业务功能需要一些基本的个人信息才能得以完成（见本政策“第一部分”）。对于额外收集的个人信息的收集和使用，您可以随时给予或收回您的授权同意。

当您需要撤回隐私同意。您可以在就医理赔管家平台“我的-设置-关于就医理赔管家-隐私政策”隐私政策右上角进行撤回操作。

当您收回同意后，我们将不再处理相应的个人信息。但您收回同意的决定，不会影响此前基于您的授权而开展的个人信息处理。

如果您不想接收我们给您发送的商业广告，您随时可通过拨打客服电话告知我们您的请求，我们将会 在 15 日内处理。 取消： 400-1143-837 转 2。

#### **(六) 个人信息主体注销账户**

您随时可注销此前注册的账户，您可以在就医理赔管家平台“个人”页面点击右上角设置图标，“安全中心”进行注销账号操作。

在注销账户之后，我们将停止为您提供产品或服务，并依据您的要求，删除您的个人信息，法律法规另有规定的除外。

## **(七) 个人信息主体获取个人信息副本**

您有权获取您的个人信息副本，您可以通过拨打客服电话提出申请：400-1143-837 转 2。

符合国家网信部门规定条件的，在技术可行的前提下，数据接口匹配，我们还可按您的要求，直接将您的个人信息副本传输给您指定的第三方。

## **(八) 约束信息系统自动决策**

在某些业务功能中，我们仅依据信息系统、算法在非人工自动决策机制做出决定。如果这些决定影响您的合法权益，您有权要求我们做出解释，并有权拒绝我们仅通过自动化决策的方式作出决定。

经您同意的情况下进行自启动或关联启动，并仅在合理的使用场景下，以为终端用户提供服务为目的，以最小的频次对 APP 的自启动与关联启动进行配置设置。

## **(九) 响应您的上述请求**

为保障安全，我们会先要求您验证自己的身份，然后再处理您的请求。

我们将在十五天内做出答复。如您不满意，还可以通过拨打客服电话投诉：

400-1143-837 转 2

对于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段（需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（涉及备份磁带上存放的信息）的请求，我们会予以拒绝。

在以下情形中，我们将无法响应您的请求：

- 1、与个人信息控制者履行法律法规规定的义务相关的；
- 2、与国家安全、国防安全直接相关的；

- 3、与公共安全、公共卫生、重大公共利益直接相关的；
- 4、与犯罪侦查、起诉、审判和执行判决等直接相关的；
- 5、个人信息控制者有充分证据表明个人信息主体存在主观恶意或滥用权利的；
- 6、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；
- 7、响应个人信息主体的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害的；
- 8、涉及商业秘密的。

## **六、我们如何处理儿童的个人信息**

我们的产品、网站和服务主要面向成人。如果没有父母或其他监护人的同意，儿童不得创建自己的用户账户。

对于经父母或其他监护人同意而收集儿童个人信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护儿童所必要的情况下使用或公开披露此信息。

尽管当地法律和习俗对儿童的定义不同，但我们将不满 14 周岁的任何人均视为儿童。

如果我们发现自己在未事先获得可证实的父母或其他监护人同意的情况下收集了儿童的个人信息，则会设法尽快删除相关数据。

## **七、您的个人信息如何在全球范围转移**

我们收集和产生的个人信息，将存储在中华人民共和国境内，不涉及向境外转移。

## **八、本政策如何更新**

我们的隐私政策变更。

未经您明确同意，我们不会削减您按照本隐私政策所应享有的权利。我们会在本页面上发布对本政策所做的任何变更。

对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，我们会通过电子邮件发送通知，说明隐私政策的具体变更内容）。

本政策所指的重大变更包括但不限于：

- 1、在法律法规有新的要求时，或在我们的业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件，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、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 3、个人信息共享、转让或公开披露的主要对象发生变化；
- 4、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；
- 5、我们负责处理个人信息安全的责任部门、联络方式及投诉渠道发生变化时；
- 6、个人信息安全影响评估报告表明存在高风险时。

我们还会将本政策的旧版本存档，供您查阅。

## **九、如何联系我们**

如果您对本隐私政策有任何疑问、意见或建议，通过以下方式与我们联系： 通过拨打 400-1143-837 转 2 进行反馈。一般情况下，我们将在十五天内回复。

如果您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以通过以下外部途径寻求解决方案：向消费者权益保护部门、监管机关举报或者向有管辖权的法院提起诉讼。