

# 隐私政策

## 引言

我们非常重视用户的隐私和个人信息保护。您在使用我们的产品与/或服务时，我们可能会收集和使用您的信息。我们希望通过《隐私政策》（“本政策”）向您说明我们的业务情形和对应需要收集您个人信息的类型，以及我们为您提供访问、更新、删除这些信息的途径和保护措施，还有当我们共享、转让、公开披露您个人信息时需要遵守的规则。本政策与您所使用的医为系院内移动应用服务以及该服务所包括的各种业务功能（以下统称“我们的产品与/或服务”）息息相关，希望您在使用我们的产品与/或服务前仔细阅读并确认您已经充分理解本政策所写明的内容（特别是加粗字体的内容），并让您可以按照本政策的指引做出您认为适当的选择。本政策中涉及的相关术语，我们用简明扼要的表述，以便您更好地理解。您使用或在我们更新本政策后（我们会及时提示您更新的情况）继续使用我们的产品与/或服务，即意味着您同意本政策(含更新版本)内容，并且同意我们按照本政策收集、使用、保存和共享您的相关信息。

需要特别说明的是，本政策仅适用于本政策定义的产品与/或服务。当您使用第三方机构直接向您提供的产品或服务并向其提供您的个人信息时，我们建议您在使用前仔细查看他们的隐私政策，了解他们如何处理您的信息，以便审慎决策。

### 1. 我们如何收集您的个人信息

我们会遵循正当、合法、必要的原则，出于本政策所述的以下目的，收集和使用您在使用产品与/或服务过程中主动提供或因使用产品与/或服务而产生的个人信息，以及从第三方获取您的相关个人信息。**如果我们要将您的个人信息用于本政策未载明的其它用途，或将基于特定目的收集而来的信息用于其他目的，我们将以合理的方式向您告知，并在使用前再次征得您的同意。**

#### 1.1. 我们如何收集您的信息

我们会通过如下三种渠道获取您的个人信息：

##### 1.1.1. 您直接提供的信息

我们可能收集并存储您在使用医为系院内移动应用服务时向我们提供的信息，包

括您在我们页面中在线填写信息时、申请产品与/或服务时、解决争议或就医为系院内移动应用服务与我们联系时所提供的信息，以及您在使用我们服务过程中产生的关于您的交易和活动的信息。

### 1.1.2. 我们主动收集的信息

在您使用医为系院内网站、APP 及相关服务过程中，我们会收集您的计算机、手机及其他访问设备发送给我们的信息。

### 1.1.3. 我们从其他来源取得的信息

在取得您同意的前提下，我们还可能关联公司及合作伙伴及依法成立并合法留存您的相关信息的第三方机构获取您的相关信息。

## 1.2. 我们收集您的哪些信息

### 1.2.1. 账号注册与登录功能

您需要注册医为账号登录医为系院内移动应用。在此过程中，为对您的账号进行验证以实现登录目的，我们将按照本政策的约定收集、存储您的**账号名、用户名、密码、联系人姓名、手机号码**用于账号注册与登录的基础账号信息和您自行选择补充提供的头像、昵称其他账号信息，请您在使用医为账号登录功能前仔细阅读相关内容。收集这些信息是用于为您提供账号登录服务以及保障您的账号安全，若您不提供上述信息，则您无法正常登录医为系院内移动应用。

### 1.2.2. 资质认证

为了确认您的身份及执业资质，您可能需要提供姓名、身份证照片、免冠正面照片、职业、资格证书、科室、职称证书、所在医院。我们可能会将上述信息提交给合法持有您上述信息的第三方机构，以便对您所提供信息的真实性和准确性进行核对。如果您不提供上述信息或验证未通过，则您无法使用医为系院内移动应用服务。您可以选择提供个人简介、擅长领域或工作胸牌，如果您不提供上述信息，不影响您使用医为系院内移动应用的服务。

### 1.2.3. 保障安全所必须的功能

为保障您使用我们的产品与/或服务时系统的稳定性和安全性，防止您的信息被非法获取，更准确地预防欺诈和保护账号安全，我们需要收集您的设备信息（**设备型**

号、设备 Mac 地址、Wifi Mac 地址、应用进程列表、设备识别码、操作系统及软件版本、设备状态、网络状况)、历史上网记录、日志信息、IP 地址、位置信息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用于对医为系院内移动应用系统问题进行分析、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时予以排查。如果您不提供上述信息，我们则无法在您使用服务过程中对您的服务及账号安全进行保护。

#### 1.2.4. 运营活动

我们会通过收集您的医院、科室、职业、机构、医院等级信息通过 APP 通知、电话、短信的方式，合理地向您发送新发起的运营活动、平台最新的有关管理和服务的消息，及其他有告知必要的服务通知。

#### 1.3. 我们通过第三方主体或使用第三方服务时间收集您信息

我们可能会在您的授权同意范围内从第三方(我们的合作方)处收集并使用您的个人信息。我们保证严格依照与第三方签订的合同以及相关法律规定处理您的个人信息，同时请您详细阅读该第三方的隐私政策及用户协议。如您拒绝第三方在提供服务时收集、使用或者传递您的个人信息，将可能导致您无法使用相应的服务。

#### 1.4. 征得授权同意的例外

依据相关法律法规及国家标准，以下情形中，我们可能会依法收集并使用您的个人信息无需征得您的同意：

- 1、与国家安全、国防安全直接有关的；
- 2、与公共安全、公共卫生、重大公共利益直接有关的；
- 3、与犯罪侦查、起诉、审判和判决执行等直接有关的；
- 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您本人同意的；
- 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；

7、根据您的要求签订和履行合同所必需的；

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、处置服务的故障；

9、法律法规规定的其他情形。

## 2. 我们如何使用您的个人信息

### 2.1. 国家法律法规及监管要求

为了遵守国家法律法规及监管要求，以及向您提供服务及提升服务质量，或保障您的账号和资金安全，我们会在以下情形中使用您的信息：

(1) 实现本政策“我们收集您的哪些信息”约定的目的。

(2) 为了保障服务的稳定性与安全性，我们会将您的信息用于身份验证、安全防范、诈骗监测、预防或禁止非法活动、降低风险、存档和备份用途。

(3) 为了使您知晓使用我们服务的状态，我们会向您发送服务提醒。

(4) 根据法律法规或监管要求向相关部门进行报告。

(5) 邀请您参与我们服务有关的客户调研。

(6) 提高、完善和优化医为系院内移动应用在线服务。

(7) 处理您对医为系院内移动应用产品与/或服务的申请或反馈请求。

(8) 我们通过技术手段对数据进行去标识化处理后，去标识化处理的信息将无法识别主体。

**请您了解并同意，在此情况下我们有权使用已经去标识化的信息；在不透露您个人信息的前提下，我们有权对用户数据库进行分析并予以商业化的利用。**

(9) 我们会对我们的产品与/或服务使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示我们的产品与/或服务的整体使用趋势。但这些统计信息不包含您的任何身份识别信息。

## 2.2. 脱敏展示

当我们展示您的个人信息时，我们会采用包括内容替换、匿名处理方式对您的信息进行脱敏展示，以保护您的信息安全。

## 2.3. 其它用途

当我们要将您的个人信息用于本政策未载明的其它用途时，或基于特定目的收集而来的信息用于其他目的时，会事先征求您的同意。**请您理解，我们向您提供的产品与/或服务将不断更新变化。如果您选择使用本政策中尚未列明的其他产品与/或服务时，在我们收集您的个人信息前，我们会通过业务协议、页面提示的方式向您详细说明信息收集的目的、方式、范围并征求您的明确同意。若您不同意提供前述信息，您可能无法使用该项服务，但不影响您使用其他服务。**

## 3. 我们如何使用 Cookie 和同类技术

### 3.1. Cookie 的使用

#### 3.1.1. 为使您获得更轻松的访问体验

为使您获得更轻松的访问体验，我们有时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 是一种网络服务器存储在计算机或移动设备上的纯文本文件，其内容只能由创建它的服务器检索或读取。每个 Cookie 对您的网络浏览器或移动应用程序都是唯一的。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，网站能够记住用户的单次访问（使用会话 Cookie）或多次访问（使用永久 Cookie）。借助于 Cookie，网站能够保存设置，例如计算机或移动设备的语言、字体大小和其他浏览偏好。这意味着，用户无需在每次访问时重新配置用户偏好设置。如果某个网站不使用 Cookie，那么在用户每一次打开网页时，该网站都会将其视为新访客。例如，如果您登录某个网站后转到另一个网页，该网站就不会识别出您，而您会被再次注销。

#### 3.1.2. 为了向您提供更为便捷的服务

为了向您提供更为便捷的服务，我们通过 Cookie 等技术为您提供以下服务：

（1）记住您的账号。例如，当您访问一个需要您登录才可以提供的信息或服务，当您登录时，我们会把您的登录名加密存储在您计算机的 Cookie 文件中，由于是不可逆转的加密存储，其他人即使可以使用您的计算机，也无法识别出您的登录

名。您并不需要额外做任何工作，所有的收集、保存和加密工作都由系统自动完成。**Cookie** 可能帮助您省去为使用我们服务而重复输入账号的步骤。

(2) 分析您使用我们服务的情况。例如，我们可通过 **Cookie**、网络信标等技术来了解您使用我们服务的具体用途，或哪些网页或服务最受您的欢迎。

(3) 我们也可能通过网络信标技术来统计匿名访问的数据，同样，这些统计信息并不包括您的个人信息。

我们不会将 **Cookie** 用于本政策所述目的之外的任何用途

### 3.1.3. 我们不会将 **Cookie** 用于本政策所述目的之外的任何用途。

您可以随时使用自带清除 **Cookie** 功能的浏览器或操作系统软件根据自己的偏好管理或删除 **Cookie**。您可以清除计算机上保存的所有 **Cookie**，大部分网络浏览器会自动接受 **Cookie**，但您通常可根据自己的需要来修改浏览器的设置以拒绝 **Cookie** 或删除 **Cookie**。但如果您这么做，您可能需要在每一次访问我们的网站时亲自更改用户设置，可能会对您所使用服务的安全性和便捷性有一定影响，但不影响您正常使用我们提供的其他服务。

### 3.2. 网络信标、像素标签等同类技术的使用

除 **Cookie** 外，我们还会在网站上使用网络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点击 **URL**。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和服务偏好并改善客户服务。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。如果您不希望自己的活动以这种方式被追踪，则可以随时选择退订。

## 4. 我们如何委托处理、共享、转让、公开披露您的个人信息

### 4.1. 委托处理

为了提高效率、降低成本，我们可能会委托关联公司或其他专业服务提供商代表我们来处理信息，例如我们会聘请服务提供商为我们提供基础设施技术服务、数据处理和客户支持服务。对我们委托处理个人信息的公司、组织和个人，我们会通过书面协议、现场审计等方式要求其遵守严格的保密义务并采取有效的保密措施，要求其只能在委托范围内处理您的信息，而不得出于其自身利益使用您的信息。

## 4.2. 共享

我们不会与东华医为科技有限公司以外的任何公司、组织和个人共享您的个人信息，除非获得您的明确同意或属于“共享、转让、公开披露个人信息时事先征得授权同意的例外”。我们可能会向关联公司、合作伙伴等第三方共享您的个人信息，以保障为您提供的服务顺利完成；但我们仅会出于合法、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。该等第三方无权将共享的个人信息用于任何其他用途。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协议、本政策要求的保密和安全措施来处理个人信息。在个人敏感数据使用上，我们要求第三方采用数据脱敏和加密技术，从而更好地保护用户数据。我们将按照法律法规及国家标准的要求以点击确认协议、具体场景下的点击确认动作等形式征求您的同意。

### 4.2.1. 业务共享

(1) 为便于我们基于统一的医为账号体系向您提供服务以及便于您进行统一管理、保障系统和账号安全，您的个人信息可能会在我们和我们的关联公司之间进行必要共享。但我们只会共享必要的个人信息，且受本政策中所声明目的的约束；我们的关联公司如要改变个人信息的处理目的，将再次征求您的授权同意。例如，为了我们的关联公司为向您提供服务而需履行监管对客户身份识别的要求，或为我们与关联公司共同向您提供或推荐服务、产品，或为了协助解决您与我们的关联公司之间就交易产生的纠纷，我们会与关联公司共享您的信息。

(2) 第三方数据服务方。我们须将您的身份信息、资质信息与第三方数据服务方共享并从第三方获取关于您身份信息、资质信息的真实性、准确性的信息，来实现确认您身份和资质的目的。

(3) 第三方支付结算服务方。基于您的委托，我们会将您的身份证照片和银行卡信息提供至合作方以便代您办理费用结算、发票开具、纳税申报、税费缴纳等事宜。

(4) 其他医生。为了更好地了解患者的疾病史、就诊史，以免发生用药禁忌等医疗差错和误诊，我们会在必要的情况下，将您的姓名以及问诊记录信息、您开具的处方信息提供至为同一患者提供医疗服务的其他医生。

(5) 委托我们进行推广的合作伙伴（“委托方”）。有时我们会接受其他企业委托向使用我们产品与/或服务的用户群进行促销推广。我们可能会使用您的个人信息以及您的非个人信息集合形成的间接用户画像与委托方共享，但我们仅会向这些委托方提

供推广的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将这些信息进行汇总，以便提供该等信息并不会识别您个人。例如我们可以告知该委托方在浏览了委托方推广信息或在看到这些信息后购买了委托方的商品的人数，或者向委托方提供不能识别个人身份的统计信息，以帮助其了解受众或顾客。

(6) 某些营销活动可能由我们与第三方联合举办（您可以在具体活动规则相关页面中查看第三方合作机构的名称），只有将您参与活动过程中产生的、为完成活动所必要的信息共享给第三方时，才能及时与您联系、发放奖品、提供服务，我们会依据法律法规或国家标准的要求，在活动规则页面或通过其他途径向您明确告知需要向第三方提供何种个人信息。

(7) 分析服务类的合作方。除非得到您的许可，否则我们不会将您的个人信息（指可以识别您身份的信息，例如姓名）与提供分析服务的合作伙伴分享。

(8) 提供技术服务的第三方 SDK 提供商。

#### 4.2.2. 法律法规规定

我们可能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。

#### 4.3. 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、在获得您的明确同意后，我们会向其他方转让您的个人信息；

2、根据适用的法律法规、法律程序的要求、强制性的行政或司法要求所必须进行提供；

3、在涉及合并、收购或破产清算时，如涉及到个人信息转让，我们会在要求新的持有您个人信息的公司、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。

#### 4.4. 公开披露

我们仅会在以下情况下，且采取符合业界标准的安全防护措施的前提下，才会公开披露您的个人信息：



1、获得您的明确同意后，按您明确同意的披露方式披露您所指定的个人信息；

2、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，我们可能会公开披露您的个人信息。在符合法律法规的前提下，当我们收到上述披露信息的请求时，我们会要求必须出具与之相应的法律文件，如传票或调查函。我们坚信，对于要求我们提供的信息，应该在法律允许的范围内尽可能保持透明。我们对所有的请求都进行了慎重的审查，以确保其具备合法依据，且仅限于执法部门因特定调查目的且有合法权利获取的数据。

#### 4.5. 共享、转让、公开披露个人信息时事先征得授权同意的例外

根据相关法律法规及国家标准，以下情形中，我们共享、转让、公开披露您的个人信息不必事先征得您的授权同意：

1、与您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、与刑事侦查、起诉、审判和判决执行等直接相关的；

5、出于维护您或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；

6、您自行向社会公众公开的个人信息；

7、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。

## 5. 我们如何保护您的个人信息

### 5.1. 我们保护您个人信息的技术与措施

我们非常重视个人信息安全，并采取一切合理可行的措施，保护您的个人信息：

#### 5.1.1. 数据安全保护措施

我们已采用符合业界标准的安全防护措施以及行业内通行的安全技术来防止您的

个人信息遭到未经授权的访问、修改，避免您的个人信息泄露、损坏或丢失：

(1) 采取加密技术对您的个人信息进行加密存储，从安全管理、策略、过程、网络体系结构等诸多方面保障交易及个人信息安全。

(2) 我们的网络服务采取了传输层安全协议等加密技术，通过 **https** 等方式提供浏览服务，确保您的个人信息在传输过程中的安全。

(3) 在使用您的个人信息时，例如个人信息展示、个人信息关联计算，我们会采用包括内容替换、**SHA256** 在内的多种数据脱敏技术增强个人信息在使用中的安全性。

### 5.1.2. 为保护个人信息采取的其他安全措施

我们通过建立数据分类分级、数据安全管理制度、安全开发规范来管理规范个人信息的存储和使用：

(1) 我们采用严格的数据访问权限和多重身份认证技术控制和保护个人信息，通过与信息接触者签署严格的保密协议、监控和审计机制来对数据进行全面安全控制，避免数据被违规使用。

(2) 我们采用代码安全检查、数据访问日志分析技术进行个人信息安全审计。

(3) 我们建立了信息安全委员会并下设信息安全小组，由各小组信息安全专员负责个人信息安全事务。

(4) 我们还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。

### 5.1.3. 安全事件处置

(1) 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。

(2) 为应对个人信息泄露、损毁和丢失等可能出现的风险，我们制定了多项制度，明确安全事件、安全漏洞的分类分级标准及相应的处理流程。我们为安全事件建

立了专门的应急响应团队，按照安全事件处置规范要求，针对不同安全事件启动安全预案，进行止损、分析、定位、制定补救措施、联合相关部门进行溯源和打击。

(3) 一旦发生个人信息安全事件，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、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。我们同时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，难以逐一告知个人信息主体时，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，主动上报个人信息安全事件的处置情况。

## 5.2. 我们如何存储和保存您的个人信息

1、我们仅在本政策所述目的所必需期间和法律法规及监管规定的时限内保存您的个人信息。我们承诺为了保证您的消费者权益，除非法律法规另有规定，您的个人信息我们将保存至您账号注销之日后的一个月。当您的个人信息超出我们所保存的期限后，我们会对您的个人信息进行删除或匿名化处理。

2、在您终止使用我们的服务后，我们会停止对您的信息的收集和使用，法律法规或监管部门另有规定的除外。如果我们终止服务或运营，我们将及时停止收集您个人信息的活动，至少提前三十天通知您，并在终止服务或运营后对您的个人信息进行删除或匿名化处理。

## 6. 您的权利

我们非常重视您对个人信息的关注，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，尽全力保障您对自己的个人信息行使以下权利：

### 6.1. 访问您的个人信息

1、您有权随时访问您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过自行访问：

2、对于您在使用我们的产品或服务过程中产生的其他个人信息，只要我们不需投入过多投入，我们会向您提供。

### 6.2. 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，您有权要求我们作出更正。如

您发现您的信息有误，您可以通过以下方式自行更正：

- 1、在医为医生 APP “首页—我的-设置-修改手机号” 可以修改您的手机号。

### 6.3. 删除您的个人信息

在以下情形中，您可以驻场服务人员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，或您注销了医为账户；
- (5) 如果我们不再为您提供产品或服务。

收到您的删除请求后，我们会根据您及相关法律法规的要求进行后续删除处理并向您反馈结果。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。

- 2、当您从我们的服务中删除信息后，我们可能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。

### 6.4. 改变您授权同意的范围或撤回您的授权

- 1、如果您希望关闭您之前已开启的敏感权限，您可以在 APP 中进行自主设置。

请您理解，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”），当您撤回同意或授权后，我们无法继续为您提供撤回同意或授权所对应的服务，也不再处理您相应的个人信息。但您撤回同意或授权的决定，不会影响此前基于您的授权而开展的个人信息处理。

### 6.5. 注销您的账户

您可以联系驻场人员发起申请，我们会对您的注销账户申请进行处理。

## 6.6. 设备权限调用说明

### 6.6.1. 系统敏感权限

在您使用我们的产品和服务时，我们可能需要向您申请下列与个人信息相关的系统敏感权限：

1、相册权限：当您使用医为系院内移动应用中的头像设置、多媒体上传等服务时，您可以通过开通相册权限以便上传设备中的图片或视频。若您不开启此权限，您将无法使用图片或视频上传相关的功能，但不影响您使用其他服务。

2、相机权限：当您使用医为系院内移动应用中的头像设置、多媒体上传、图像识别等服务时，您可以通过开通相机权限以便进行实时拍摄并上传图片或视频。在需要人脸识别的场景下，则需要调用您的摄像头进行人脸的拍摄。若您不开启此权限，您将无法使用图片或视频拍摄相关的功能，但不影响您使用其他服务。

3、麦克风权限：当您使用医为系院内移动应用中的语音录制、语音输入、视频通话等服务时，您可以开启麦克风权限点击语音按钮进行录音，以便我们收集您的语音内容并进行必要的处理。若您不开启此权限，您将无法使用语音输入相关的功能，但不影响您使用其他服务。

4、定位权限：当您使用医为系院内移动应用中的医嘱录入、诊疗问诊等服务时，您可以开启定位权限，以便我们收集您的位置并进行必要的处理。若您不开启此权限，您可能无法使用医嘱录入、诊疗问诊等相关的功能，但不影响您使用其他服务。

### 6.6.2. 权限和使用目的

上述扩展功能可能需要您在您的设备中向我们开启您的相机（摄像头）、相册（图片库）、电话状态、外部存储、麦克风，以实现这些功能所涉及的信息的收集和使用。您可以在医为系院内移动应用或设备系统中逐项查看您上述权限的开启状态，并可以决定将这些权限随时的开启或关闭（我们会指引您在您的设备系统中完成设置）。请您注意，您开启这些权限即代表您授权我们可以收集和使用这些个人信息来实现上述的功能，您关闭权限即代表您取消了这些授权，则我们将不再继续收集和使用您的这些个人信息，也无法为您提供上述与这些授权所对应的功能。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的处理。除此以外，我们在相关业务功能中可能还需要您开启设备的其他访问权限。

我们申请获取的权限将与提供的服务功能保持一致，若我们提供的业务功能调整，我们申请的权限也将随之调整。我们会在首次调用设备权限时会单独提示您是否开启并对权限申请目的进行解释。请您注意，您开启这些权限即代表您授权我们可以收集和使用这些个人信息来实现上述的功能，您关闭权限即代表您取消了这些授权，则我们将不再继续收集您的这些个人信息，也无法为您提供上述与这些授权所对应的功能。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的处理。

## 7. 我们如何处理儿童的个人信息保护

1、我们非常重视对儿童个人信息的保护。我们的产品与/或服务仅面向成人。对于经父母或其他法定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、父母或其他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。

2、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，或儿童的父母或其他监护人撤回其同意的，则会设法尽快删除相关数据。

## 8. 本政策中关键词定义

### 8.1. “医为系院内移动应用”

指医为医生、院长日报、移动医疗

### 8.2. “个人信息”

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。本定义出自于 GB/T 35273-2020《信息安全技术 个人信息安全规范》，以下为个人信息示例（非本政策所收集的个人信息，仅作参考说明）

个人信息举例

个人基本信息 个人姓名、生日、性别、民族、国籍、家庭关系、地址、个人电话号码、电子邮箱等

个人身份信息 身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等

个人生物识别信息 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等

网络身份标识信息 个人信息主体账号、IP 地址、个人数字证书等

个人健康生理信息 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等

个人教育工作信息 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等

个人财产信息 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息

个人通信信息 通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等

联系人信息 通讯录、好友列表、群列表、电子邮件地址列表等

个人上网记录 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等

个人常用设备信息 指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息

个人位置信息 包括行踪轨迹、精准定位信息、住宿信息、经纬度等

其他信息 婚史、宗教信仰、性取向、未公开的违法犯罪记录等

### 8.3. “个人敏感信息”

“个人敏感信息”是指一旦泄露、非法提供或滥用可能危害人身或财产安全，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。本定义出自于 GB/T 35273-2020《信息安全技术 个人信息安全规范》，以下为个人敏感信息示例（非本政策所收集的个人信息，仅作参考说明）

## 个人敏感信息举例

个人财产信息 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息

个人健康生理信息 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等

个人生物识别信息 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等

个人身份信息 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等

其他信息 性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

**更新日期：2022 年 5 月 20 日**

**生效日期：2022 年 5 月 20 日**