平安健康信息安全及数据安全管理政策声明

随着信息系统与数据规模的不断扩大，在国家《网络安全法》、《数据安全法》、《个人信息保护法》的法律要求下，严格的信息安全及数据安全管控将成为平安健康实现平稳可持续发展的重要保障。

平安健康严格遵循并执行各项法律法规，根据市场监管变化、技术的更新以及行业最佳实践的不断变革，在技术和管理层面持续优化提升公司信息安全及数据安全工作，制定最新版信息安全管理体系制度，包含信息安全方针、信息安全策略、信息安全标准、信息安全基线（通常适用于 IT 系统）、指引五大类管理制定，制定最新版的数据安全管理体系制度包含数据安全管理制度、数据全生命周期安全管理制度、数据安全管理体系运行制度三大类管理制度，并适用于平安健康所有相关业务线和子公司。

信息安全及数据安全管理制度每年经过内部及外部认证、审计机构进行评估，以上各项管理规范适用于平安健康及分子公司的所有部门和员工、以及能够接触信息资产的第三方人员，将指引平安健康实践信息安全及数据安全的管理。

一、信息安全保护

（一）信息安全保护原则

l 严格遵循国家法律、监管机构法规及行业常规和守则的信息安全要求，并以最高标准作为规范原则；

l 公司信息资产必须受到适当的保护，确保信息的保密性、完整性和可用性；

l 构建信息及信息系统，以深度防御及默认安全作为实施原则；

l 公司信息及信息系统所建立的保护，与其敏感程度、价值大小以及重要性相匹配。

（二）信息安全管理体系

平安健康主要系统已获得中国网络安全等级保护三级认证，平安健康已获得 ISO27001/27701/27799 信息及隐私安全管理体系标准认证，平安健康 APP 已获得中国信通院健康医疗大数据可信选型评估认证证书。

为规范和指导员工相关操作，有效提高信息安全风险控制能力，根据 ISO27001/27701/27799 相关标准，平安健康制定了完善的信息安全政策和制度，主要涉及信息安全总纲、资产安全、运维安全、网络安全、人员安全、应急处理预案等安全相关的各个方面，共计 30 多项制度（见《附：信息安全管理制度列表》），形成以围绕安全管理、安全运营、安全技术三大控制领域为核心的平安健康信息安全管理体系分别包含以下控制原则的信息安全保护：

1、资产安全

所有信息资产，包括著述、口述、及电子信息，都应该根据其敏感性、重要程度以及业务所要求的访问限制原则进行分类和标识。

所有与信息相关的重要资产都将在资产清单中标出，并及时维护更新。

2、安全组织及人员安全

所有工作岗位必须有安全职责描述，并且说明岗位的敏感性。

员工在入职前必须通过背景调查，并签订保密协议，人员岗位发生变化或离司时，必须执行相关程序，确保信息资产保护不受影响。

违反信息安全规范的人员将根据平安健康内部处罚规定处理。

在信息安全意识宣导上，平安健康每年都对所有员工、外包人员及承包商开展网络安全、数据安全、客户隐私等主题培训，全面加强员工的信息与数据安全保护意识及能力。

3、访问控制

所有行为必须被记录，可追溯至负责的执行者；非授权的行为要进行适当的处理。

用户在访问信息和信息系统之前，需要进行身份认证，认证方式与信息的敏感性及风险程度相适应。

遵循权限最小化原则，仅面向系统用户开通业务所需必要的最小权限，并设定访问权限的最小有效期，定期清理权限。

信息资产必须按照信息分类做出合适的保护。绝密、机密信息发放必须有业务需要的依据。

信息资料必须防止被非授权篡改或者删除。

4、应用系统开发安全

在应用系统开发、发布、更新过程中，实施安全规范。电子商务应用系统的开发确保客户信息在公共网络环境中的保密性及完整性，并确保交易的不可否认性。

所使用的加密算法必须达到数据保护的原则，包括：

- 达到保护数据的保密性、完整性、认证性及不可抵赖性的要求；
- 选用的加密运算必须公开论证；
- 加密密钥在整个密钥生命周期中必须妥善管理。

对重要业务系统采用如双因子认证等强身份认证手段，严格遵行“知其必须”的权限管理原则防止内部数据窃取行为的发生；同时，采用先进的技术手段加强系统日志审计，追踪、发现数据泄露行为。

5、业务连续性

平安健康制定并完善适用于平安健康所有相关业务线及各分子公司、以及能接触到信息资产的第三方人员的制度文件，开展对业务连续性及业务运营风险相关因素的识别工作，并从危机发生前、危机中、危机发生后的过程中制定了相应的应对机制与危机应对和业务连续性管理方案，结合培训、训练等多种方式确保业务连续性。我们的危机和业务连续性管理流程同时覆盖了自身业务运营范围与供应链。平安健康建立了适当防范措施，确保信息能够提供给授权的使用方。当原始信息破坏或者丢失时，提取最近的备份信息以实现业务对于数据使用的连续性。

6、合规

平安健康严格遵循国家法例、监管机构法规、行业常规和守则的信息安全要求，以各要求中的最高规范为实施原则，按照法律、法规、合同要求，保护客户信息及隐私，保障业务系统及网络安全。

7、第三方服务管理

在信息领域，平安健康与合作伙伴有着深入的合作。针对第三方的服务管理，平安健康制定了明确的管理条例和合作协议，以确保采购、合作符合国家相关管理部门的规定。

8、内容安全

为维护良好的网络传播秩序和清朗的网络环境，平安健康建立互联网信息内容安全审核机制，遵循“先审后发”原则，确保信息内容合法、准确、真实。

9、风险管理及事件响应

平安健康识别和评估信息安全风险，及时响应和处理信息安全事件，保障信息资产以及各项业务的安全稳定运行。

10、安全防护

重大网络及操作系统必须在适当的时间内进行重要补丁，新构建的操作系统必须配置最新的补丁。

所有服务器、工作台及其他设备必须安全防病毒、防侦察软件，及时升级防病毒系统、更新病毒库，防止被恶意代码攻击。

全公司采取了员工上网行为管理、打印控制、文档加密、水印跟踪等一系列的行为控制和安全防护手段。

11、安全区域边界

根据网络区域的不同，在网络边界部署相应的访问控制机制，设置访问控制规则。

对网络性能、流程、非法接入等行为进行监控，异常情况及时处理和上报。

12、网络通信安全

所有连接到平安健康网络的线路，均采取适当的安全措施，以保护内网、信息系统以及网络传输中信息的安全。

13、物理及环境安全

平安健康采取了严格的物理安全防范措施，以防止信息资产与信息系统在未经授权下收到物理访问、破坏或者干扰。针对火灾、水灾、骚乱等天灾、意外或者人为灾难对信息设备的影响，设计和实施了相对应的物理环境保护措施。

附：信息安全管理制度列表

《信息安全与数据安全管理委员会工作章程》
《信息安全管理制度（2023 版）》
《信息安全标准-方针》
《信息安全标准-策略》
《信息安全标准-可用性》
《信息安全标准-完整性》
《信息安全标准-资产安全》
《信息安全标准-风险管理》
《信息安全标准-安全组织》
《信息安全标准-人员安全》
《信息安全标准-物理环境安全》
《信息安全标准-授权》
《信息安全标准-认证》
《信息安全标准-安全监控》
《信息安全标准-安全防护》
《信息安全标准-安全通信》
《信息安全标准-安全区域边界》
《信息安全标准-安全运维》
《信息安全标准-加密算法》
《信息安全标准-第三方服务安全管理》
《信息安全标准-数据全生命周期管理》

《信息安全标准-应用系统开发》
《信息安全标准-个人信息保护》
《信息安全标准-合规》
《信息安全标准-内容安全》
《应用系统账号权限指引》
《应用程序接口安全管理办法》
《外部咨询顾问信息安全管理办法》
《信息安全事件应急管理办法》
《终端安全管控策略实施细则》
《信息安全基线》

二、数据安全保护

自 2021 年《中华人民共和国数据安全法》实施以来，随着客户权益、社会责任、公司业务发展和日常经营等外部内部两大驱动下，公司建立数据安全管理体系，包含数据安全策略、数据安全管理、数据安全支撑、数据安全监督四个层面，以保障业务和日常应景合法合规，提升业务竞争力和品牌形象。

数据安全策略层面包括数据安全发展和策略，开展数据安全文化建设。

数据安全管理层面包括构建数据安全组织、制定数据据安全制度、实施贯穿数据全生命周期的事前/事中/事后安全措施。建立围绕数据生命周期的风险管理机制。

数据安全支撑层面包括依靠以流程机制、技术平台为主的管理和技术手段，推动和促进数据安全要求的落地，提供人员和预算相关资源，开展数据安全宣传和人员培训，实施奖惩，组织公司内外部之间的沟通和交流。

数据安全监督层面包括通过监控和审计对执行过程和效果进行监督，并对数据安全水平的 达成实施考核和度量。

（一）数据安全管理原则

- 合法合规原则：与数据相关的活动符合法律法规、规章制度和监管要求；
- 最小化原则：与数据相关的活动中所涉及的数据和权限仅能满足该活动所需，并将在规定的时间后删除数据，并且不从第三方收集个人数据（法律要求的除外）；
- 数据保密性、完整性、可用性原则：确保数据不被提供或泄漏给非授权的人员、过程或实体；确保数据准确和完整，不被篡改和删除；确保授权使用数据的实体可以在需要时访问和使用数据；
- 安全审计原则：对数据活动中的操作进行记录并对日志实施严格的保护措施，确保所有操作可以被追溯和审计；实施日志审查和分析；
- 责任不随数据转移原则：数据所有者对数据负责，当数据转移给其他单位时，责任不随数据转移而转移；
- 人人有责原则：公司全体人员，包括员工和第三方员工，必须遵守国家法律法规，并承担法律责任；全体人员都有责任保护数据的安全性，必须理解并执行公司数据安全相关规定，任何违反规定的人员将受到处罚，情节严重时将移交司法机关；
- 持续性原则：数据安全管理过程是计划、执行、检查、调整不断循环深入的过程，建立长效机制，持续推进。

（二）数据安全管理体系

平安健康已获得中国工信部 TLC 数据安全管理能力认证证书，并结合国内外数据安全管理合规要求及行业最佳实践，平安健康围绕数据全生命周期安全为数据安全管理核心，制定数据安全管理体政策及管理制度，共计 30 多项，（见《附：数据安全及个人信息保护管理制度列表》）实施数据安全管理体系的有效运行，分别包含以下控制原则的数据安全保护：

1、数据分类分级

明确了数据分类分级依据的标准、操作流程、相关职责、形成了分类分级模板和清单。

结合数据安全要求和数据特征，对公司数据进行数据分类分级，建立统一的分类方法，所有数据必须按照数据分级要求进行分级和定级处理，并基于数据分级情况，实现数据分级访问管控。

2、数据安全组织

平安健康建立了层级化数据安全组织架构，明确数据安全相关职责。

建立公司与内外部组织和监管机构的沟通机制。

在员工的雇佣前、雇佣中、雇佣终止阶段分别进行管理，确保与所有员工签署保密协议，雇佣中员工受公司数据安全要求的约束。

开展数据安全方面的意识培训，保证公司人员充分理解数据安全要求，提升员工数据安全保护意识。

3、数据收集安全

平安健康在进行数据收集时，满足以下安全要求：

- 确保数据收集行为和数据来源合法合规；
- 在数据收集前获得授权，且仅收集业务开展和公司经营所需的数据；
- 明确数据收集相关方的责任、义务和权利；
- 采取必要的技术手段和管理措施确保数据的保密性、完整性和可用性；
- 确保数据收集过程可追溯、可审计。

4、数据传输安全

平安健康在数据传输过程中，满足以下安全要求：

- 满足最小化原则，并在数据传输前获得充分授权；
- 在数据的网络传输和物理传输中，根据传输过程中数据面临的威胁和数据分类分级情况，指定数据传输安全方案，确保数据的保密性和完整性；
- 对数据传输过程进行记录，确保传输过程可追溯。

5、数据存储安全

平安健康在数据存储方面，满足以下安全要求：

- 根据知悉需要和最小化原则，确定数据存储的访问权限、访问方式和审批手段；
- 根据存储过程中数据面临的威胁和数据分类分级情况，指定数据传输安全方案，确保数据的保密性和完整性和可用性；
- 对数据存储、授权、使用过程进行记录，确保数据存取过程可追溯；
- 数据保存期限符合国家法律法规、规章制度和监管要求。

6、数据使用安全

平安健康在数据使用方面，满足以下安全要求：

- 符合国家法律法规、规章制度和监管要求，对数据使用的目的进行限制；
- 数据使用遵循最小化原则；

l 识别数据在访问、计算分析、修改等使用场景中面临的风险，实施数据脱敏、访问控制、操作规范、记录操作日志等安全措施。

7、数据交换安全

平安健康在数据交换方面，满足以下安全要求：

l 数据交换符合法律法规、规章制度和监管要求，维护数据主题的合法权益；

l 在数据交换前获得充分的授权审批；

l 数据交换遵循正当、必要、最小化原则；

l 进行数据脱敏、数据加密、安全通道等安全措施，对数据使用进行审计和监控。

8、数据销毁安全

平安健康在数据销毁方面，满足以下安全要求：

l 采取必要的数据销毁技术手段和安全措施，确保销毁数据后无法实现实质性的数据重读或重组；

l 建立销毁审批机制，指定操作规范，实施数据销毁监督、记录和核查，保障数据销毁过程安全。

9、合作方数据安全管理

平安健康在开展与合作方的业务合作过程中，满足以下安全要求：

合作前，验证合作方数据安全管理和数据安全技术能力，要求合作方提供客观评价的资质、安全证书材料。

与合作方签订数据合作合同，明确合作双方数据保护义务和责任，阐明合作场景、合作方式、违约责任等。

合作中对合作方采取台账记录并动态监测合作方安全事件舆情、合作安全风险，并针对重要合作方定期开展安全审查工作。

10、数据权限审批管理

平安健康在数据访问权限管理方面，满足以下要求：

制定不同秘密级别数据权限申请时的具体规范要求和具体申请审批流程。

定期核查数据权限，并定期清理不再适用的、非开展业务所必要最小的用户数据权限。

11、数据安全投诉举报管理

平安健康对外向用户提供清晰、便捷的投诉渠道，对内明确规范数据安全投诉举报管理、处置机制、具体处置流程和内部惩处措施。

12、数据安全应急管理

平安健康为数据安全事件的处置，建立事件应急响应处置机制，针对不同数据安全事件维度和场景，建立对应的应急响应预案，明确处置各关节具体责任人和各环节处置流程，并开展应急预案演练，不断优化预案及响应处置流程。

附：数据安全及个人信息保护管理制度列表

《数据安全管理体系管理制度》

《数据安全管理手册》

《数据安全标准-数据分类分级规范》

《数据安全标准-组织和角色管理规范》

《数据安全标准-数据收集安全规范》

《数据安全标准-业务规划与管理规范》

《数据安全标准-数据传输安全规范》

《数据安全标准-数据存储安全规范》
《数据安全标准-数据交换安全规范》
《数据安全标准-数据使用安全规范》
《数据安全标准-数据销毁安全规范》
《数据安全标准-遵从性规范》
《数据分类分级-参考目录》
《数据安全标准-合作方数据安全管理规范》
《数据安全标准-数据安全风险自评估管理规范》
《数据安全标准-数据安全管理审计规范》
《数据安全标准-数据安全教育培训管理规范》
《数据安全标准-数据安全举报投诉管理规范》
《数据安全标准-数据安全事件应急响应规范》
《数据安全标准-数据权限审批管理规范》
《对外数据交换安全管理办法》
《对外数据交换管理指引》
《敏感信息展示屏蔽及下载管理办法》
《数据库安全管理办法》
《应用日志去敏感信息指引》
《应用系统员工行为操作埋点指引》
《个人信息保护政策管理指引》
《个人信息收集管理指引》
《个人行权操作管理指引》
《个人信息删除管理指引》
《个人信息对外传输管理指引》
《APP 隐私权限开发指引》
《生物特征识别安全指引》
《个人信息影响评估指引》
《应用软件（含 APP）个人信息安全合规指引》

平安健康隐私保护政策声明

一、个人信息保护承诺

平安健康采取各种安全技术及配套的管理体系来保证客户的个人信息不会被泄露、毁损、误用、非授权访问、非授权披露和更改，以实现平安健康对个人信息保护的承诺。平安健康将遵守所有关于个人信息保护的法规要求。

二、个人用户隐私政策

平安健康对提供的产品或者服务制定有专门的用户隐私政策。希望可以通过专门的用户隐私政策了解平安健康对用户的个人信息的收集、使用和披露方式。在用户使用相应的产品或者服务时，这些专门的用户隐私政策将优先适用。目前，平安健康面向用户专门的隐私政策为：《平安健康会员隐私政策》。

三、个人信息保护基本原则

平安健康开展个人信息处理活动遵循合法、正当、必要、诚信、公开、透明、安全的原则，具体包括：

丨个人合法正当：遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息；

丨目的明确：具有明确、清晰、具体的个人信息处理目的；

丨选择同意：向个人明示个人信息处理目的、方式、范围、规则等，征求其授权同意；

丨最小必要：只处理实现处理目的的最小范围的个人信息；

丨公开透明：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督；

丨保障安全：具备与所面临的安全风险匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性和可用性。

四、个人信息收集原则

平安健康用户的个人信息，仅能由公司来收集，员工以公司名义收集个人信息时必须出示足够的公司授权证明，除法律要求外，不会主动从第三方收集用户个人信息。

个人信息收集在遵循个人保护基本原则外，还必须遵守以下规则：

丨合法合规原则：确保数据收集符合法律法规、规章制度和监管要求；

丨职责明确原则：明确数据收集相关方的责任、义务和权利；

丨数据最小化原则：仅收集义务开展和公司经营所需的数据；

丨主动明示原则：收集信息前，需要用户主动同意授权收集；

丨先告知后收集原则：收集信息前，需征得用户同意后，方可收集。

五、个人信息对外提供

平安健康及其合作伙伴负有保密义务,不会主动共享、转让、出租或出售个人信息至第三方，不会出于完成交易/服务以外的目的向第三方出租、出售或提供个人数据。如存在该情形时，平安健康会向个人信息主体告知使用目的、数据类型并征得明示授权同意。平安健康向合作方提供其处理的个人信息，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

在共享用户的个人信息之前以及共享的过程中，我们将充分评估该等共享的合法性、正当性、必要性，并采用适当的管理措施与技术措施，以保障用户的个人信息安全。平安集团关联公司如果想要改变隐私政策声明的个人信息使用目的，将再次征求用户的授权同意。

六、用户个人权利

按照国家相关的法律、法规、标准，以及其他国家、地区的通行做法，平安健康保障用户对自己的个人信息行使以下权利：

丨访问或要求我们提供在产品和服务使用过程中提供、产生的账户信息、搜索信息及其他个人信息；

丨要求我们更正不准确的用户个人信息；

丨满足特定情形，要求我们删除用户个人信息；

丨随时给予或收回用户对于个人信息收集和使用的授权同意；

丨注销用户个人账户；

丨获取用户的个人信息副本。

平安健康的各项产品和服务都提供了针对个人信息内容的查询、修改、沟通、投诉等通道，客户可通过其访问、管理个人信息，行使用户权利。用户隐私政策的修订、更新会及时通知用户，并向用户重新取得授权同意。

七、儿童个人信息保护

平安健康的产品和服务主要面向成年人，但我们同样非常重视儿童及未成年人个人信息的保护。若客户为儿童但没有获得父母或监护人的同意，儿童不得创建自己的用户账户。对于经父母或者监护人同意而处理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。

平安健康尊重并保护所有客户的隐私权，在保证可用性的基础上严格执行内部的规范文件，并及时根据国家的相关法律法规修订隐私保护规范，承担企业责任，实现可持续发展。

八、个人信息的删除

平安健康仅在为提供产品及服务之目的所必须的最短期间内保存用户的个人信息。超出必要期限后，将对用户的个人信息进行删除或匿名化处理，且不从第三方收集个人数据，遵循以下法律法规另有规定的除外：

- 对于用户的问诊相关信息，我们会在用户注销其账户后继续保存 15 年；
- 对于用户在我们平台上购买的商品和服务信息、交易信息，我们会在用户注销其账户后继续保存 3 年；
- 除法律另有规定外，对于用户的其他信息，我们会在用户注销其账户时同步删除。