平安健康資訊安全及數據安全管理政策聲明

隨著資訊系統與數據規模的不斷擴大，在國家《網路安全法》、《數據安全法》、《個人資訊保護法》的法律要求下，嚴格的資訊安全及數據安全管控將成為平安健康實現平穩可持續發展的重要保障。

平安健康嚴格遵循並執行各項法律法規，根據市場監管變化、技術的更新以及行業最佳實踐的不斷變革，在技術和管理層面持續優化提升公司資訊安全及數據安全工作，制定最新版資訊安全管理體系制度，包含資訊安全方針、資訊安全策略、資訊安全標準、資訊安全基線（通常適用於 IT 系統）、指引五大類管理制定，制定最新版的數據安全管理體系制度包含數據安全管理制度、數據全生命週期安全管理制度、數據安全管理體系運行制度三大類管理制度，並適用於平安健康所有相關業務線和子公司。

資訊安全及數據安全管理制度每年經過內部及外部認證、審計機構進行評估，以上各項管理規範適用於平安健康及分子公司的所有部門和員工、以及能夠接觸資訊資產的第三方人員，將指引平安健康實踐資訊安全及數據安全的管理。

一、資訊安全保護

（一）資訊安全保護原則

l 嚴格遵循國家法律、監管機構法規及行業常規和守則的資訊安全要求，並以最高標準作為規範原則；

l 公司資訊資產必須受到適當的保護，確保資訊的保密性、完整性和可用性；

l 構建資訊及資訊系統，以深度防禦及默認安全作為實施原則；

l 公司資訊及資訊系統所建立的保護，與其敏感程度、價值大小以及重要性相匹配。

（二）資訊安全管理體系

平安健康主要系統已獲得中國網路安全等級保護三級認證，平安健康已獲得 ISO27001/27701/27799 資訊及隱私安全管理體系標準認證，平安健康 APP 已獲得中國信通院健康醫療大數據可信選型評估認證證書。

為規範和指導員工相關操作，有效提高資訊安全風險控制能力，根據 ISO27001/27701/27799 相關標準，平安健康制定了完善的資訊安全政策和制度，主要涉及資訊安全總綱、資產安全、運維安全、網路安全、人員安全、應急處理預案等安全相關的各個方面，共計 30 多項制度（見《附：資訊安全管理制度列表》），形成以圍繞安全管理、安全運營、安全技術三大控制領域為核心的平安健康資訊安全管理體系分別包含以下控制原則的資訊安全保護：

1、資產安全

所有資訊資產，包括著述、口述、及電子資訊，都應該根據其敏感性、重要程度以及業務所要求的訪問限制原則進行分類和標識。

所有與資訊相關的重要資產都將在資產清單中標出，並及時維護更新。

2、安全組織及人員安全

所有工作崗位必須有安全職責描述，並且說明崗位的敏感性。

員工在入職前必須通過背景調查，並簽訂保密協議，人員崗位發生變化或離司時，必須執行相關程式，確保資訊資產保護不受影響。

違反資訊安全規範的人員將根據平安健康內部處罰規定處理。

在資訊安全意識宣導上，平安健康每年都對所有員工、外包人員及承包商開展網路安全、數據安全、客戶隱私等主題培訓，全面加強員工的資訊與數據安全保護意識及能力。

3、訪問控制

所有行為必須被記錄，可追溯至負責的執行者；非授權的行為要進行適當的處理。

用戶在訪問資訊和資訊系統之前，需要進行身份認證，認證方式與資訊的敏感性及風險程度相適應。

遵循許可權最小化原則，僅面向系統用戶開通業務所需必要的最小許可權，並設定訪問許可權的最小有效期，定期清理許可權。

資訊資產必須按照資訊分類做出合適的保護。絕密、機密資訊發放必須有業務需要的依據。

資訊資料必須防止被非授權篡改或者刪除。

4、應用系統開發安全

在應用系統開發、發佈、更新過程中，實施安全規範。電子商務應用系統的開發確保客戶資訊在公共網路環境中的保密性及完整性，並確保交易的不可否認性。

所使用的加密演算法必須達到數據保護的原則，包括：

- 達到保護數據的保密性、完整性、認證性及不可抵賴性的要求；
- 選用的加密運算必須公開論證；
- 加密密鑰在整個密鑰生命週期中必須妥善管理。

對重要業務系統採用如雙因數認證等強身份認證手段，嚴格遵行“知其必須”的許可權管理原則防止內部數據竊取行為的發生；同時，採用先進的技術手段加強系統日誌審計，追蹤、發現數據洩露行為。

5、業務連續性

平安健康制定並完善適用於平安健康所有相關業務線及各分子公司、以及能接觸到資訊資產的第三方人員的制度檔，開展對業務連續性及業務運營風險相關因素的識別工作，並從危機發生前、危機中、危機發生後的過程中制定了相應的應對機制與危機應對和業務連續性管理方案，結合培訓、訓練等多種方式確保業務連續性。我們的危機和業務連續性管理流程同時覆蓋了自身業務運營範圍與供應鏈。平安健康建立了適當防範措施，確保資訊能夠提供給授權的使用方。當原始資訊破壞或者丟失時，提取最近的備份資訊以實現業務對於數據使用的連續性。

6、合規

平安健康嚴格遵循國家法例、監管機構法規、行業常規和守則的資訊安全要求，以各要求中的最高規範為實施原則，按照法律、法規、合同要求，保護客戶資訊及隱私，保障業務系統及網路安全。

7、第三方服務管理

在資訊領域，平安健康與合作夥伴有著深入的合作。針對第三方的服務管理，平安健康制定了明確的管理條例和合作協議，以確保採購、合作符合國家相關管理部門的規定。

8、內容安全

為維護良好的網路傳播秩序和清朗的網路環境，平安健康建立互聯網資訊內容安全審核機制，遵循“先審後發”原則，確保資訊內容合法、準確、真實。

9、風險管理及事件回應

平安健康識別和評估資訊安全風險，及時回應和處理資訊安全事件，保障資訊資產以及各項業務的安全穩定運行。

10、安全防護

重大網路及操作系統必須在適當的時間內進行重要補丁，新構建的操作系統必須配置最新的補丁。

所有伺服器、工作臺及其他設備必須安全防病毒、防偵察軟體，及時升級防病毒系統、更新病毒庫，防止被惡意代碼攻擊。

全公司採取了員工上網行為管理、列印控制、文檔加密、浮水印跟蹤等一系列的行為控制和安全防護手段。

11、安全區域邊界

根據網路區域的不同，在網路邊界部署相應的訪問控制機制，設置訪問控制規則。

對網路性能、流程、非法接入等行為進行監控，異常情況及時處理和上報。

12、網路通信安全

所有連接到平安健康網路的線路，均採取適當的安全措施，以保護內網、資訊系統以及網路傳輸中資訊的安全。

13、物理及環境安全

平安健康採取了嚴格的物理安全防範措施，以防止資訊資產與資訊系統在未經授權下收到物理訪問、破壞或者干擾。針對火災、水災、騷亂等天災、意外或者人為災難對資訊設備的影響，設計和實施了相對應的物理環境保護措施。

附：資訊安全管理制度列表

《資訊安全與數據安全管理委員會工作章程》
《資訊安全管理制度（2023 版）》
《資訊安全標準-方針》
《資訊安全標準-策略》
《資訊安全標準-可用性》
《資訊安全標準-完整性》
《資訊安全標準-資產安全》
《資訊安全標準-風險管理》
《資訊安全標準-安全組織》
《資訊安全標準-人員安全》
《資訊安全標準-物理環境安全》
《資訊安全標準-授權》
《資訊安全標準-認證》
《資訊安全標準-安全監控》
《資訊安全標準-安全防護》
《資訊安全標準-安全通信》
《資訊安全標準-安全區域邊界》
《資訊安全標準-安全運維》
《資訊安全標準-加密演算法》
《資訊安全標準-第三方服務安全管理》
《資訊安全標準-數據全生命週期管理》

《資訊安全標準-應用系統開發》
《資訊安全標準-個人資訊保護》
《資訊安全標準-合規》
《資訊安全標準-內容安全》
《應用系統帳號許可權指引》
《應用程式介面安全管理辦法》
《外部諮詢顧問資訊安全管理辦法》
《資訊安全事件應急管理辦法》
《終端安全管控策略實施細則》
《資訊安全基線》

二、數據安全保護

自 2021 年《中華人民共和國數據安全法》實施以來，隨著客戶權益、社會責任、公司業務發展和日常經營等外部內部兩大驅動下，公司建立數據安全管理體系，包含數據安全策略、數據安全管理、數據安全支撐、數據安全監督四個層面，以保障業務和日常應景合法合規，提升業務競爭力和品牌形象。

數據安全策略層面包括數據安全發展和策略，開展數據安全文化建設。

數據安全管理層麵包括構建數據安全組織、制定數據據安全制度、實施貫穿數據全生命週期的事前/事中/事後安全措施。建立圍繞數據生命週期的風險管理機制。

數據安全支撐層面包括依靠以流程機制、技術平臺為主的管理和技術手段，推動和促進數據安全要求的落地，提供人員和預算相關資源，開展數據安全宣傳和人員培訓，實施獎懲，組織公司內外部之間的溝通和交流。

數據安全監督層面包括通過監控和審計對執行過程和效果進行監督，並對數據安全水準的 達成實施考核和度量。

（一）數據安全管理原則

- 合法合規原則：與數據相關的活動符合法律法規、規章制度和監管要求；
- 最小化原則：與數據相關的活動中所涉及的數據和許可權僅能滿足該活動所需，並將在規定的時間後刪除數據，並且不從第三方收集個人數據（法律要求的除外）；
- 數據保密性、完整性、可用性原則：確保數據不被提供或洩漏給非授權的人員、過程或實體；確保數據準確和完整，不被篡改和刪除；確保授權使用數據的實體可以在需要時訪問和使用數據；
- 安全審計原則：對數據活動中的操作進行記錄並對日誌實施嚴格的保護措施，確保所有操作可以被追溯和審計；實施日誌審查和分析；
- 責任不隨數據轉移原則：數據所有者對數據負責，當數據轉移給其他單位時，責任不隨數據轉移而轉移；
- 人人有責原則：公司全體人員，包括員工和第三方員工，必須遵守國家法律法規，並承擔法律責任；全體人員都有責任保護數據的安全性，必須理解並執行公司數據安全相關規定，任何違反規定的人員將受到處罰，情節嚴重時將移交司法機關；
- 持續性原則：數據安全管理過程是計畫、執行、檢查、調整不斷迴圈深入的過程，建立長效機制，持續推進。

（二）數據安全管理體系

平安健康已獲得中國工信部 TLC 數據安全管理能力認證證書，並結合國內外數據安全管理合規要求及行業最佳實踐，平安健康圍繞數據全生命週期安全為數據安全管理核心，制定數據安全管理體政策及管理制度，共計 30 多項，（見《附：數據安全及個人資訊保護管理制度列表》）實施數據安全管理體系的有效運行，分別包含以下控制原則的數據安全保護：

1、數據分類分級

明確了數據分類分級依據的標準、操作流程、相關職責、形成了分類分級範本和清單。

結合數據安全要求和數據特徵，對公司數據進行數據分類分級，建立統一的分類方法，所有數據必須按照數據分級要求進行分級和定級處理，並基於數據分級情況，實現數據分級訪問管控。

2、數據安全組織

平安健康建立了層級化數據安全組織架構，明確數據安全相關職責。

建立公司與內外部組織和監管機構的溝通機制。

在員工的雇傭前、雇傭中、雇傭終止階段分別進行管理，確保與所有員工簽署保密協議，雇傭中員工受公司數據安全要求的約束。

開展數據安全方面的意識培訓，保證公司人員充分理解數據安全要求，提升員工數據安全保護意識。

3、數據收集安全

平安健康在進行數據收集時，滿足以下安全要求：

- 確保數據收集行為和數據來源合法合規；
- 在數據收集前獲得授權，且僅收集業務開展和公司經營所需的數據；
- 明確數據收集相關方的責任、義務和權利；
- 採取必要的技術手段和管理措施確保數據的保密性、完整性和可用性；
- 確保數據收集過程可追溯、可審計。

4、數據傳輸安全

平安健康在數據傳輸過程中，滿足以下安全要求：

- 滿足最小化原則，並在數據傳輸前獲得充分授權；
- 在數據的網路傳輸和物理傳輸中，根據傳輸過程中數據面臨的威脅和數據分類分級情況，指定數據傳輸安全方案，確保數據的保密性和完整性；
- 對數據傳輸過程進行記錄，確保傳輸過程可追溯。

5、數據存儲安全

平安健康在數據存儲方面，滿足以下安全要求：

- 根據知悉需要和最小化原則，確定數據存儲的訪問許可權、訪問方式和審批手段；
- 根據存儲過程中數據面臨的威脅和數據分類分級情況，指定數據傳輸安全方案，確保數據的保密性和完整性和可用性；
- 對數據存儲、授權、使用過程進行記錄，確保數據存取過程可追溯；
- 數據保存期限符合國家法律法規、規章制度和監管要求。

6、數據使用安全

平安健康在數據使用方面，滿足以下安全要求：

- 符合國家法律法規、規章制度和監管要求，對數據使用的目的進行限制；
- 數據使用遵循最小化原則；

l 識別數據在訪問、計算分析、修改等使用場景中面臨的風險，實施數據脫敏、訪問控制、操作規範、記錄操作日誌等安全措施。

7、數據交換安全

平安健康在數據交換方面，滿足以下安全要求：

l 數據交換符合法律法規、規章制度和監管要求，維護數據主題的合法權益；

l 在數據交換前獲得充分的授權審批；

l 數據交換遵循正當、必要、最小化原則；

l 進行數據脫敏、數據加密、安全通道等安全措施，對數據使用進行審計和監控。

8、數據銷毀安全

平安健康在數據銷毀方面，滿足以下安全要求：

l 採取必要的數據銷毀技術手段和安全措施，確保銷毀數據後無法實現實質性的數據重讀或重組；

l 建立銷毀審批機制，指定操作規範，實施數據銷毀監督、記錄和核查，保障數據銷毀過程安全。

9、合作方數據安全管理

平安健康在開展與合作方的業務合作過程中，滿足以下安全要求：

合作前，驗證合作方數據安全管理和數據安全技術能力，要求合作方提供客觀評價的資質、安全證書材料。

與合作方簽訂數據合作合同，明確合作雙方數據保護義務和責任，闡明合作場景、合作方式、違約責任等。

合作中對合作方採取台賬記錄並動態監測合作方安全事件輿情、合作安全風險，並針對重要合作方定期開展安全審查工作。

10、數據許可權審批管理

平安健康在數據訪問許可權管理方面，滿足以下要求：

制定不同秘密級別數據許可權申請時的具體規範要求和具體申請審批流程。

定期核查數據許可權，並定期清理不再適用的、非開展業務所必要最小的用戶數據許可權。

11、數據安全投訴舉報管理

平安健康對外向用戶提供清晰、便捷的投訴管道，對內明確規範數據安全投訴舉報管理、處置機制、具體處置流程和內部懲處措施。

12、數據安全應急管理

平安健康為數據安全事件的處置，建立事件應急回應處置機制，針對不同數據安全事件維度和場景，建立對應的應急回應預案，明確處置各關節具體責任人和各環節處置流程，並開展應急預案演練，不斷優化預案及回應處置流程。

附：數據安全及個人資訊保護管理制度列表

《數據安全管理體系管理制度》

《數據安全管理手冊》

《數據安全標準-數據分類分級規範》

《數據安全標準-組織和角色管理規範》

《數據安全標準-數據收集安全規範》

《數據安全標準-業務規劃與管理規範》

《數據安全標準-數據傳輸安全規範》
《數據安全標準-數據存儲安全規範》
《數據安全標準-數據交換安全規範》
《數據安全標準-數據使用安全規範》
《數據安全標準-數據銷毀安全規範》
《數據安全標準-遵從性規範》
《數據分類分級-參考目錄》
《數據安全標準-合作方數據安全管理規範》
《數據安全標準-數據安全風險自評估管理規範》
《數據安全標準-數據安全管理審計規範》
《數據安全標準-數據安全教育培訓管理規範》
《數據安全標準-數據安全舉報投訴管理規範》
《數據安全標準-數據安全事件應急回應規範》
《數據安全標準-數據許可權審批管理規範》
《對外數據交換安全管理辦法》
《對外數據交換管理指引》
《敏感資訊展示遮罩及下載管理辦法》
《資料庫安全管理辦法》
《應用日誌去敏感資訊指引》
《應用系統員工行為操作埋點指引》
《個人資訊保護政策管理指引》
《個人資訊收集管理指引》
《個人行權操作管理指引》
《個人資訊刪除管理指引》
《個人資訊對外傳輸管理指引》
《APP 隱私許可權開發指引》
《生物特徵識別安全指引》
《個人資訊影響評估指引》
《應用軟體（含 APP）個人資訊安全合規指引》

平安健康隱私保護政策聲明

一、個人資訊保護承諾

平安健康採取各種安全技術及配套的管理體系來保證客戶的個人資訊不會被洩露、毀損、誤用、非授權訪問、非授權披露和更改，以實現平安健康對個人資訊保護的承諾。平安健康將遵守所有關於個人資訊保護的法規要求。

二、個人用戶隱私政策

平安健康對提供的產品或者服務制定有專門的用戶隱私政策。希望可以通過專門的用戶隱私政策瞭解平安健康對用戶的個人資訊的收集、使用和披露方式。在用戶使用相應的產品或者服務時，這些專門的用戶隱私政策將優先適用。目前，平安健康面向用戶專門的隱私政策為：《平安健康會員隱私政策》。

三、個人資訊保護基本原則

平安健康開展個人資訊處理活動遵循合法、正當、必要、誠信、公開、透明、安全的原則，具體包括：

l 個人合法正當：遵循合法、正當、必要和誠信原則，不得通過誤導、欺詐、脅迫等方式處理個人資訊；

l 目的明確：具有明確、清晰、具體的個人資訊處理目的；

l 選擇同意：向個人明示個人資訊處理目的、方式、範圍、規則等，徵求其授權同意；

l 最小必要：只處理實現處理目的的最小範圍的個人資訊；

l 公開透明：以明確、易懂和合理的方式公開處理個人資訊的範圍、目的、規則等，並接受外部監督；

l 保障安全：具備與所面臨的安全風險匹配的安全能力，並採取足夠的管理措施和技術手段，保護個人資訊的保密性、完整性和可用性。

四、個人資訊收集原則

平安健康用戶的個人資訊，僅能由公司來收集，員工以公司名義收集個人資訊時必須出示足夠的公司授權證明，除法律要求外，不會主動從第三方收集用戶個人資訊。

個人資訊收集在遵循個人保護基本原則外，還必須遵守以下規則：

l 合法合規原則：確保數據收集符合法律法規、規章制度和監管要求；

l 職責明確原則：明確數據收集相關方的責任、義務和權利；

l 數據最小化原則：僅收集義務開展和公司經營所需的數據；

l 主動明示原則：收集資訊前，需要用戶主動同意授權收集；

l 先告知後收集原則：收集資訊前，需征得用戶同意後，方可收集。

五、個人資訊對外提供

平安健康及其合作夥伴負有保密義務,不會主動共用、轉讓、出租或出售個人資訊至第三方，不會出於完成交易/服務以外的目的向第三方出租、出售或提供個人數據。如存在該情形時，平安健康會向個人資訊主體告知使用目的、數據類型並征得明示授權同意。平安健康向合作方提供其處理的個人資訊，應當向個人告知接收方的名稱或者姓名、聯繫方式、處理目的、處理方式和個人資訊的種類，並取得個人的單獨同意。

在共用用戶的個人資訊之前以及共用的過程中，我們將充分評估該等共用的合法性、正當性、必要性，並採用適當的管理措施與技術措施，以保障用戶的個人資訊安全。平安集團關聯公司如果想要改變隱私政策聲明的個人資訊使用目的，將再次徵求用戶的授權同意。

六、用戶個人權利

按照國家相關的法律、法規、標準，以及其他國家、地區的通行做法，平安健康保障用戶對自己的個人資訊行使以下權利：

l 訪問或要求我們提供在產品和服務使用過程中提供、產生的帳戶資訊、搜索資訊及其他個人資訊；

l 要求我們更正不准確的用戶個人資訊；

l 滿足特定情形，要求我們刪除用戶個人資訊；

l 隨時給予或收回用戶對於個人資訊收集和使用的授權同意；

l 註銷用戶個人帳戶；

l 獲取用戶的個人資訊副本。

平安健康的各項產品和服務都提供了針對個人資訊內容的查詢、修改、溝通、投訴等通道，客戶可通過其訪問、管理個人資訊，行使用戶權利。用戶隱私政策的修訂、更新會及時通知用戶，並向用戶重新取得授權同意。

七、兒童個人資訊保護

平安健康的產品和服務主要面向成年人，但我們同樣非常重視兒童及未成年人個人資訊的保護。若客戶為兒童但沒有獲得父母或監護人的同意，兒童不得創建自己的用戶帳戶。對於經父母或者監護人同意而處理兒童個人資訊的情況，我們只會在受到法律允許、父母或監護人明確同意或者保護兒童所必要的情況下使用或公開披露此信息。

平安健康尊重並保護所有客戶的隱私權，在保證可用性的基礎上嚴格執行內部的規範檔，並及時根據國家的相關法律法規修訂隱私保護規範，承擔企業責任，實現可持續發展。

八、個人資訊的刪除

平安健康僅在為提供產品及服務之目的所必須的最短期間內保存用戶的個人資訊。超出必要期限後，將對用戶的個人資訊進行刪除或匿名化處理，且不從第三方收集個人數據，遵循以下法律法規另有規定的除外：

- 對於用戶的問診相關資訊，我們會在用戶註銷其帳戶後繼續保存 15 年；
- 對於用戶在我們平臺上購買的商品和服務資訊、交易資訊，我們會在用戶註銷其帳戶後繼續保存 3 年；
- 除法律另有規定外，對於用戶的其他資訊，我們會在用戶註銷其帳戶時同步刪除。