Ping An Health Information Security and Data Security Management Policy Statement

With the continuous expansion of information systems and data scale, under the legal requirements of the "Cybersecurity Law of the People's Republic of China," " Data Security Law of the People's Republic of China," and "Personal Information Protection Law of the People's Republic of China," strict information security and data security controls will become a crucial guarantee for Ping An Health to achieve stable and sustainable development.

Ping An Health strictly complies with and implements all relevant laws and regulations. In response to changes in market supervision, technological updates, and continuous evolution of industry best practices, the company continuously optimizes and enhances its information security and data security efforts at both technical and management levels. It has formulated the latest version of the Information Security Management System, which includes five categories of management: Information Security Policy, Information Security Strategy, Information Security Standards, Information Security Baselines (typically applicable to IT systems), and Guidelines. Additionally, the latest version of the Data Security Management System has been established, encompassing three categories: Data Security Management Policies, Data Full Lifecycle Security Management Policies, and Data Security Management System Operation Policies. These apply to all relevant business lines and subsidiaries of Ping An Health.

The information security and data security management policies undergo annual evaluations by internal and external certification and audit organizations. These management standards apply to all departments and employees of Ping An Health and its subsidiaries, as well as third-party personnel who have access to information assets, guiding Ping An Health’s practice of information security and data security management.

I. Information Security Protection

A. Principles of Information Security Protection

l Strictly follow national laws, regulatory requirements, and industry conventions and codes related to information security, adopting the highest standards as normative principles;

l Company information assets must be appropriately protected to ensure confidentiality, integrity, and availability of information;

l Construct information and information systems based on principles of defense in depth and default security;

l The protection established for company information and information systems shall correspond to their sensitivity, value, and importance.

B. Information Security Management System

Ping An Health’s main systems have obtained China’s Cybersecurity Classified Protection Level 3 certification. Ping An Health has also achieved ISO 27001/27701/27799 certifications for information and privacy security management systems. The Ping An Health app has received

the China Academy of Information and Communications Technology (CAICT) Trusted Evaluation Certification for Health and Medical Big Data.

To standardize and guide employee operations and effectively enhance information security risk control capabilities, Ping An Health has developed comprehensive information security policies and systems based on ISO 27001/27701/27799 standards. These cover over 30 policies (see Appendix: Information Security Management Policy List), addressing aspects such as overall information security guidelines, asset security, operation and maintenance security, network security, personnel security, and emergency response plans. The Ping An Health Information Security Management System revolves around three core control areas: security management, security operations, and security technology, implementing the following control principles for information security protection:

1.Asset Security

All information assets—including written, oral, and electronic information—should be classified and labeled according to their sensitivity, importance, and business access control requirements.

All critical information assets must be listed in an asset inventory, which is regularly maintained and updated.

2.Security Organization and Personnel Security

Every job position must have a security responsibility description, including the sensitivity of the role.

Employees must pass background checks before onboarding and sign confidentiality agreements. When personnel change roles or leave the company, relevant procedures must be followed to ensure protection of information assets is not compromised.

Violations of information security policies will be dealt with according to Ping An Health's internal disciplinary rules.

Ping An Health conducts annual cybersecurity, data security, and customer privacy training for all employees, outsourced personnel, and contractors to comprehensively enhance awareness and capabilities in information and data security protection.

3.Access Control

All actions must be logged and traceable to the responsible executor; unauthorized actions must be appropriately handled.

Users must undergo identity authentication before accessing information and information systems, with authentication methods commensurate with the sensitivity and risk level of the information.

The principle of least privilege is followed, granting only the minimal necessary permissions to system users for business needs, with minimal effective duration and periodic permission reviews and cleanups.

Information assets must be protected according to their classification.

Distribution of top-secret and confidential information must be based on business necessity.

Information must be protected against unauthorized modification or deletion.

4.Application System Development Security

Security standards are implemented during application system development, release, and updates. E-commerce application systems ensure confidentiality and integrity of customer information in public network environments and guarantee transaction non-repudiation.

Encryption algorithms used must meet data protection principles, including :

l Confidentiality, integrity, authentication, and non-repudiation;
l Selected encryption algorithms must be publicly vetted;
l Encryption keys must be properly managed throughout their lifecycle.

Important business systems adopt strong authentication methods such as two-factor authentication and strictly enforce the “need-to-know” principle to prevent internal data theft. Advanced technical measures strengthen system log audits to track and detect data leakage.

5.Business Continuity

Ping An Health has established and improved policies applicable to all relevant business lines, subsidiaries, and third parties with access to information assets. It identifies factors related to business continuity and operational risks and has developed corresponding response mechanisms and business continuity management plans covering pre-crisis, crisis, and post-crisis phases. Training and drills ensure business continuity. The crisis and continuity management processes cover both internal operations and supply chains.Appropriate preventive measures ensure information is available to authorized users. When original information is damaged or lost, the most recent backup is restored to maintain business continuity.

6.Compliance

Ping An Health strictly adheres to national laws, regulatory requirements, industry conventions, and codes, implementing the highest standards among these requirements. It protects customer information and privacy and ensures business systems and network security in accordance with legal, regulatory, and contractual obligations.

7.Third-Party Service Management

Ping An Health maintains deep cooperation with partners in the information domain. Clear management regulations and cooperation agreements are established for third-party services to ensure procurement and collaboration comply with relevant national regulatory requirements.

8.Content Security

To maintain a healthy online communication order and a clean network environment, Ping An Health has established an internet content security review mechanism following a “review before release” principle, ensuring information content is lawful, accurate, and truthful.

9.Risk Management and Incident Response

Ping An Health identifies and assesses information security risks, promptly responds to and handles information security incidents, ensuring the security and stable operation of information assets and business activities.

10.Security Protection

Critical networks and operating systems must be patched timely; newly built operating systems must be configured with the latest patches.

All servers, workstations, and other devices must have antivirus and anti-spyware protection, with timely updates of antivirus systems and virus definitions to prevent malware attacks.

The company employs employee internet behavior management, print controls, document encryption, watermark tracking, and other behavioral and security protection measures.

11.Security Zone Boundaries

Appropriate access control mechanisms are deployed at network boundaries according to different network zones, with access control rules set accordingly.

Network performance, processes, and unauthorized access are monitored, with anomalies promptly handled and reported.

12.Network Communication Security

All lines connected to Ping An Health's network adopt appropriate security measures to protect internal networks, information systems, and information during network transmission.

13.Physical and Environmental Security

Ping An Health implements strict physical security measures to prevent unauthorized physical access, damage, or interference to information assets and systems. Physical and environmental protection measures are designed and implemented against natural disasters (fire, flood), riots, accidents, or human-made disasters affecting information equipment.

Appendix: Information Security Management System List

"Charter of the Information Security and Data Security Management Committee"
"Information Security Management Policy (2023 Edition)"
"Information Security Standards – Policy"
"Information Security Standards – Strategy"
"Information Security Standards – Availability"
"Information Security Standards – Integrity"
"Information Security Standards – Asset Security"
"Information Security Standards – Risk Management"
"Information Security Standards – Security Organization"
"Information Security Standards – Personnel Security"
"Information Security Standards – Physical and Environmental Security"
"Information Security Standards – Authorization"
"Information Security Standards – Authentication"
"Information Security Standards – Security Monitoring"
"Information Security Standards – Security Protection"
"Information Security Standards – Secure Communication"
"Information Security Standards – Security Zone Boundaries"
"Information Security Standards – Secure Operations and Maintenance"
"Information Security Standards – Encryption Algorithms"
"Information Security Standards – Third-Party Service Security Management"
"Information Security Standards – Data Full Lifecycle Management"
"Information Security Standards – Application System Development"
"Information Security Standards – Personal Information Protection"
"Information Security Standards – Compliance"
"Information Security Standards – Content Security"
"Application System Account Permission Guidelines"
"API Security Management Measures"
"External Consultant Information Security Management Measures"
"Information Security Incident Emergency Management Measures"
"Terminal Security Control Strategy Implementation Details"

“Information Security Baseline”

II. Data Security Protection

Since the implementation of the "Data Security Law of the People's Republic of China" in 2021, driven by customer rights, social responsibility, business development, and daily operations, the company has established a data security management system comprising four layers: data security strategy, data security management, data security support, and data security supervision, to ensure legal compliance in business and operations, enhance business competitiveness, and improve brand image.

The data security strategy layer includes data security development and strategy, and promotes data security culture construction.

The data security management layer involves building a data security organization, formulating data security policies, and implementing pre-, during-, and post-data lifecycle security measures. It establishes a risk management mechanism centered on the data lifecycle.

The data security support layer relies on process mechanisms and technical platforms to promote the implementation of data security requirements, provide personnel and budget resources, conduct data security publicity and training, implement rewards and penalties, and organize communication and exchanges inside and outside the company.

The data security supervision layer monitors and audits the execution process and effectiveness, conducting assessments and measurements of data security levels.

A. Data Security Management Principles

l Legality and Compliance: All data-related activities comply with laws, regulations, and regulatory requirements;

l Minimization: Data and permissions involved in activities are limited to what is necessary and deleted after a prescribed period; personal data is not collected from third parties unless legally required;

l Confidentiality, Integrity, and Availability: Data must not be disclosed or leaked to unauthorized persons, processes, or entities; data must be accurate and complete, protected against unauthorized alteration or deletion; authorized entities must have access to data when needed;

l Security Auditing: All data operations are logged, with strict protection of logs to ensure traceability and auditability; logs are reviewed and analyzed;

l Responsibility Does Not Transfer With Data: Data owners remain responsible for data even when it is transferred to other units;

l Everyone’s Responsibility: All personnel, including employees and third-party staff, must comply with laws and bear legal responsibility; everyone must protect data security and comply with company data security policies; violations will be punished and may be referred to judicial authorities;

l Continuity: Data security management is a continuous cycle of planning, execution, inspection, and adjustment, establishing long-term mechanisms for ongoing improvement.

B. Data Security Management System

Ping An Health has obtained the Ministry of Industry and Information Technology’s TLC Data Security Management Capability Certification. Combining domestic and international compliance requirements and industry best practices, Ping An Health centers its data security management on the full data lifecycle, formulating data security policies and over 30 management policies (see Appendix: Data Security and Personal Information Protection Management Policy List) to ensure effective operation of the data security management system. The system implements the following data security protection control principles:

1.Data Classification and Grading

Clear standards, operational procedures, and responsibilities for data classification and grading are established, along with classification templates and inventories.

Data is classified and graded uniformly according to security requirements and data characteristics. All data must be classified and graded accordingly, enabling graded access controls based on classification.

2.Data Security Organization

A hierarchical data security organizational structure is established with clearly defined responsibilities.

Communication mechanisms with internal and external organizations and regulatory bodies are maintained.

Employee management during hiring, employment, and termination phases ensures confidentiality agreements are signed and employees are bound by data security requirements.

Data security awareness training is conducted to ensure personnel fully understand and comply with data security requirements, enhancing data protection awareness.

3.Data Collection Security

Data collection must meet the following security requirements:

l Ensure data collection activities and sources are lawful and compliant;

l Obtain authorization before data collection and collect only data necessary for business and company operations;

l Clearly define responsibilities, obligations, and rights of parties involved in data collection;

l Apply necessary technical and management measures to ensure confidentiality, integrity, and availability of collected data;

l Ensure data collection processes are traceable and auditable.

4.Data Transmission Security

Ping An Health adheres to the following security requirements during data transmission:

l Adherence to the principle of least privilege, and obtaining full authorization prior to data transmission.

l Implementing data transmission security solutions for both network and physical data transfers, based on the threats identified during transmission and the data classification/categorization, to ensure data confidentiality and integrity.

l Recording the data transmission process to ensure traceability.

5. Data Storage Security

Ping An Health adheres to the following security requirements for data storage:

l Determining data storage access permissions, access methods, and approval procedures based on the principle of need-to-know and least privilege.

l Implementing data storage security solutions based on the threats identified during storage and the data classification/categorization, to ensure data confidentiality, integrity, and availability.

l Recording data storage, authorization, and usage processes to ensure traceability of data access.

l Ensuring data retention periods comply with national laws, regulations, and supervisory requirements.

6. Data Usage Security

Ping An Health adheres to the following security requirements for data usage:

l Restricting the purpose of data usage in compliance with national laws, regulations, and supervisory requirements.

l Adhering to the principle of least privilege for data usage.

l Identifying risks in data usage scenarios such as access, computational analysis, and modification, and implementing security measures including data de-sensitization, access control, operational guidelines, and logging of operations.

7. Data Exchange Security

Ping An Health adheres to the following security requirements for data exchange:

l Ensuring data exchange complies with laws, regulations, and supervisory requirements, and safeguards the legitimate rights and interests of data subjects.

l Obtaining full authorization and approval prior to data exchange.

l Adhering to the principles of legitimacy, necessity, and least privilege for data exchange.

l Implementing security measures such as data de-sensitization, data encryption, and secure channels, and conducting auditing and monitoring of data usage.

8. Data Destruction Security

Ping An Health adheres to the following security requirements for data destruction:

l Employing necessary data destruction technical means and security measures to ensure that destroyed data cannot be substantially re-read or reconstructed.

l Establishing a destruction approval mechanism, specifying operational guidelines, and implementing supervision, recording, and verification of data destruction to ensure the security of the data destruction process.

9. Partner Data Security Management

When engaging in business collaborations with partners, Ping An Health adheres to the following security requirements:

Prior to collaboration: Verify the partner's data security management and technical capabilities, requiring them to provide objective evaluation qualifications and security certifications.

Contractual agreement: Sign data cooperation contracts with partners, clearly defining both parties' data protection obligations and responsibilities, and clarifying cooperation scenarios, methods, and liabilities for breach of contract.

During collaboration: Maintain records of partners and dynamically monitor public sentiment regarding partner security incidents, as well as cooperation security risks. Regularly conduct security reviews for key partners.

10. Data Access Permission Management

Ping An Health adheres to the following requirements for data access permission management:

Establishing specific normative requirements and detailed application and approval processes for data access permission requests across different secrecy levels.

Regularly reviewing data permissions and periodically clearing user data permissions that are no longer applicable or are not the minimum necessary for business operations.

11. Data Security Complaint and Reporting Management

Ping An Health provides clear and convenient complaint channels to external users, and internally establishes clear and standardized management, handling mechanisms, specific resolution procedures, and internal disciplinary measures for data security complaints and reports.

12. Data Security Emergency Management

Ping An Health establishes an incident emergency response mechanism for handling data security incidents. It develops corresponding emergency response plans for different dimensions and scenarios of data security incidents, clearly defines the specific responsible persons and handling procedures for each key stage, conducts emergency plan drills, and continuously optimizes the plans and response procedures.

Appendix: Data Security and Personal Information Protection Management Systems List

"Data Security Management System Management Regulations"
"Data Security Management Manual"
"Data Security Standard - Data Classification and Grading Specification"
"Data Security Standard - Organization and Role Management Specification"
"Data Security Standard - Data Collection Security Specification"
"Data Security Standard - Business Planning and Management Specification"
"Data Security Standard - Data Transmission Security Specification"
"Data Security Standard - Data Storage Security Specification"
"Data Security Standard - Data Exchange Security Specification"
"Data Security Standard - Data Usage Security Specification"
"Data Security Standard - Data Destruction Security Specification"
"Data Security Standard - Compliance Specification"
"Data Classification and Grading - Reference Catalog"
"Data Security Standard - Partner Data Security Management Specification"
"Data Security Standard - Data Security Risk Self-Assessment Management Specification"
"Data Security Standard - Data Security Management Audit Specification"
"Data Security Standard - Data Security Education and Training Management Specification"
"Data Security Standard - Data Security Reporting and Complaint Management Specification"
"Data Security Standard - Data Security Incident Emergency Response Specification"
"Data Security Standard - Data Access Permission Approval Management Specification"
"Measures for External Data Exchange Security Management"
"Guidelines for External Data Exchange Management"
"Measures for Sensitive Information Display Masking and Download Management"
"Database Security Management Measures"
"Guidelines for De-sensitizing Sensitive Information in Application Logs"
"Guidelines for Employee Behavior Operation Tracking Points in Application Systems"
"Guidelines for Personal Information Protection Policy Management"
"Guidelines for Personal Information Collection Management"
"Guidelines for Personal Rights Exercise Operation Management"
"Guidelines for Personal Information Deletion Management"
"Guidelines for External Transmission of Personal Information"
"Guidelines for APP Privacy Permission Development"
"Guidelines for Biometric Recognition Security"
"Guidelines for Personal Information Impact Assessment"
"Guidelines for Personal Information Security Compliance of Application Software (including APPs)"

Ping An Health Privacy Protection Policy Statement

I. Commitment to Personal Information Protection

Ping An Health employs various security technologies and a comprehensive management system to ensure that customers' personal information is not leaked, damaged, misused, unauthorizedly accessed, unauthorizedly disclosed, or altered, thereby fulfilling Ping An Health's commitment to personal information protection. Ping An Health will comply with all regulatory requirements concerning personal information protection.

II. Personal User Privacy Policy

Ping An Health has formulated specific user privacy policies for the products or services it provides. We hope that through these dedicated user privacy policies, you can understand how Ping An Health collects, uses, and discloses users' personal information. When you use the corresponding products or services, these specific user privacy policies will take precedence. Currently, Ping An Health's dedicated privacy policy for users is: "Ping An Health Member Privacy Policy".

III. Fundamental Principles of Personal Information Protection

Ping An Health conducts personal information processing activities in accordance with the principles of legality, legitimacy, necessity, integrity, openness, transparency, and security. Specifically, these include:

l Legitimate and Lawful Processing: Adhering to the principles of legality, legitimacy, necessity, and integrity; personal information shall not be processed through misleading, fraudulent, or coercive means.

l Clear Purpose: Having clear, explicit, and specific purposes for personal information processing.

l Choice and Consent: Clearly informing individuals of the purpose, method, scope, and rules of personal information processing, and obtaining their authorized consent.

l Minimality: Processing only the minimum scope of personal information necessary to achieve the processing purpose.

l Openness and Transparency: Publicly disclosing the scope, purpose, and rules of personal information processing in a clear, understandable, and reasonable manner, and accepting external supervision.

l Security Assurance: Possessing security capabilities commensurate with the security risks faced, and adopting sufficient management measures and technical means to protect the confidentiality, integrity, and availability of personal information.

IV. Principles of Personal Information Collection

Personal information of Ping An Health users can only be collected by the company. When employees collect personal information on behalf of the company, they must present sufficient company authorization proof. Unless legally required, Ping An Health will not proactively collect user personal information from third parties.

In addition to adhering to the fundamental principles of personal information protection, personal information collection must also comply with the following rules:

l Legality and Compliance Principle: Ensuring data collection complies with laws, regulations, and supervisory requirements.

l Clear Responsibilities Principle: Clarifying the responsibilities, obligations, and rights of parties involved in data collection.

l Data Minimization Principle: Collecting only the data necessary for fulfilling obligations and for company operations.

l Proactive Disclosure Principle: Before collecting information, users must proactively consent to authorize the collection.

l Inform Before Collect Principle: Before collecting information, it must be collected only after obtaining user consent.

V. Provision of Personal Information to External Parties

Ping An Health and its partners are bound by confidentiality obligations and will not proactively share, transfer, lease, or sell personal information to third parties. Personal data will not be leased, sold, or provided to third parties for purposes other than completing transactions/services. Should such a situation arise, Ping An Health will inform the personal information subject of the purpose of use and data type, and obtain explicit authorization and consent. When Ping An Health provides personal information it processes to a partner, it shall inform the individual of the recipient's name, contact information, processing purpose, processing method, and types of personal information, and obtain the individual's separate consent.

Before and during the sharing of user personal information, we will fully assess the legality, legitimacy, and necessity of such sharing, and adopt appropriate management and technical measures to ensure the security of user personal information. If Ping An Group affiliates wish to change the purpose of personal information usage stated in their privacy policy, they will again seek the user's authorized consent.

VI. User Personal Rights

In accordance with relevant national laws, regulations, standards, and common practices in other countries and regions, Ping An Health guarantees users the following rights regarding their personal information:

l Access or Request: To access or request us to provide account information, search information, and other personal information provided or generated during the use of products and services.

l Correction: To request us to correct inaccurate user personal information.

l Deletion: To request us to delete user personal information under specific circumstances.

l Consent Management: To give or withdraw user authorization and consent for the collection and use of personal information at any time.

l Account Cancellation: To cancel user personal accounts.

l Data Portability: To obtain a copy of user personal information.

Ping An Health's various products and services provide channels for inquiry, modification, communication, and complaints regarding personal information content, through which customers can access and manage their personal information and exercise their user rights. Revisions and updates to the user privacy policy will be promptly notified to users, and re-authorization and consent will be obtained from users.

VII. Protection of Children's Personal Information

Ping An Health's products and services are primarily aimed at adults, but we also attach great importance to the protection of personal information of children and minors. If a customer is a child but has not obtained the consent of a parent or guardian, the child may not create their own user account. For situations where children's personal information is processed with the consent of a parent or guardian, we will only use or publicly disclose this information when legally permitted, with the explicit consent of the parent or guardian, or when necessary to protect the child.

Ping An Health respects and protects the privacy rights of all customers, strictly implements internal normative documents on the basis of ensuring usability, and promptly revises privacy

protection norms in accordance with relevant national laws and regulations, fulfilling corporate responsibility and achieving sustainable development.

VIII. Deletion of Personal Information

Ping An Health retains users' personal information only for the shortest period necessary to provide products and services. After the necessary period, users' personal information will be deleted or anonymized, and no personal data will be collected from third parties, unless otherwise stipulated by the following laws and regulations:

l For users' consultation-related information, we will retain it for 15 years after the user cancels their account.

l For information on goods and services purchased by users on our platform, and transaction information, we will retain it for 3 years after the user cancels their account.

l Unless otherwise stipulated by law, for other user information, we will delete it concurrently when the user cancels their account.