美時化學製藥股份有限公司

Lotus Pharmaceutical Co., Ltd.

Personal Data File Security Maintenance Plan

初版制定日期：2026 年 7 月 21 日

Version 01：July 21, 2026

修訂記錄表 Revision Record

修訂版次 Version	生效日期 Effective Date	修訂摘要 Summary of Revision
01	July 21, 2026	新制定 New Draft

1. Purpose

The Company engages in pharmaceutical research and development, manufacturing, import and export, sales, and related business activities. In the course of its operations, the Company collects, processes, and uses personal data of domestic and overseas customers, medical institutions, business partners, employees, and other relevant individuals in accordance with applicable laws and regulations. Such data is managed and processed through information systems and cloud-based services.

To ensure the proper protection of personal data, prevent unauthorized access, disclosure, alteration, or loss of personal data, and safeguard the rights and interests of data subjects, the Company hereby establishes this Personal Data File Security Maintenance Plan (hereinafter referred to as the "Plan").

2. Legal Basis

This Plan is established pursuant to the Company's **Personal Data Protection Management Policy**, and the **Regulations for the Security and the Maintenance of Personal Information Files in Wholesaling and Retailing Western Pharmaceuticals** promulgated by the Ministry of Health and Welfare.

3. Scope of Application

This Plan applies to the following:

1. All departments, branch offices, and affiliated enterprises under the Company's actual control.
2. All directors, supervisors, managers, employees, contract personnel, and individuals participating in the Company's operations, including contractors and dispatched personnel (collectively referred to as "Personnel").
3. Domestic and overseas third parties entrusted by the Company to process personal data on its behalf, including cloud service providers and system service providers.

4. Organizational Responsibilities

(1) Responsible Person of the Company

The responsible person of the Company shall:

1. Approve personal data protection and information security policies.
2. Supervise the handling of major personal data protection matters, including cross-border data transfers and information security incidents.

(2) Legal Department

The Legal Department shall:

1. Establish, amend, and oversee the implementation of this Plan.
2. Provide legal advice and appropriate management recommendations on personal data protection matters.

(3) Information Technology / Information Security Unit

The Information Technology or Information Security Unit shall:

1. Establish and maintain system security, cloud platforms, and technical protection measures.
2. Implement access control, system monitoring, vulnerability management, and system backup mechanisms.

(4) Department Heads

Department heads shall:

1. Ensure that the collection, processing, and use of personal data within their departments comply with the specified purposes and the principle of data minimization.

(5) Personnel

All Personnel shall:

1. Comply with personal data protection and information security regulations.
2. Refrain from accessing, copying, or disclosing personal data without proper authorization.

(6) Internal Audit Unit

The Internal Audit Unit shall:

1. Audit the effectiveness of this Plan.
2. Periodically report the performance of personal data protection management to the Board of Directors.

(7) Independence Requirement

Personnel assigned to the roles described in Sections (2) and (6) shall not be the same person.

5. Personal Data Risk Assessment

(1) Categories of Personal Data

Personal data processed by the Company includes, but is not limited to:

1. Information of customers, product users, medical institutions, healthcare professionals, and academic collaborators
2. Personnel and recruitment information of employees and job applicants

3. Information of suppliers, distributors, and domestic and overseas business partners

(2) Risk Assessment Mechanism

1. The Company shall conduct personal data protection and information security risk assessments at least once annually.
2. Risk assessment results shall be documented and incorporated into risk management and improvement tracking mechanisms.

6. The Security and Maintenance Measures of Personal Data Protection

(1) Physical and Document Security

1. Paper documents containing personal data shall be centrally managed and stored in locked cabinets with restricted access.
2. The retention, archiving, and destruction of documents shall be conducted in accordance with internal policies and applicable legal requirements.

(2) Information System Security

1. Information systems shall adopt role-based access control and hierarchical account management.
2. System access activities shall be logged and periodically reviewed.
3. Systems shall undergo regular updates, vulnerability scanning, and data backup procedures.

(3) Personnel Management

1. Newly hired personnel shall complete personal data protection and information security training.
2. Existing personnel shall receive periodic refresher training.
3. System access privileges shall be promptly revoked or adjusted upon personnel transfer or termination

7. Cross-Border Data Transfer Management

1. Confirm the legality, purpose, and necessity of the cross-border transfer.
2. Assess the adequacy of personal data protection in the receiving country or region.
3. Execute appropriate contractual arrangements with overseas affiliates or entrusted parties to ensure personal data protection.
4. Establish and maintain records of data access and transfer activities.
5. Implement additional technical or administrative safeguards where necessary.

8. Personal Data Incident Notification and Response

(1) Definition of Personal Data Incident

A personal data incident refers to any event in which personal data is leaked, lost, altered, illegally accessed, or otherwise compromised during collection, processing, use, cross-border transfer, or within system or cloud environments, resulting in possible harm to the rights and interests of data subjects.

(2) Reporting Requirements

1. Upon becoming aware of a personal data incident, the Company shall report the incident to the competent authority within seventy-two (72) hours using the notification form in the Appendix.
2. The reporting period shall commence from the time the Company becomes aware of the incident.
3. If the full scope of the incident has not yet been determined, an initial report shall still be submitted, followed by supplementary information when available.

(3) Incident Handling Procedures

1. Any personnel who discover or receive notification of a personal data incident shall immediately report the matter to the head of the his/her unit and notify the Legal Department and Internal Audit Unit. Where the incident involves cross-border data transfer, systems, or cloud services, the head of the Information Security Unit shall also be notified.
2. Incident response and containment measures shall be implemented promptly to prevent further damage.
3. An impact assessment shall be conducted to determine the types of data involved, the volume of affected data, and the affected individuals.
4. Affected data subjects shall be notified where required by law or deemed necessary based on the nature and severity of the incident.
5. After the incident is resolved, corrective and preventive measures shall be implemented and documented.

9. Revision, Retention, and Implementation

1. This Plan shall be reviewed and revised periodically or whenever there are changes in relevant laws, regulations, or the Company's operational practices.
2. The Plan, audit reports, and incident records shall be retained for at least five (5) years.

10. Appendix

Appendix: Personal Data Infringement Incident Notification Form