

The United Laboratories Privacy Policy

Article 1 Purpose

The United Laboratories International Holdings Ltd (hereinafter referred to as "the Company") attaches great importance to privacy and data security. This Privacy Policy (hereinafter referred to as "the Policy") is intended to clarify the principles and management practices of the Company and its subsidiaries (collectively referred to as "the Group", "the entire Group" or "we") regarding personal privacy and data protection, so as to ensure the security of personal privacy and data.

To practice the “people-oriented” philosophy and fully fulfill the enterprise's responsibility for human rights protection, in accordance with international human rights and medical ethics standards such as the *Universal Declaration of Human Rights* and the *Declaration of Helsinki*, and in strict compliance with applicable laws and regulations, national standards and regulatory requirements including the *Personal Information Protection Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Cybersecurity Law of the People's Republic of China* and the *Information Security Technology - Personal Information Security Specification*, we take privacy protection as a core component of the human rights protection system and establish a full-process privacy rights protection mechanism covering drug research and development, clinical trials, production and operation.

We commit to adopting appropriate security measures to protect personal data (the definition of "Personal Data" is set out in Article 2) in accordance with the applicable laws and regulations of the Group and well-established security standards within the industry, and to continuously improving the Group's data security management.

We respect and care about your privacy and will make every effort to protect the security of your personal data. This Policy helps you (the definition of "You" is set out in Article 2) understand our management principles and measures in terms of data protection, including what personal data we collect, why we collect such data, how we collect and use such personal data, how we protect your personal data, your personal rights, and the like.

We recommend that you carefully read and understand this Policy before using our products, services or engaging in other interactions with us. If you have any questions about the processing of your personal data or this Policy, please contact us (please refer to Article 12 for contact details). We may update this Policy from time to time through the Company's official website (see Article 11), so please check back periodically for such updates.

Our website may contain links to third-party websites and services that are not owned or controlled by the Group. We are not responsible for the operation methods of these

third parties or their processing of your personal data, nor do we have control over the actions of these third-party websites. We strongly recommend that you read the privacy policies of these third parties to ensure that you are aware of how your personal data will be collected and processed.

Article 2 Scope of Application and Definitions

This Policy shall apply to the Company and all of its subsidiaries, covering all business lines of the Group.

The terms “**Personal Data**” or “**Personal Information**” as used in this Policy refer to any information recorded by electronic or other means that relates to an identified or identifiable natural person, excluding information that has been anonymized.

The aforementioned “natural person” (i.e., referred to as “Individual” or “You” in this Policy) includes, but is not limited to:

1. Our customers
2. Our patients
3. Our employees
4. Our shareholders
5. Our partners and their employees (including but not limited to suppliers, distributors, contractors, and the like.)
6. Visitors to our premises
7. Users of our websites, mini-programs, official WeChat accounts, or other digital services
8. Participants in events, conferences, and training sessions organized by us
9. Pharmacovigilance reporters
10. Investigators and subjects involved in our clinical trials
11. Job applicants
12. Individuals who contact us via telephone, text messages, emails, or other means
13. Other individuals who interact with us

Article 3 Collection and Use of Personal Information

We adhere to the principles of "legitimacy, propriety, necessity, good faith, openness and transparency", collect and use personal information for the purposes specified below in this Policy. If we intend to use personal information for any other purposes not specified herein, or collect personal information for any other specific purposes, we will notify you in a reasonable manner and obtain your prior consent again before such use.

The Group observes the principle of "minimization and necessary collection". The personal data collected is commensurate with the needs of the Group's business operations and management and is consistent with the content agreed upon in our

contractual terms and privacy agreements, with no data collected beyond the necessary scope. When we cease the relevant business, the purpose of processing is achieved, you withdraw your consent, or there is no longer a need to continue data collection, we will immediately cease data collection activities and, upon the expiration of the data retention period, delete your personal information or anonymize it.

I. What Personal Information of Yours We Collect

Depending on how you interact with us, we may collect and process personal information that can directly identify you, including but not limited to the following categories:

1. Basic Information: Name, date of birth, gender, ethnicity, nationality, family relations, residential address, telephone number, email address, and the like.
2. Identity Information: Information contained in valid identity documents such as ID cards, military IDs, passports, driver's licenses, employee ID cards, entry-exit permits, social security cards, residence permits, and the like.
3. Biometric Information: Personal genetic data, fingerprints, voiceprints, facial recognition features, biological samples, and the like.
4. Network Identification Information: IP address, personal digital certificate, and the like.
5. Health and Physiological Information: Relevant records generated in connection with medical treatment or illness, such as medical records, hospitalization records, medical orders, test reports, surgical and anesthesia records, nursing records, medication records, drug and food allergy information, fertility information, past medical history, diagnosis and treatment status, family medical history, current medical history, infectious diseases, smoking history, alcohol abuse history, drug abuse history, and the like., as well as information related to an individual's physical health status, such as weight and height.
6. Educational and Employment Information: Occupation, position, employer, department, employee ID number, academic background, academic degree, education history, work experience, training records, academic transcripts, employment separation certificates, qualification qualifications, and the like.
7. Property Information: Bank account details, deposit information (including fund amounts, payment and receipt records, etc.), real estate information, credit records, credit reports, transaction and consumption records, account statements, tax information, financial disclosure forms, social security certificates and other property-related information; as well as virtual property information such as virtual currencies and virtual transactions.
8. Communication Information: Communication records and content, text messages, multimedia messages, emails, as well as data describing personal communications (commonly referred to as metadata).
9. Contact Information: Emergency contacts, address books, group lists, email address lists, and the like.

10. Online Activity Records: Personal operation records stored in logs, including website browsing history, software usage records, click records, and the like.
11. Frequently Used Device Information: Hardware serial numbers, device MAC addresses, software lists, and the like, which describe the basic details of an individual's frequently used devices.
12. Location Information: Travel trajectories, precise positioning data, accommodation information, longitude and latitude coordinates, and the like.
13. Other Information: Marital status, social credit certificates, undisclosed criminal records, registration information for conference attendance, check-in records, and the like.

If you provide us with any personal information of third parties (such as the information of patients' family members, emergency contact information, and the like), such act shall be deemed as your having obtained the legitimate authorization of such individuals, and you are deemed to have authorized us to use such information solely in accordance with this Policy.

II. Purposes for Collecting Your Personal Information

We will process and use your personal information within the scope of our daily business activities, for the purposes specified in this Policy, or when permitted or required to do so under applicable information security laws. During personal information processing, there may be differences between the laws applicable to your place of residence and our place of operation. Notwithstanding such differences, we will ensure the protection of your personal information in accordance with the provisions of the *Personal Information Protection Law of the People's Republic of China* and other relevant regulations, as well as the documents based on your informed consent.

The main purposes for which we use your personal information are listed below:

1. Information Voluntarily Provided by You or Collected with Your Consent

(1) Pharmaceutical Development

We may collect and process your personal information throughout the entire life cycle of the Group's pharmaceutical products (including drug products, active pharmaceutical ingredients and intermediates, diagnostic reagents and devices), covering pre-clinical, clinical trial, marketing authorization and post-marketing phases. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect it.

In certain circumstances, we will request to collect your personal information in accordance with the requirements of applicable laws and regulations. Such requests are necessary for the purposes of evaluating product safety and efficacy, improving health-

related matters, conducting scientific research, fulfilling pharmaceutical registration or regulatory obligations, and monitoring adverse drug reactions.

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed exclusively for our scientific research and business operations and used for our commercial purposes to the extent permitted by law.

(2) Marketing and Promotion

While conducting our business, we may promote our products, services, academic knowledge, news and the like to you through various means. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect such information.

(3) Purchase and Use of Products and Services

When you purchase and use our products and services, you may choose to voluntarily provide your personal information to us or authorize us to collect it. The personal information voluntarily provided by you or collected with your consent in this process will be stored and processed exclusively for the purposes of providing you with the ordered products, after-sales services related to medication use, collecting feedback on adverse drug reactions, as well as delivering health services such as routine blood glucose monitoring and health management, and the like.

(4) Account Registration

To access certain of our services, you may be required to register in advance to create an account. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect such information. We will process and use your personal information for the duration of your account's validity to support the provision of technical administration and our services.

The personal information voluntarily provided by you or collected with your consent in this process will be stored and processed exclusively for account management, service provision and technical maintenance.

(5) Conclusion and Performance of Contracts

We will collect your personal information to facilitate the conclusion and performance of contracts entered with you. If you choose not to provide your personal information, we may be unable to establish and maintain contact with you or your employer, as well as conduct business activities with you or your employer.

The personal information you voluntarily provide or authorize us to collect will be stored and processed solely for the initiation, signing and execution of our contracts.

(6) Contact Requests

When you need to contact us for business or other reasons, you may be required to provide your personal information to enable us to establish and maintain contact with you. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect it.

We store and process the personal information voluntarily provided by you or collected with your consent in this process exclusively for responding to and handling your contact requests.

(7) Newsletters

To maintain contact with you and keep you updated on our latest information, we offer various newsletter services for you to subscribe to. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect it.

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed solely for fulfilling the newsletter services provided to you.

(8) Access Management

When you visit our premises in person or use the wireless network provided by us, we may request you to provide your personal information for necessary security management purposes.

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed solely for providing you with relevant services and ensuring the safety and order of our workplace.

(9) Human Resources Management

To maintain our normal business activities, we conduct daily human resources management activities, including but not limited to recruitment management, on-the-job employee management, and workplace environment management. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect it.

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed solely for carrying out work related to human resources management.

(10) Accounting

We may collect and process your personal information for legitimate accounting purposes to fulfill our obligations under relevant laws such as tax laws and company laws. For instance, when conducting accounting activities including but not limited to recording and processing invoices, making remittances or refunds, the personal information we need to collect from you mainly includes: your contact information (including name, phone number, email address, and the like), accounting data (including purchased goods and services, bank information, tax identification number, invoice number, invoice date, and the like), and your career information (including position, employee ID, department, and the like).

(11) Complaints and Reports

When you submit a complaint or report to us regarding product or service quality, anti-fraud, data privacy, or other matters, you may be required to provide your personal information so that we can establish and maintain contact with you and provide feedback on the investigation and handling results.

You may also file complaints and reports anonymously through the contact information for corresponding matters in the Sustainability section of our official website or other channels specified in our company policies. In such cases, we will conduct relevant investigations based on the issue descriptions received from you (including the specific content of the complaint or report, and the like).

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed solely for handling and responding to your complaints and reports.

(12) Artificial Intelligence (AI)

To improve our work efficiency, we may use artificial intelligence (AI) tools in our business activities. In such cases, we will inform you of the content generated by AI tools through various means to enable you to identify AI-generated content. During this process, you may choose to voluntarily provide your personal information to us or authorize us to collect such information.

The personal information you voluntarily provide or authorize us to collect during this process will be stored and processed solely for the normal operation and function implementation of AI tools. Meanwhile, when using AI tools in business activities, we will de-identify your personal information to avoid various biases arising in this process.

2. Automatically Collected Information

When you access our website, APP, mini-program, or use our other digital services, we and our service providers may automatically collect your personal data, such as browser type, operating system, device type, device model, unique device identifier, IP address,

webpages you view, links you click, your location information, search terms you enter, information you view, hover over or click, and the duration of your visit to our website, among others.

We collect such data in order to safeguard our network security, comply with legal obligations to retain network logs, diagnose and resolve technical issues, and analyze the overall usage of our services, so as to maintain service quality, provide personalized settings for your experience, and improve our services.

(1) Network Security

To ensure the secure operation of our website and services, enhance operational quality and efficiency, and prevent malicious programs, we automatically collect your personal data, including but not limited to the following types: network identity identifiers such as IP address, personal device information (including device MAC address, operating system version, browser type and version, screen resolution, language used, etc.), and personal access behavior records (including website browsing history, page URLs, request time, click records, etc.).

(2) Improving Access Experience and Usage Analysis

Our website uses Cookie technology to help make our website more user-friendly, more efficient, and more secure. The primary purpose of our use of Cookies is to enhance your browsing experience. For example, they are used to record your preferences during browsing (such as language, region, etc.) and apply them to future visits. The information recorded by Cookies also enables us to improve our website by estimating the number of users and usage patterns. Improvements may include customizing content based on your interests, accelerating your search speed, and other enhancements. Most of the Cookies we use are so-called “session Cookies,” which are automatically deleted when you end your visit; some Cookies are set with an expiration period and are automatically deleted upon expiration. You can configure your browser settings to learn about the use of Cookies, so that you can decide whether to accept them based on your specific circumstances.

For Cookies that are necessary to enable electronic communication or to provide certain functions you wish to use, we will store and process the data in accordance with the laws and regulations of China and other applicable countries or regions.

We may engage third-party service providers (such as website analytics tool providers like Baidu Tongji) to assist in collecting the above information for the purpose of website access statistics and usage analysis. These service providers act solely as processors under our instructions and will not use the data for their own purposes.

You can manage Cookies through your browser settings (most browsers provide relevant options in the “Settings” or “Help” menu). Please note that rejecting Cookies may cause certain functions of the website to become unavailable or not work properly.

3. Information Collected from Public Sources

We may periodically collect and use information about you obtained from legitimate public sources (such as government department public websites, public databases, academic journals, authoritative media reports, information published by industry associations, public social media platforms, or other third parties). The primary purpose of such collection is to conduct necessary internal information verification, validation processes, and compliance reviews.

4. Information Collected from Third Parties

We collect and use your personal information from third parties (such as clinical trial institutions, hospitals, or other partners with whom we cooperate) only when you have expressly consented to such third parties providing the relevant information to us, and within the scope of your authorization and consent.

We will strictly comply with our agreements with the third parties, conduct due diligence on the legitimacy of the source of personal information, and process your personal information only in accordance with applicable laws and regulations. Such use shall be limited to the scope of your consent and the purposes described above in this Policy.

III. Collection and Processing of Sensitive Personal Information

We collect your sensitive personal information only, when necessary, such as in the context of human resources management, clinical trials, or other similar situations. Such collection is entirely based on our need to maintain normal business operations and fulfill duties, while strictly adhering to the principle of “minimization.”

Unless there is a specific requirement or explicit request in particular circumstances, we will not proactively ask you to provide your sensitive personal information.

Our business operations may involve the collection and processing of certain sensitive personal information from you. The main categories include the following:

1. Identity Information: Information from identification documents such as ID cards, military IDs, passports, driver's licenses, employee ID cards, entry-exit permits, social security cards, residence permits, and other similar identity documents.
2. Biometric Information: Personal genetic data, fingerprints, voiceprints, palm prints, ear patterns, iris patterns, facial recognition features, biological samples, and other biometric characteristics

3. **Health and Physiological Information:** Relevant records generated in connection with medical treatment or illness, such as medical records, hospitalization records, medical orders, test reports, surgical and anesthesia records, nursing records, medication records, drug and food allergy information, fertility information, past medical history, diagnosis and treatment status, family medical history, current medical history, history of infectious diseases, smoking history, alcohol abuse history, drug abuse history, medical reports, and other information related to an individual's physical health status, such as weight, height, lung capacity, and similar data.
4. **Property Information:** Bank account details, authentication information (such as Dynamic Verification Code), deposit information (including fund amounts, payment and receipt records, etc.), real estate information, credit records, credit reports, transaction and consumption records, account statements, tax information, financial disclosure forms, social security certificates, and other property-related information, as well as virtual currency and virtual transaction information.
5. **Other Sensitive Information:** Marital status, undisclosed criminal records, communication records and content, address books, friend lists, group lists, location tracking data, web browsing records, accommodation information, precise location information, and similar data.

We place the highest importance on protecting your data privacy and commit to processing such sensitive personal information only within the scope that is necessary and lawful.

Article 4 How We Share Your Personal Information

Within the purposes set forth in this Policy, the Company and its subsidiaries may share your personal information with each other to the extent necessary.

We may share your personal information with third parties (such as our suppliers, service providers, business partners, affiliates, and similar entities) in order to conduct our business activities, fulfill our service obligations, and comply with applicable laws and regulations. To this end, we will enter into Data Confidentiality agreements with such third parties in accordance with this Policy and relevant laws and regulations to fully safeguard your personal information. During the course of cooperation, we will strictly require these third parties to process your personal information in accordance with the scope, manner, and methods stipulated in this Policy, the signed agreements, privacy agreements, and applicable laws and regulations, and to adopt necessary security measures. Where necessary, we will obtain your separate consent.

As our business develops, if the transfer of your personal information to a third party becomes necessary due to mergers, acquisitions, asset transfers, or similar transactions, we will notify you in a timely manner through push notifications, announcements, or other appropriate means. We will require the receiving party to use and protect your personal information in accordance with this Policy and applicable laws and regulations.

We will also continue to ensure that your personal information is adequately protected in accordance with relevant laws and regulations, and at a standard no lower than that set forth in this Policy.

In addition, we may disclose your personal information where such disclosure is necessary to comply with regulatory requirements, government requests, court orders, judicial proceedings, or to protect the safety, rights, or property of the public. We reserve the right to make such disclosures as required by law.

Upon obtaining your consent, we may also use and disclose your personal information in other ways.

Article 5 Cross-Border Transfer of Personal Information

In principle, personal information collected by us within the territory of the People's Republic of China will be stored within the territory of the People's Republic of China.

Given that our business has expanded to multiple countries and regions worldwide, your personal information may, with your authorization and consent, be stored in other countries or regions, or accessed from other countries or regions.

Regardless of where your personal information is stored or accessed, we will protect it in accordance with the applicable laws and regulations, the informed consent documents, and the provisions of this Policy.

Article 6 Protection of Children's Personal Information

We do not proactively collect personal information from children under the age of 14, except where we have lawfully obtained the consent of their parents or other guardians, or where such collection is necessary to fulfill obligations under applicable laws and regulations.

If you are under the age of 14, please do not provide us with any of your personal information.

If your child has submitted personal information to us and you wish to exercise rights such as accessing, correcting, deleting such personal information, or withdrawing consent (except where retention is required by law), you may contact us (please refer to Article 12 for contact details).

Article 7 How We Protect and Store Your Personal Information

We will take all reasonable and feasible measures to protect your personal information, including but not limited to encryption technologies, access controls, firewalls, and other security measures, to prevent unauthorized access, public disclosure, use, modification, damage, or loss of personal information.

Although we have made every effort to protect your personal information, due to limitations in current security technologies, we cannot guarantee absolute security of the data. Personal information may be leaked, stolen, or otherwise compromised due to force majeure events or other security incidents not attributable to us. In such cases, we will promptly take reasonable measures in accordance with legal requirements, the Group's internal Personal Information Security and Privacy Protection Policy, and related procedures to minimize relevant risks and adverse impacts to the extent possible. If you have reason to believe that your interaction with us is no longer secure, please contact us immediately (please refer to Article 12 for contact details).

Unless otherwise required or permitted by law to extend the retention period, we will retain your personal information only for the minimum period necessary to achieve the purposes set forth in this Policy or to comply with legal or regulatory requirements. Upon expiration of the retention period, we will delete or anonymize your personal information.

In addition, where an account is necessary to provide services to you, we will retain your registration information. You may also choose to cancel your account. Upon cancellation of your account, we will cease providing products and services based on that account and delete or anonymize your corresponding personal information, except where retention is otherwise required by laws or regulations.

The Group's Information Security Management Committee and Digital Center are responsible for periodically reviewing whether the measures for the collection, storage, and processing of personal information are sufficiently secure and effective to prevent unauthorized access.

Article 8 Your Rights Regarding Personal Information

All personal information you submit should be accurate and complete. We will make reasonable efforts to maintain the accuracy and integrity of your personal information and update it in a timely manner.

To the extent permitted by applicable law, you have the following rights with respect to your personal information:

1. Right of access: to access, review, and copy the personal information we hold about you;
2. Right to rectification: to correct, update, or supplement your personal information;
3. Right to erasure: to request deletion of your personal information;
4. Right to object: to object to or restrict our collection, processing, or use of your personal information;
5. Right to withdraw consent: to change the scope of authorization or withdraw your consent;

6. Right to data portability: to request the transfer of your personal information to another data processor designated by you;
7. Other rights granted by applicable laws.

We attach great importance to protecting your rights. If you wish to exercise any of the above rights, please contact us using the contact details provided in Article 12. To ensure security, you may be required to provide a written request, and we will verify your identity in accordance with applicable laws and regulations.

To the extent permitted by applicable law, where we process your personal information based on your consent, you have the right to withdraw such consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out based on your consent prior to the withdrawal. However, if the processing is also based on other lawful grounds (such as the performance of a contract or compliance with legal obligations), withdrawal of consent will not affect our continued processing of your personal information on those grounds.

In the following circumstances, we may be unable to fulfill your request to exercise your rights to comply with laws and regulations or to protect significant public interests or other major legitimate rights and interests:

1. Where your request is contrary to our obligations under applicable laws and regulations;
2. Where your request is directly related to national security or national defense security;
3. Where your request is directly related to public security, public health, or significant public interests;
4. Where your request is directly related to criminal investigation, prosecution, trial, or execution of judgments;
5. Where we have sufficient evidence to demonstrate that you have subjective malice or are abusing your rights;
6. Where the purpose is to protect your life, health, property, or other major legitimate rights and interests, or those of other individuals, but it is difficult to obtain your authorization and consent;
7. Where fulfilling your request to exercise rights would cause serious harm to the legitimate interests of you, other individuals, or organizations;
8. Where your request involves trade secrets.

If you are dissatisfied with the way we handle your personal information, you may submit a request to us (please refer to Article 12 for contact information). We will promptly investigate and address your concerns.

Article 9 Management Measures

To prevent possible risks in data protection work, and to respond to potential personal data breaches and security incidents, the Group has adopted both proactive preventive measures and reactive response measures at the same time.

We have also established corresponding management measures specifically for incident identification, incident response, and incident reporting, with the aim of quickly containing the incident and minimizing the adverse impact of any data breach or security incident on individuals' rights and interests as well as on the Group.

Article 10 Regular Audit

The Group's Digital Center, in collaboration with the Information Security Auditor, shall conduct an audit of the implementation of this Policy and the Group's information systems at least once every three years. This is to ensure the effectiveness of privacy and data protection measures and to promptly update the information security strategy accordingly.

Article 11 Policy Updates

This Policy takes effect on the date of its publication. This Policy may be amended when there are changes to the applicable laws and regulations, or when there are material changes to the functions of the Group's products or services. However, without your explicit consent, we will not reduce the rights you are entitled to under this Policy.

For any material changes to this Policy, we will provide you with prominent notice (including but not limited to announcements on the Group's official website, push notifications or other means). If you do not agree with the relevant content of the updated Policy, you may contact us at any time (please refer to Article 12 for contact details).

Article 12 How to Contact Us

If you have any questions, comments, or suggestions regarding this Policy or our handling of your personal information, please contact us through the following channels:

Email: privacy@tul.com.cn

Telephone: +86 - 0760 - 8713 3912

Under normal circumstances, we will respond to you within 5 working days.

Article 13 Policy Governance

This Policy has been reviewed and approved by the Information Security Management Committee. The Information Security Management Committee shall regularly report to

the Board of Directors on the implementation of this Policy and provide recommendations for the Board's decision-making and oversight.

The Information Security Management Committee is responsible for the interpretation and revision of this Policy.

For matters not covered in this Policy, relevant laws, regulations, and normative documents shall apply.

This Policy shall take effect from the date of its promulgation.