Excerpt from The United Laboratories Patient Information Protection Policy

The United Laboratories International Holdings Limited (Stock Code: 3933.HK) ("TUL", the "Group", "we") must comply with national laws and the Group's internal policies and relevant statements on personal information protection in the process of collecting, storing, transmitting and deleting patient information.

1. Information Collection

(1) When initiating a new project, conducting an activity, or collecting patient information based on business needs, prior the Group's approval is required. Collection of patient personal information is prohibited without such approval.

(2) During the collection process, patients must be clearly informed and prompted to carefully read the Group's privacy statement. Written consent must be obtained, and the patient must be made aware of the purpose, scope, method of information collection, data protection measures and available complaint channels.

(3) Patient personal information must not be collected beyond the scope required by the Group, and information irrelevant to the service provided must not be collected.

2. Use of Information

Collected patient personal information shall only be used for periodic follow-ups and for collecting data on symptoms and adverse reactions experienced during medication use. Follow-ups must be conducted without disrupting the patient's daily work or life. During the follow-up, the purpose must be clearly explained, and the patient's understanding must be obtained. At the same time, our employees are strictly prohibited from providing medication guidance to patients and must advise them to consult professional physicians instead.

3. Management and Protection of Information

(1) The Marketing Department is responsible for the overall management of collected patient information, while the Group's Digital Centre is responsible for managing and maintaining the patient record system to prevent the leakage, damage, tampering, or loss of personal patient information within the system.

(2) Each region must designate dedicated personnel to properly store collected paper-based patient personal information; such documents must not be discarded or destroyed at will.

(3) For electronically recorded patient information, the Group assigns access permissions to relevant personnel to ensure controlled management.

(4) Our employees are strictly prohibited from disclosing or selling patient information to any third party, or from using such information for profit or any other improper purpose.