

October 19, 2026

To whom it may concern:

Company Name:	TOHO HOLDINGS CO.,LTD.
Corporate Representative:	Hiromi Edahiro, Representative Director, President and CEO (Prime Market of Tokyo Stock Exchange Securities Code: 8129)
Contact	Makoto Kawamura, Senior Executive Corporate Officer and General Manager, Corporate Strategy Division (TEL: 81-3-6838-2803)

Notice Regarding Unauthorized Access and Information Leakage at a Subsidiary

TOHO HOLDINGS CO.,LTD. (the “Company”) hereby announces that it has been confirmed that a database managed by its non-consolidated subsidiary, enTouch KK (Head Office: Tokyo; Representative Director: Tamayo Tsujiura; hereinafter “enTouch”), which operates a remote detailing business (a business providing information remotely to medical institutions) and other services, was subject to unauthorized access by a third party, and that a portion of the information stored therein was leaked to the outside.

We deeply apologize for the considerable inconvenience and concern this may cause to all parties concerned.

In this regard, the remote detailing business is conducted either under outsourcing contracts from TOHO PHARMACEUTICAL CO.,LTD. (Head Office: Tokyo; President and Representative Director: Akira Umada), a pharmaceutical wholesaling subsidiary of the Company, or under direct outsourcing contracts between enTouch and pharmaceutical companies.

Based on the report received from enTouch, the Company announces the facts that have been confirmed at this time and the status of response as follows.

1. Overview of the incident and current status

At around 16:00 on October 13, 2026, it was discovered that data related to the remote detailing business had been leaked to the outside from a database managed by enTouch. The incident was caused by unauthorized access by a third party claiming to be a ransomware group, and it has been confirmed that information in the database held by enTouch was exfiltrated.

This event occurred solely within the system managed by enTouch and is completely isolated from other systems within the Company’s group; therefore, there is no impact on any other systems of the Company’s group. In addition, no alteration or deletion of data has been confirmed, and there is no disruption to the business continuity of enTouch.

2. Information that may have been leaked

The information confirmed to have been leaked at this time is as follows. The exact number of affected items and the detailed scope of impact are currently under investigation:

- Names, affiliated medical institutions, and prefectures of location of healthcare professionals who used the service
- Information of users accessing the platform (administrators, eMRs, etc.), including names and email addresses
- Phone numbers and email addresses entered as contact information upon reservation
- Product names and pharmaceutical company names subject to reservation
- Reservation creation date and time, interview date and time, and interview status

Note: Content files used for providing information in projects and recorded video/audio data are not stored in the affected database and are therefore outside the scope of this information leak.

3. Measures taken

Immediately following the discovery of this incident, enTouch implemented the following emergency defensive measures:

- Application of security patches to the software accessing the database
- Preservation of access logs and forced reset of all passwords
- Consultation with the Cybercrime Division of the Tokyo Metropolitan Police Department
- Submission of a report to the Personal Information Protection Commission (PIPC) (Reports regarding matters based on business outsourcing from Toho Pharmaceutical are submitted by TOHO PHARMACEUTICAL)

4. Future actions and measures to prevent recurrence

enTouch is in the process of engaging an investigation by an external specialized agency (a forensic investigation firm) and is currently working in cooperation with experts to determine the cause, identify the scope of impact, and examine countermeasures. We kindly ask our customers to remain vigilant regarding suspicious emails or communications.

We once again offer our deepest apologies to all related parties for the immense concern and inconvenience caused. Should any new significant facts come to light as the investigation progresses, we will promptly disclose them.

Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.
--