December 6, 2021

To persons concerned

Company name: Linical, Co., Ltd.
Representative: Kazuhiro Hatano, President & CEO
(Securities Code: 2183, First Section of the Tokyo Stock Exchange)
Contact: Akihiro Takahashi, Executive Vice President, Chief Financial Officer (CFO)
(TEL.06-6150-2582)

Notice and Apology regarding Possible Leakage of Personal Information, etc., due to Unauthorized Access

Linical Co., Ltd., confirmed on November 3rd that, as a result of an unauthorized access attack from a third party, there may have been leakage of the personal information and some corporate information held by the group.

After that, as we conducted an investigation to determine whether or not there was an actual leak and the extent of the leak, we received advice and guidance from outside experts and decided to give top priority to preventing secondary damage, so we notified the people concerned by using **the current maximum estimate** of personal information, etc., that may have been leaked based on the information in the restored Japanese servers.

A system in a separate cloud server environment is used to collect and store the data on subjects in the clinical trials that are entrusted to our company by clients such as pharmaceutical companies and that data has not been affected by this unauthorized access.

The current status is that the internal server that received the unauthorized access has been restored and there is no problem in the execution of our operations. Furthermore, under the advice and supervision of experts such as a specialist IT team from a consulting company affiliated to an auditing firm, in addition to our initial response, we are also steadily implementing measures to strengthen our security and personal information protection from the aspects of both technical countermeasures and organizational

countermeasures. As it will take more time until we can report the final results of the investigation, we will make an interim report as follows.

At the current time, there have been no reports of damage such as the actual misuse of the leaked information.

In addition, following advice from outside lawyers, the police, and public authorities, our company does not intend to have contact with the criminal group, which has become an international problem, or to respond to ransom demands.

We deeply apologize for the inconvenience and concern we have caused to the owners of the personal information, to our customers, and to the many other concerned parties.

1. Personal information that may have been leaked (Article 2, Paragraph 1 of the Act on the Protection of Personal Information)

The numbers shown below for the total items of information that may have been leaked indicates **the maximum number at the current time** based on the information in the restored Japanese servers.

(1) Personal information (shareholders, job applicants, etc.)

Japan - Information on job applicants (excluding the employment of people with disabilities) (approx. 14,000 items)

Two or more items from the names, dates of birth, telephone numbers, e-mail addresses, etc.

Japan - Information on applicants for employment of people with disabilities (approx. 300 items)

Name, disability grade, etc.

Japan - Shareholder register information

(Individual shareholders listed in the shareholder registry from 2015/3/31 to 2021/6/30 - approx. 21,000 items

Individual shareholders listed in the shareholder registry from 2009/3/31 to 2014/12/31 - approx. 60,000 items (Total number))

Name, address, shareholder number, number of shares held, etc.

Japan - Information on retirees and their families (approx. 500 items)

Name, e-mail address, personnel information, etc.

Japan - Business card information of institutional investors, etc. (approx. 40 items)

Name, company name, telephone number, e-mail address, etc.

Japan - Information on compensation for our company advisors, etc. (approx. 70 items)

Name, contact information, compensation payment, etc.

China - Information on job applicants (approx. 60 items)

Two or more items from the names, dates of birth, telephone numbers, e-mail addresses, etc.

China - Retirees (3 items)

Name, e-mail address, personnel information

Korea - Information on job applicants (4 items)

Two or more items from the names, dates of birth, telephone numbers, e-mail addresses, etc.

Korea - Retirees (approx. 70 items)

Name, e-mail address, personnel information

Taiwan - Retirees (approx. 20 items)

Name, e-mail address, personnel information

Taiwan - Information on job applicants (approx. 30 items)

Two or more items from the names, dates of birth, telephone numbers, e-mail addresses, etc.

(2) Personal information (employees and people related to personnel information)

Japan - Personnel information (approx. 500 items)

Europe - Personnel information (approx. 300 items)

China - Personnel information (approx. 35 items)

Korea - Personnel information (approx. 70 items)

Taiwan - Personnel information (approx. 20 items)

(3) Personal information (employees of trading partners)

Japan - Name, company name, department, job title, e-mail address, telephone number, etc. (approx. 30,000 items)

(4) Personal information (responsible physicians and subinvestigators for clinical trials)

Japan - Name, affiliation, job title, telephone number, e-mail address, items included on clinical study résumé, etc. (approx. 35,000 items)

(5) Personal information (clinical trial coordinators, collaborators, etc.)

Japan - Name, name of medical institution, affiliation, job title, etc. (approx. 60,000 items)

(6)Trading partner information

Electronic files of documents necessary for clinical trial implementation, contracts with trading partners, etc.

(7)Our company corporate information

Management materials, sales materials, etc.

2. Response for persons who may have had personal information leaked

We will continue to investigate regarding the information that may have been stolen or leaked.

In addition, we have set up the dedicated inquiry contact point shown below for the persons related to the information that may have been leaked.

Contact point for inquiries about unauthorized access to Linical
Telephone number (toll-free): 0120-513-230
Reception hours: 10:00 to 17:00 Monday to Friday (except national holidays and New Year holidays)
Contact point for inquiries about personal information of Europe (employees and people related to personnel information):email; dpo@linical.com (Linical EU DPO)

3. History of the discovery and response

(1) History of the discovery

On October 3rd, we discovered evidence of unauthorized access by a third party to servers at our Japanese headquarters and at our group base in Taiwan. On October 4th, we began to take measures to recover the servers and to investigate the details of the cause of the unauthorized access and the damage caused.

On October 5th, we posted an “Apology and Report for Temporary Suspension of File Server to Investigate Cause of Illegal Access” on our company website.

On October 22nd European time, we recognized unauthorized access to a European base of our group, so we suspended our network within Europe and the networks with Japan, Asia, and the United States, and a team including a local IT security research company engaged in the recovery response and investigation.

On October 26th European time, we became aware of a threatening message from a criminal group demanding a ransom for the data it claimed had been stolen, so we consulted with the European and Japanese police authorities about this matter, and began to assess the damage situation with a response team that included an investigation company.

On October 27th, we posted “Cyberattacks against the European subsidiaries of our group” on our company website.

On November 3rd, an external research company discovered traces suggesting possible information theft from servers in Japan and Taiwan. In response, our company conducted analysis to determine the extent of the outflow.

However, due to physical and technical difficulties, the investigation ran into difficulty and stalled. At that time, based on the advice and guidance of external experts, and from the

viewpoint of preventing secondary damage, we **estimated the current maximum possible** personal information and partial corporate information that may have been leaked based on the information in the restored servers, compiled interim results as of December 3rd, and published them on December 6th. (This release)

(2) Response to the regulatory authorities

We have informed the data protection authorities of EU member states, the Personal Information Protection Commission in Japan, and the relevant authorities in Taiwan about the unauthorized access.

(3) Initial response to ensure safety

In addition to correcting the vulnerability of the VPN device that was the origin point for the unauthorized access, we strengthened multiple authentication and reconstructed the server before performing a clean install of the backup data. We then implemented a virus check on the server and PCs, and the server is now operating normally. We have also taken measures to enhance security, such as adding countermeasure software and strengthening server monitoring.

With regards to the investigation of the cause, the recovery action and the recurrence prevention measures for the system aspects of this problem, we have entrusted the verification to a consulting company affiliated with an auditing firm and we will work to secure further safety by taking additional measures to prevent recurrence or for strengthening based on the results of that verification.

We also reported the situation to major IT vendors, experts with a deep knowledge of cybersecurity, the JPCERT Coordination Center, and external lawyers, and have established a system to receive guidance and advice.

In the future, as the investigation progresses, we will start contacting the people and related parties for whom the leakage of information is confirmed, and will continue to investigate other information that may have been stolen.

4. Future response

(1) We will continue to cooperate with the police authorities in Japan and overseas, to provide timely reports to the personal information protection organizations in the relevant countries, and to maintain a system to receive advice.

(2) As mentioned above, in addition to the measures taken previously, we will request the cooperation of a specialist IT team from a consulting company affiliated to an auditing firm and from major IT vendors and others, and will clarify the full extent of the damage caused by this attack and work to prevent its recurrence.

(3) We have already started countermeasure meetings with the participation of external security experts, but we will also newly establish an advisory organization for system security with external experts and will work to prevent a recurrence.

The reason for reporting today is that this unauthorized access involved the encryption of information stored in servers and the deletion of access logs, so it has taken time to investigate and analyze the unauthorized access and the situation of damage.

The impact of this problem on the consolidated financial results of our group for the fiscal year ending March 2022 cannot be reasonably calculated at this time due to our continuing implementation of the measures above. If further disclosure is required, we will make a separate announcement promptly.

Our company takes this situation seriously and we will make further effort to strengthen our management system to prevent such incidents from happening again. We will also deal with any criminal acts such as unauthorized access severely.

(Contact for inquiries about this matter: Monday to Friday (except national holidays and New Year holidays))
Contact information for media and investor inquiries
Finance Department, Administrative Unit 06-6150-2582 (Reception hours: 10:00 to 17:00)
Contact information for inquiries regarding personal information
Contact point for inquiries about unauthorized access to Linical: 0120-513-230 (Reception hours: 10:00 to 17:00)
Contact point for inquiries about personal information of Europe (employees and people related to personnel information):email; dpo@linical.com (Linical EU DPO)
Contact information for inquiries about the clinical trials entrusted to our company
Customer Relations Office 080-6853-8783 (Reception hours: 10:00 to 17:00)

End