日本語版はこちらをご覧ください。(Click here for Japanese Pages)

For Immediate Release

April 28, 2017

Pharmaceuticals and Medical Devices Agency

Regarding the loss of a USB flash drive containing of electronic product application data during approval review

The Pharmaceuticals and Medical Devices Agency (PMDA) receives electronic clinical trial data from applicant companies in connection with its reviews of new medical product applications. However, on April 11, 2017, PMDA discovered that one (1) USB flash drive containing portions of electronic application data had gone unaccounted for while in its custody.

After making the aforementioned discovery, PMDA reported the pertinent details to the relevant parties while conducting repeated internal searches for the missing drive. PMDA has also filed a missing item report with the appropriate police station. As of the date of this statement, the missing drive has not yet been located.

PMDA offers its deepest apologies for these events and for causing such concern and inconvenience to all parties concerned.

As of the date of this statement, PMDA has not determined that the flash drive in question was taken outside of PMDA's offices or that the information contained in the drive was leaked to outside parties.

The data contained in the USB flash drive in question is password-protected, and the corresponding security software has the function of blocking all further operations after a certain number of incorrect password entry attempts. The information contained in the missing drive also cannot be read without the use of specialized software for statistical analysis and visualization of clinical trial data.

1. Data contained in the missing USB flash drive

When receiving electronic clinical trial data submissions from applicant companies through PMDA's electronic application data system, as PMDA verifies abnormalities that occur using computer terminals not connected to the Internet ("verification terminals"), the data contained in the USB flash drive in question is used when transferred to the relevant verification terminal.

The data contained in the missing USB flash drive is described below.

USB flash drive contents

- Clinical trial data related to five (5) products (8,371 cases). The case data provides subject sex, age, ethnicity, and name of applicable clinical trial site(s). All case report data has been anonymized and contains no individually identifying information.
- The names of the corresponding clinical investigators (264 individuals). Of these, there are descriptions of facility names (150 facilities in all).
  *For some of the investigators, there is published literature mentioning the individual's participation in the relevant trial.
- The names of the sponsor or relevant contract research organization (CRO) (107 individuals).
  *For some of the 107 individuals, there is published literature mentioning the individual's involvement in the relevant trial.

2. Preventative measures

PMDA will administer additional thorough training for all staff to review the importance of information handling and management. PMDA has implemented and plans to implement the following preventative measures to prevent recurrence.

Measures already implemented

- In accordance with PMDA's information security policy, PMDA takes steps to delete all confidential or otherwise sensitive information stored on USB flash drives as soon as it is no longer needed.
  In addition, PMDA adheres to the following practices in accordance with its procedural manual for the handling and management of electronic application data:

  1) USB flash drives are only to be used when transferring data to a verification terminal.
  2) Data contained on USB flash drives that is no longer needed is deleted each day, and the drive must be returned to the authorized handler.

- The location of verification terminals was moved to the sides of the desk of the office managers and the USB drive port was extended to their desktops, to enable them to visually verify the insertion and removal of USB flash drives.

Planned measures

- Switch from the use of portable media (e.g. USB flash drives) for migrating data to verification terminals to non-portable media (planned for early-May 2017).
- Conduct an urgent “risk management training” program for all our staff (to begin in mid-May 2017).

End of Document