

Wrongful Disclosure of Personal Data Through Mishandling of Medical Reports by a Charitable Organisation

Investigation Findings

Published under Section 48(2) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) has completed its investigation into a case relating to the wrongful disclosure of personal data through mishandling of disease risk assessment reports by a registered charitable organisation.

The investigation arose from a complaint received by the PCPD, which was related to a medical programme implemented by a charitable organisation aiming at identifying the onset of a specific hereditary disease. A participant of the programme (the Complainant) lodged a complaint with the PCPD, alleging that the organisation concerned wrongfully uploaded her disease risk assessment report, which contained her sensitive personal data, to the account of another programme participant.

In July 2025, the Complainant received notification from the organisation alerting her to access three documents through the account registered at a health management platform. Upon checking, the Complainant discovered that the laboratory test report and the doctor's referral letter uploaded to her account belonged to another programme participant, and she therefore reported the matter to the organisation. The organisation later confirmed to the Complainant that her disease risk assessment report was also erroneously uploaded in June 2025 to that relevant participant's account at the platform and subsequently accessed. The report concerned contained personal data including the Complainant's name, Hong Kong Identity Card number, date of birth, age, anthropometric measurements and the relevant medical history, the indicators analysed and the associated risks. The organisation explained that due to the similarity of the participant numbers of the Complainant and the other participant concerned, the staff member responsible for the dissemination of documents uploaded the wrong documents to their respective accounts by mistake.

Upon discovering the Complainant's disease risk assessment report being wrongfully uploaded and accessed, the organisation changed the setting of the document to restrict further access to the report. In addition, the organisation proactively initiated a review of the documents uploaded onto the platform which belonged to the participants who were at high risk of

developing the disease to confirm whether they belonged to the authentic account users, and conducted checks on all documents contained in the relevant folders of its internal system to ascertain whether they were correctly filed on record according to the participants' numbers. In the course of inspection, no further cases of personal data being wrongfully disclosed were identified. To avoid recurrence of similar incidents, the organisation stated that only the participants' names and participant numbers would be recorded in their medical reports for the purposes of identification going forward. The organisation has also deployed additional manpower to conduct document verification and review procedures in order to strengthen the vetting process, while at the same time reminded the relevant staff members to stay prudent to ensure that correct information was being uploaded. Furthermore, the organisation has enhanced staff training and circulated reference materials regularly to enhance their awareness of personal data protection and information security.

Investigation Findings

The PCPD has commenced an investigation into the incident and made four rounds of enquiries with the organisation. The organisation admitted that the incident was caused by human error on the part of its staff, resulting in the incorrect uploading of the programme participants' documents to the relevant platform and the unauthorised or accidental access to personal data by participants who were not the data subjects.

Having considered the circumstances of the incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of the organisation were the main contributing factors to the occurrence of the incident:-

- 1. Absence of written procedures in relation to uploading documents to the relevant platform** for staff members responsible for verifying and/or uploading the participants' documents to follow, so as to check and ensure that the documents to be uploaded belong to the correct account holder;
- 2. Failure to provide sufficient and regular training** to the relevant staff members to ensure that they fully comprehended the points to note when handling personal data; and
- 3. Failure to take measures for ensuring the secure transmission of the personal data**, such as protecting the documents to be uploaded with encryption or password protection, to ensure that even if relevant personal data was erroneously uploaded to the platform, it would not be subject to unauthorised or accidental access.

The Privacy Commissioner's Decision

Data Protection Principle (DPP) 4(1) in Schedule 1 to the PDPO stipulates that all practicable steps shall be taken to ensure that any personal data held by a data user should be protected against unauthorised or accidental access, processing, erasure, loss or use.

Having taken into account the deficiencies in the personal data security measures of the organisation, the Privacy Commissioner found that the relevant organisation had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) of the PDPO concerning the security of personal data.

The Privacy Commissioner has served an Enforcement Notice on the relevant organisation, directing it to take measures to remedy the contravention in order to prevent recurrence of similar contraventions in future.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
10 July 2026

— End —