

Non-Compliance Report: Accidental Leakage of Personal Information

Case Study

In an email to the study sponsor, Dr X unintentionally included the name and NRIC number of a research subject. The name and NRIC number were overlooked as they were right at the end of a long email thread. Upon realization, Dr X immediately notified his sponsor. Dr X also sought the sponsor's written assurance that they would delete the personal information received. Simultaneously, Dr X submitted a Non-Compliance Report to the DSRB. Due to the involvement of personal information, Dr X was also advised to inform the institution's Data Protection Officer (DPO) of the incident.

The incident was subsequently reported to MOH and PDPC for investigations.

What the PI should have done

CHECK carefully that all subjects' personal and sensitive information are removed before sending any email.

Lessons to Learn

CHECK carefully that all subjects' personal and sensitive information are removed before sending any email.

1. It is easy to make a slip. Every study team member must work to ensure that all subjects' personal and sensitive information are managed prudently. When corresponding with research stakeholders, the study team must be diligent and ensure that personal data are not shared unless consent has been given for the specific purpose.
2. In cases where research subjects' personal data is involved, in addition to reporting to the DSRB, the PI must also inform their institutions' Data Protection Officer (DPO). This reporting allows the institution to manage the data breach promptly and appropriately.²
3. The PI must review the circumstances leading to the breach, assess the risks and impact and take steps to prevent future breaches.

Human Biomedical Research Act (HBRA), Personal Data Protection Act (PDPA) and NHG Personal Data Protection Policy on disclosure of information and personal data

1. "Personal data" means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access¹.

2. A data breach generally refers to the accidental and/or intentional unauthorized access and retrieval of information that may include corporate and personal data².
3. An organisation shall not disclose personal data about an individual unless consent has been obtained (or deemed to have been obtained) from the individual to the disclosure³.
4. Any individually-identifiable information of any research subject should not be disclosed unless except under the following circumstances:
 - a) Consent of the research subject or authorized person has been obtained;
 - b) The information is necessary for the administration or execution of anything under the HBRA;
 - c) The disclosure is ordered by a court;
 - d) The information is publicly available;
 - e) The disclosure of information to persons or class of persons is in the public interest, in the opinion of the Director of Medical Services;
 - f) Any other right of disclosure arises under the HBRA or any other written law or rule of law; or
 - g) In such other circumstances and to such persons as may be prescribed.

Disclosing any individually-identifiable information of any research subject which has come to his or her knowledge in the course of his conduct of Human Biomedical Research is an offence under the Act. More information on the potential penalties may be found in HBRA, Section 29.⁴

Staff should refer to their Institutions PDP Office or equivalent for their data breach management processes. This is to ensure that personal data breach incidents are communicated and escalated in a timely and consistent manner and that appropriate measures can be taken to minimize disruptions and to coordinate responses to help address public concerns².

References

¹ Personal Data Protection Act 2012 – Part I (Preliminary) (<https://sso.agc.gov.sg/Act/PDPA2012?Provides=P1I-#pr1->)

² NHG Personal Data Protection Policy Guide Rev 5 – Section 11 (Points 73 & 71)

³ Personal Data Protection Act 2012 – Part IV (Collection, Use and Disclosure of Personal Data)

(<https://sso.agc.gov.sg/Act/PDPA2012#P1IV->)

⁴ Human Biomedical Research Act 2015 – Section 29 (<https://sso.agc.gov.sg/Act/HBRA2015>)

Clara Lim

Research Institution (RI) Secretariat
Research Compliance Unit
Research & Development Office
National Healthcare Group