Bord Altranais agus Cnáimhseachais na hÉireann
Nursing and Midwifery Board of Ireland

NMBI Personal Data Security Breach Policy and Procedures

Key Details

- Prepared by Dr Aoibhín de Búrca, Data Protection Officer: 09/04/2018
- Approved by Board: 17/04/2018
- Policy operational from: 17/04/2018
- Updated: 07/08/2018
- Next review date: 25/05/2019

1. NMBI is obliged, under Irish Data Protection legislation and the General Data Protection Regulation (GDPR), to process personal data in a manner that respects the rights of data subjects to have their data processed lawfully, fairly and transparently. It is also under a specific obligation to ensure appropriate security of personal data.

2. This policy and procedures document addresses situations where personal data has been put at risk of unauthorised disclosure or access, loss, damage, destruction or alteration.

3. The Data Protection Commission is the independent supervisory authority responsible for data protection and GDPR in Ireland, and the focus of the Data Protection Commission is on the rights of the affected data subjects in relation to the processing of their personal data.

4. Where an incident gives rise to a risk of unauthorised disclosure or access, loss, damage, destruction or alteration of personal data, in manual or electronic form, NMBI must give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, NMBI should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

5. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, NMBI may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

6. All incidents of loss of control of personal data in manual or electronic form **must be reported immediately to the line manager within NMBI and the Data Protection Officer**.

7. NMBI **must report the personal data breach to the Data Protection Commission without undue delay, and no later than 72 hours** after having becoming aware of the incident, outlining the circumstances surrounding the incident.

This initial contact must be made by the Data Protection Officer using the DPC Notification Forms. The NMBI Directorate involved will provide the information to the Data Protection Officer. The forms can be sent separate or together, but must be sent within 72 hours.

The Data Protection Officer must also notify NMBI's President and CEO at this time.

The Board of NMBI will receive a verbal report from the Data Protection Officer and a copy of the Data Breach Notification Forms at the next Board meeting.

The Data Protection Commission will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Data Protection Commission request NMBI to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- a chronology of the events leading up to the loss of control of the personal data;
- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident; and
- the measures being taken to prevent repetition of the incident.

This report will be prepared by the NMBI Directorate involved and presented to the NMBI Board no later than two months after the initial breach notification to the Data Protection Commission, regardless of whether the Data Protection Commissioner requests the report at the time of the personal data security breach or closes the file.

9. Depending on the nature of the incident, the Data Protection Commission may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where NMBI has not already done so. If necessary, the Commissioner may use enforcement powers to compel appropriate action to protect the interests of data subjects.

10. The Data Protection Officer is responsible for maintaining the record and log of data breaches for the organisation.

Even where there is no notification of the Data Protection Commission, NMBI should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Data Protection Commission. Such records should be provided to the Data Protection Commission upon request.