Bord Altranais agus
Cnáimhseachais na hÉireann

Nursing and Midwifery Board
of Ireland

NMBI Data Protection Policy

NMBI Data Protection Policy

Context and Overview

Key Details

- Prepared by Dr Aoibhín de Búrca, Data Protection Officer: 08/05/2018
- Approved by Board: 23/05/2018
- Policy became operational on: 24/05/2018
- Next review date: 25/05/2019

Introduction

NMBI needs to gather and use certain information about individuals.

These can include registrants, student nurses and midwives, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet NMBI's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures NMBI:

- Complies with national data protection law and the General Data Protection Regulation (GDPR);
- Follows good practice;
- Protects the rights of registrants, staff and partners;
- Is transparent about how it stores and processes individuals' data; and
- Protects itself from the risks of a data breach.

Data Protection law

National data protection law and the GDPR describes how organisations – including NMBI – must collect, process and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by six important principles. These say that personal data must:

1. Be processed lawfully, fairly and transparently (lawfulness, fairness and transparency);
2. Be obtained only for specified, explicit and legitimate purposes (purpose limitation);

3. Be adequate, relevant and limited to what is necessary (data minimisation);
4. Be accurate and kept up to date (accuracy);
5. Be kept only for as long is necessary (storage limitation); and
6. Be processed with appropriate security (integrity and confidentiality).

People, risk and responsibilities

Policy scope

This policy applies to:

- NMBI staff
- NMBI Board and committee members
- All contractors, suppliers and other people working on behalf of NMBI.

It applies to all personal data NMBI holds. 'Personal data' means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data protection risks

This policy helps to protect NMBI from data security risks including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Reputational damage**. For instance, if NMBI had inadequate security regarding personal data.

Responsibilities

Everyone who works for, or with, NMBI has responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- **The Board** is ultimately responsible for ensuring that NMBI meets its legal obligations, including data protection.

- **The Data Protection Officer** is responsible for:

- Keeping the Board, CEO and SMT updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Providing legal processor agreements and amendments for staff to include in contracts where personal data is being processed.
- Arranging data protection training and advice for the people covered by this policy.
- Dealing with requests from individuals to see the data that NMBI holds on them (also called subject access requests).
- Communicating with, and acting as the key contact point with the supervisory authority (Data Protection Commission).

- **The IT Manager is responsible for:**
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third party services NMBI is considering using to store or process data. For instance, cloud computing services.

- **The CEO and SMT** are responsible for:
  - Ensuring that they, and staff in their department/unit are fully compliant with the policies.
  - Ensuring legal processor agreements and amendments are in place with contractors and suppliers where personal data is being processed.
  - Assisting their Data Protection Representatives with all necessary record keeping and documentation, and the data protection annual review.
  - Ensure data protection by design and default on all new projects and initiatives. Where sensitive personal data and special category data is being processed, ensure local policies are put in place that are suitable and specific.
  - Provide, or direct line staff to provide, information to the DPO in a timely manner, in the event of a data breach or subject access request.

General staff and members guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line manager.

- **NMBI will provide training and workshops** to all employees to help them understand their responsibilities when handling data. (All Data Protection Representatives will be certified in data protection.)
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should never be disclosed** to unauthorised people, either within NMBI or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to staff line managers, the IT Manager or the Data Protection Officer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer, locker or filing cabinet.**
- Employees, Board members and committee members should make sure paper and printouts are **not left where unauthorised people could see them**, like in a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is stored electronically, it must be protected from all types of breaches such as accidental or unlawful destruction, loss, alteration, and/or unauthorised disclosure:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or USB), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service**.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with NMBI's backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets and smart phones. If this does occur, delete it immediately.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

It is absolutely crucial to NMBI's mission that personal data held by NMBI is accurate: it is needed to maintain the Register of Nurses and Midwives, to investigate complaints, and to carry out site visits, as well as to perform contracts. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. If there are any concerns regarding the security of personal data, ask the IT Manager about the level of security before transferring the material.
- Personal data **must not be transferred** outside of the European Economic Area or to an international organisation, unless there is an adequate level of protection.
- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy

NMBI is required by law to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming details when a registrant calls or gets in contact.
- NMBI will make it **easy for data subjects to update the information it holds** about them, especially once the new Registrant system is live.
- Data should be **updated as inaccuracies are discovered**. For instance, if mail is returned the address should be removed from Miller.

Subject access requests

All individuals who are subject to personal data held by NMBI are entitled to:

- Ask **what information** NMBI holds and why;
- Ask **how to gain access**;
- Be informed about **how to keep their personal data up to date**; and
- Be informed about **NMBI's data protection policies**.

If an individual contacts a member of staff in NMBI looking for the personal data NMBI holds regarding them, this is a subject access request and should be sent immediately to the Data Protection Officer.

Subject access requests must be made in writing. They can be sent by postal address to Data Protection Officer, 18/20 Carysfort Avenue, Blackrock, Co Dublin, A94 R299 or by email to dataprotection@nmbi.ie.

There is no charge to make a subject access request.

A subject access request will be processed as quickly as possible, and in no longer than one month.

Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

NMBI's Subject Access Request Policy contains more detailed information on subject access requests.

Please note: All organisational email and electronic folders may be searched as part of a subject access request.

Disclosing data for other reasons

In certain circumstances legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, NMBI will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board and NMBI's legal advisers where necessary.

Pre-processing notices and transparency

NMBI aims to ensure that individuals are aware that their data is being processed, and that they fully understand in advance of processing how the data is being used and how to exercise their rights.

To these ends, NMBI has a privacy statement, setting out how data relating to individuals is used by the company and the statutory basis for doing so. This is available on request and on the NMBI website.