Data Protection & Confidentiality

Your personal responsibility

Northern Ireland mdta Medical & Dental Training Agency

Single Lead Employer
for Doctors & Dentists in Training

Following the transfer of your employment to NIMDTA Single Lead Employer, please take this opportunity to familiarise yourself with your responsibilities under the Data Protection Act (DPA, 1998) and, as updated, the General Data Protection Regulation (GDPR, 2018).

Good Medical Practice *Confidentiality is central to the doctor-patient relationship. Both the GMC and GDC make clear that patients have a right to expect that information about them will be held in confidence by their medical & dental professionals.*

Data Breaches can:

- *Cause distress to patients and their families;*
- *Cause reputational damage to you, NIMDTA and your Host Organisation;*
- *Incur fines of up to £500,000 under the DPA or over £17,000,000 under GDPR*

***All** employees of NIMDTA have:*

- *An ethical responsibility to protect confidentiality;*
- *A common law duty of confidence to their patients and employer;*
- *A personal responsibility to act according to the principles of data protection and confidentiality.*

Data Protection Legislation

The Data Protection Act 2018 is the framework for data protection law and is the UK's implementation of the General Data Protection Regulation (GDPR). It updates and replaces the Data Protection Act 1998.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'.

Data must be:

1. Used fairly, lawfully and transparently;
2. Used for specified, explicit purposes;
3. Adequate, relevant and limited to only what is necessary;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary;
6. Processed securely including protection against unlawful or unauthorised copying, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinion
- Religious belief
- Trade union membership
- Genetics
- Biometrics
- Health
- Sex or sexual orientation

During the course of your duties, you are likely to come into contact with a variety of sensitive information and your understanding of these principles is vital in ensuring both personal and organisational compliance with Data Protection Legislation.

Data Breaches

Many data breaches and inappropriate disclosures of information are **unintentional.**

To avoid this, care should be taken to ensure:

- *Password security – **never** share or write down your passwords;*
- *Account security – **never** share log in details such as usernames;*
- *Device security – **always** lock your computer/laptop or other device when unattended or not in use;*
- *Record security – **always** ensure physical records are not left in public view or accessed by unauthorised individuals*

Sharing Information

Access to information should be controlled and released on a 'need to know' basis in compliance with the legislation. Disclosure should be limited to only as much information as is necessary for the purpose or task intended.

Any personal information given or received in confidence for one purpose, may not be used for a different purpose, or passed to anyone else without the knowledge and consent of the individual (or if appropriate, their representative).

An individual has the right to withhold or restrict the transfer of their personal information, unless in designated circumstances where you have a duty to provide information for legal or statutory purposes or to protect the public.

The SLE Trainee Employment Team will issue you with an **@HSCNI email address**.
Your new email address will remain with you throughout your training in Northern Ireland.

We will use this as our primary means of communication with you, so please ensure that you check it regularly. It is also strongly advised that you use this email address during the course of your duties where the transmission of sensitive or confidential information will be required. Your Host Organisation may also provide a local trust email address, however please note that this may expire should you rotate to a placement with another trust.

Transporting Information

Staff must safeguard all confidential information while travelling between Host Organisations or sites, or through the use of third parties such as courier services. It is recommended that staff should avoid taking confidential information outside HSCNI sites wherever possible. However, it is accepted that there are certain circumstances where this will be unavoidable, for example:

- To facilitate care or treatment across HSCNI Trusts and Sites;
- To facilitate care or treatment in a recognised non-HSCNI organisation such as a Hospice;
- When attending meetings at another site or with another recognised organisation;
- For domiciliary visits
- To meet legal or statutory requirements;
- For home working where secure electronic means of transferring information are unavailable.

Information should be transported in a secure container and kept out of sight, for example, in the boot of a car. Personal information should never be left unattended in a public area.

You must also familiarise yourself with any local policies or procedures on Data Protection, confidentiality and records management as applicable in your Host Organisation.

If you have any questions or concerns regarding this issue, or any others relating to your employment, please contact the SLE Trainee Employment Team at ddit-nimdta@hscni.net

Further information also is available at:
https://www.gov.uk/data-protection

https://ico.org.uk/your-data-matters/