NIPEC/24/20

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Records Management Policy

July 2024

Any request for the document in another format or language will be considered

James House
2 – 4 Cromac Avenue
BELFAST
BT7 2JA

Tel: 0300 300 0066

https://nipec.hscni.net

Developed by:	Business Manager
Approved by / date:	**BTM:** 8th December 2020; 10th September 2024. **Council:** 31st December 2020; 18th September 2024.
Date of next Review:	July 2028
Equality Screened by / date:	Business Manager -June 2024

CONTENTS

1. Introduction and Policy Statement

All Health and Social Care (HSC) records are public records under the terms of the Public Records Act (NI) 1923 and in the Disposal of Documents (Northern Ireland) Order (1925). The Act sets out the broad responsibilities for everyone who works with such records, and as such, NIPEC has a statutory duty to make arrangements for the management and safekeeping of its records, and for the eventual disposal of its records.

Furthermore, information is a corporate asset and NIPEC's records are important sources of information in addition to administrative, financial, legal and historical information. They are vital to the organisation in its current and future work, for the purposes of accountability, and for an awareness and understanding of its history. They are the corporate memory of the organisation.

Records Management is the process by which NIPEC will manage all aspects of its records, from their creation all the way through their lifecycle to their eventual disposal or permanent preservation (known as the 'records lifecycle').

Good records' management is therefore critical in order to evidence its strategic objectives, as set out within its annual quality reports. NIPEC is therefore committed to the creation, maintenance and management of its records and the documentation of its principal activities.

This policy should be read in conjunction with the following NIPEC policies and other guidance:

- Information Governance Policy with IG Framework
- Adverse Incident Policy
- Retention Disposal Schedule
- Data Protection Policy
- Clear Desk and Screen Policy
- FOI Policy
- ICT Security Policy
- Operational Procedure for NIPEC's filing system

2. Purpose and Aims

The purpose of this policy is to ensure that NIPEC adopts best practices in the management of its records so that authentic, reliable and useable records are created, maintained and managed, which are capable of supporting business functions and activities for as long as they are required and which assist to support and evidence its strategic objectives.

Compliance with this policy will help NIPEC ensure that:

- records are present, accurate and complete;
- the record provides a reliable and accountable representation of business activity and, if relevant, provides the rationale behind the decision-making process;
- effective filing systems are maintained that support improved information retrieval methods;
- records are made accessible to enable well-informed and appropriate judgements to be made;
- records are kept securely and protected from accidental loss, destruction and unauthorised access;
- records are kept for no longer than is necessary, in accordance with legal and professional obligations and with due regard to the regionally agreed retention and disposal schedule known as Good Management, Good Records;
- staff are made aware of and trained in the management of records within their sphere of work or responsibility.

Compliance with this policy will ensure that NIPEC can provide evidence of performance and demonstrate accountability, as well as providing information about its decisions and activities.

3. Scope

The international standard of managing records, ISO 15489 defines a record as *"information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".*

In the context of this policy a record is any recorded information that contains information, in any media which is created, collected, processed, used stored and/or disposed of by NIPEC employees, as well as those acting as its agents in the course of NIPEC business.

This policy applies to **all staff**. In this document, the term 'all staff' refers to regular full-time, regular part-time, associates, contractors, consultants, agency staff and temporary employees and third-party service providers acting on behalf of NIPEC.

4. Roles and Responsibilities

The **Council** has overall responsibility to ensure compliance in all areas of information governance, including records management.

The **Chief Executive** and **Senior Team** have a duty to ensure that NIPEC complies with the requirements of legislation affecting management of the records. They will oversee the effective record management within NIPEC, and with **designated NIPEC staff**, have a duty to ensure that NIPEC complies with the requirements of legislation affecting the management of records and with supporting regulations and codes.

The **Personal Data Guardian (PDG)** is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

The **Senior Information Risk Officer (SIRO)** is a senior manager who has responsibility to ensure compliance with legislation through the development and monitoring of policy and codes of practice. The SIRO is supported in this role by Information Asset Owners (IAOs) who must provide assurance to the SIRO that information risk is managed effectively for the information assets that they own.

The Data Protection Officer will work closely with NIPEC to ensure that there is consistency in the management of records and that advice and guidance on good records management practice is provided throughout the organisation. NIPEC's Data Protection service is provided by the Business Services Organisation via an annual SLA.

The **Information Governance Group** is responsible for maintaining the accuracy and relevance of this policy and providing assurance to NIPEC's Business Team and Council as to its implementation and effectiveness. They will work closely with all staff to ensure that there is consistency in the management of records and that advice and guidance on good records management practice is provided throughout the organisation.

All members of NIPEC staff are responsible for documenting their actions and decisions in the records and for maintaining records in accordance with section 5 of this policy. They have a duty to protect and ensure that any information they add to the record is necessary, accurate and complete. The confidentiality of client and staff records must always be of primary concern to NIPEC staff.

All staff are responsible for:

- ensuring they have a clear understanding of records management and demonstrate commitment to duties relating to record keeping;
- creating records which are consistent, reliable, accurate and complete;
- capturing records which authentically document activities in the course of which they were produced;
- accessibility of a record: filing records correctly in the appropriate area of NIPEC's filing system on the server;
- applying security and access controls to records where appropriate;
- identifying and applying appropriate disposal and retention periods to records.

5. Records Filing Structure

NIPEC's records are stored electronically on a central server. In the past NIPEC maintained a dual manual and electronic filing system, however, in April 2017, it was agreed NIPEC would move to a paper-lite system and as a first step, cease creating paper based/manual folders in which to store records.

The Head of Corporate Services will monitor the storage and retention of NIPEC's records and, through the **Information Governance Group,** ensure NIPEC's Operational Procedure for its filing system and guidance within GMGR is updated, shared and being followed by all staff.

6. Confidentiality and Access

All of NIPEC records are public records and are therefore subject to a number of statutory provisions regarding confidentiality, access and disclosure.

Specific guidance on matters of data protection and confidentiality can be found in NIPEC's Data Protection Policy.

The Freedom of Information Act (2000) and Environmental Information Regulations (2004) provide members of the public with a general right of access to information held by public authorities which includes NIPEC. NIPEC's Freedom of Information Policy covers this aspect of records' management.

7. Retention and Disposal of Records

All records should be retained and disposed of in accordance with the Department of Health's Good Management, Good Records (GMGR).

A regular quality check / audit of NIPEC's filing system, at least once every two years, will be undertaken. In liaison with NIPEC's Business Team and approval of the Chief Executive, relevant electronic files will be archived, disposed of, and, where relevant, forwarded to PRONI for permanent preservation. However, no information should be destroyed if it is the subject of a current request under relevant legislation, or any other legal process such as an inquest or public inquiry.

A record of destruction should be maintained.

8. Specific Record Types: Email

Personal email accounts tend to be structured according to personal preference. The data held within an email account is not routinely searchable or organised in a systematic way, making email accounts unsuitable for record storage purposes.

Email accounts should therefore not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents.

Documents distributed by email that need to be retained as NIPEC records should be moved to the electronic filing system and the email copy destroyed as soon as is practicable.

Where email is declared as a record, the entire email must be retained, including attachments, so the record remains integral – e.g. email approving a business case.

9. Specific Record Types: Scanned Records

Where paper records are scanned, the main consideration is that the information can perform the same function as the paper counterpart did, and like any evidence, scanned records can be challenged in a court.

Provided scanning is carried out to an acceptable standard, and quality assured, original documents should be destroyed after scanning, in order to prevent duplication.

10. Monitoring Compliance

Monitoring of compliance with this policy will be undertaken by NIPEC's Information Governance Group, reporting any issues to NIPEC's Business Team in order to agree any changes required or action to be taken.

A failure to adhere to this policy and any associated procedures may result in disciplinary action.

11. Equality

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998.

The screening has identified no significant equality implications have been identified therefore the policy will not be subject to an equality impact assessment.

The equality screening has been published and can be accessed here:
https://bso.hscni.net/directorates/people-and-place/655-2/equality-and-human-rights-screening/equality-screening/