



Feidhmeannacht na Seirbhíse Sláinte  
Health Service Executive



## National Ambulance Service (NAS)

### Business Support Policy for Records Management

Document reference number	<b>NASBS010</b>	Document developed by	NAS HQ
Revision number	<b>4</b>	Document approved by	<b>Martin Dunne Director of NAS</b>
Approval date	<b>28<sup>th</sup> May 2012</b>	Responsibility for implementation	<b>Each Senior Manager</b>
Revision date	<b>31<sup>st</sup> December 2019</b>	Responsibility for review and audit	<b>Business Manager</b>

**Table of Contents:**

<b>1.0</b>	<b>Policy</b>
<b>2.0</b>	<b>Purpose</b>
<b>3.0</b>	<b>Scope</b>
<b>4.0</b>	<b>Legislation/other related policies</b>
<b>5.0</b>	<b>Glossary of Terms and Definitions</b>
<b>6.0</b>	<b>Roles and Responsibilities</b>
<b>7.0</b>	<b>Procedure</b>
<b>8.0</b>	<b>Implementation Plan</b>
<b>9.0</b>	<b>Revision history</b>
<b>10.0</b>	<b>Appendices</b>
<b>11.0</b>	<b>Signatures of Approval</b>

## **1.0 POLICY**

- 1.1 It is the policy of the National Ambulance Service (NAS) that a systematic, planned and controlled approach will be operated in relation to the management of records. This is to ensure that the information gathered by the NAS is of the highest quality and that it is treated confidentially. The record effectively serves the need for which it was created and is disposed of when it is no longer required in accordance with the Retention of Records policy.

## **2.0 PURPOSE**

- 2.1 To ensure a safe and secure handling of records to protect patients, staff, and financial resources.
- 2.2 To describe the safe and secure system for the control and handling of all records in the NAS within a framework provided by legislation and official guidance.

## **3.0 SCOPE**

- 3.1 This Policy applies to all Managers, Supervisor and Staff in the NAS.
- 3.2 This policy applies to all records in any format generated, received, held or managed by the NAS

## **4.0 LEGISLATION/OTHER RELATED POLICIES**

- A. Code of Practice for Healthcare Records Management 2007
- B. Data Protection Data Security Guidance 2010
- C. HIQA National Standards for Better Safer Healthcare
- D. Health Act 2004
- E. Data Protection Acts 1988 and 2003.
- F. Freedom of Information Acts 1997 and 2003.

## **5.0 GLOSSARY OF TERMS AND DEFINITIONS**

### **5.1 What is a Record?**

- 5.1.1 A record is defined as any document, memorandum, plan, map, diagram, pictorial or graphic work, photograph, film or recording (whether of sound or images or both).
- 5.1.2 It is also any form in which data (within the meaning of the Data Protection Acts 1988 and 2003, including machine readable form), are held in which information is held or stored manually, mechanically or electronically.
- 5.1.3 A record is anything that is a part or a copy, in any form of any of the foregoing or is a combination of two or more of the foregoing (Freedom of Information Acts 1997 and 2003).

## **5.2 Service Records**

### **5.2.1 Service records include:**

- A. Computerised patient records on the Ambulance Control System.
- B. Administrative records (including personnel, estates, financial and accounting records and notes associated with complaints handling).
- C. Photographs, slides and other images.
- D. Audio recordings in relation to transmission systems, cassettes, CD-ROM, etc.
- E. Computer databases, output and disks, etc. and all other electronic records.
- F. Fleet Management records including VDI Forms, Vehicle/Equipment Defect Forms and Equipment maintenance contracts.
- G. Quality/Performance records that demonstrate that a Quality System is in place, including internal and external audit reports, Key Performance Indicator reports, management review reports etc.
- H. Typed and printed information, letters and reports, whether received from outside organisations, other services within the HSE or have been sent from services.
- I. Training records including records of attendance and examination results.

5.2.2 The guidance applies to any material, which holds information gathered as part of your work in the HSE and this list is not exhaustive. It is important to remember that the ownership and copyright of these records is with the HSE, not with any individual employee.

## **5.3 Clinical Records**

5.3.1 Clinical records relate to information gathered in connection with a person who is/has been treated by the NAS. This includes information in relation to any or all of the following:

- A. Patient Care Records and 12 Lead ECG Transmissions
- B. Demographic information
- C. Information relating to the person's past and present physical and mental history, assessments and treatments
- D. Information relating to the person's contacts with social, legal, judicial, prison, probation and any other relevant services
- E. Information on the person's family, relations and friends
- F. Any other information relating to the person
- G. Information received in traditional hard copy or electronic format received from other parties in relation to the person about whom the record exists, e.g. G.P. letters
- H. Records of Drug administration, including controlled drugs

5.3.2 Clinical Records include information obtained and recorded by the following persons:

- A. Clinical Personnel (health and related professionals) in the HSE
- B. Non Clinical Service Personnel in the HSE
- C. Clinical/Non Clinical Personnel from other Services outside the HSE

#### **5.4 Abbreviations**

- PCR – Patient Care Report
- CPG – Clinical Practice Guidelines
- CD – Controlled Drug
- PIN – Personal Information Number

#### **5.5 Controlled Drugs**

For the purposes of this policy, a controlled drug (CD) is a drug named in Schedule 2 (CD2) or schedule 3 (CD3) of the regulations under the Misuse of Drugs Acts 1977 and 1984 and any amendments, and also any drugs which it is considered necessary to control for risk management reasons.

### **6.0 ROLES AND RESPONSIBILITIES**

6.1 The HSE is placing an emphasis on achieving a more open and accountable public service. One of the most important contributors to this process is to have an effective records management structure in place with appropriately defined responsibilities.

6.2 Responsibilities can be defined under the following headings:

#### **6.2.1 Statutory Responsibility**

- A. There are many references in legislation to record creation; however, few refer to record management as a whole. These legislative documents, which must be complied with include, Data Protection Acts 1988 and 2003, National Archives Act 1976 and the Comptroller and Auditor General (Amendment) Act 1993.
- B. The provisions contained in the Health Act 2004 also outline specific responsibilities. These statutory requirements place an onus of responsibility on the HSE to provide for the safekeeping and maintenance of its records.
- C. This duty is strengthened by the introduction of the Freedom of Information Acts 1997 and 2003, which allows the public access to records, amendment of records and also obliges the HSE to give reasons for decisions.
- D. Another requirement of the Freedom of Information legislation is that public bodies must publish details of the classes of records maintained by each service including the NAS.

## **6.2.2 Managerial Accountability and Responsibility**

The Director and each Senior Manager are accountable for the quality of records within their respective spheres of responsibility. However, commitment is required from all staff in:

- A. Ensuring the NAS operates a systematic and regulated approach to record management and that individual locations support any such development.
- B. Ensuring that staff are aware of, and apply the appropriate guidelines in relation to record management e.g. confidentiality, privacy, access, maintenance and storage guidelines.
- C. Familiarising themselves with relevant NAS and HSE Protocols
- D. Ensuring that policies and procedures are adopted and adhered to in routine daily activities within each location

## **6.2.3 Individual Responsibility**

Every individual is responsible for any records they create and use as defined by law. Every person working for the NAS who records, handles, stores or otherwise comes across information has a duty of confidentiality.

## **7.0 GUIDELINES**

### **7.1 Best Practice Guidelines in Record Management**

- 7.1.1 A record should correctly reflect all important and relevant information, making sure that it is complete.
- 7.1.2 Records should support the needs of the NAS to which it relates and be used for accountability purposes.
- 7.1.3 Records must be authentic in that they can be proven to:
  - A. Be what it purports to be
  - B. Have been created by the person purported to have created it.
  - C. Have been created at the time purported
- 7.1.4 Records must be reliable. A reliable record is one whose contents can be trusted as a full and accurate representation of the actions to which they attest.
- 7.1.5 Records must be legible so that they can be easily read and reproduced when required. Records must be clear and unambiguous.
- 7.1.6 Any required alterations must be made by scoring out the error with a single line followed by the correct entry, which must be signed, dated and timed. Alterations should not be obliterated by tippex, ink or any other means. Additions to existing entries in a record must be dated, timed and signed.
- 7.1.7 Records must not include abbreviations, meaningless phrases and offensive subjective statements unrelated to the purpose of the record.
- 7.1.8 The use of initials for major entries is not permissible and where their use is allowed for other entries, arrangements for identifying initials and signatures must exist. Samples of initials and signatures for both past and present staff must be maintained.

- 7.1.9 Entries in records must not be made by pencil (carries risk of erasure).
- 7.1.10 Records must be useable. A useable record is one that can be located, Retrieved, presented and interpreted. Records must be stored in such a way as to facilitate easy retrieval and to minimise the potential for deterioration and loss.

## **7.1 Best Practice Guidelines in Record Management**

7.1.1 The principles of good practice for PCRs are:

- A. The patient/client should be clearly identified and the PCR should set out assessment, history and treatment.
- B. PCRs should be kept neat and tidy with legible entries recorded and dated in black ink. Similarly, printed electronic records should be in black ink.
- C. PCRs should be kept up to date and filed in chronological order with the most recent on top.
- D. PCR folders and the content should have clear order, and should be organised chronologically.
- E. PCRs should be scanned one month in arrears based on a minimum data set of characters to facilitate ease of retrieval and access
- F. The standard of record keeping of Post Graduate Interns under supervision should be monitored by the registered Practitioner charged with responsibility for the mentoring of her/his delegate.

## **7.2 Quality of Record Keeping**

7.2.1 The quality of record keeping can be further assessed using standards, which were produced from the above principles based upon good practice concerning legibility, patient identification, Practitioner interventions, confidentiality and storage of PCRs.

7.2.2 The standards are as follows:

- A. The PCR is clear and unambiguous
- B. The patient is identifiable
- C. The PCR is tidy
- D. The PCR folder is in a good state of repair
- E. PCRs are accurate in each entry as to date and time
- F. PCR is completed as soon as possible after the event to which it relates
- G. All PCRs contain the responding Practitioners PIN number(s). Author identification is by means of a hand-written signature.

## **7.3 Creating Records / Temporary Files**

The NAS must be clear on the nature and the purpose of the records that it creates and retains.

## Records:

- A. Preserve the NAS memory, which ensures that informed decisions are made by personnel and it facilitates their successors.
- B. Provide evidence of Patient treatment.
- C. Inform management/staff of significant happenings in the NAS.
- D. Provide evidence of completed ambulance calls.
- E. Provide for legal compliance requirements.

### 7.4 File Level Operations

Guidance for staff in the following areas:

#### 7.5 Opening new files

Before opening a file:

- A. Determine that there is a need to open a file e.g. files should not be opened for the storage of non-record material
- B. When opening **PCR files** they should be given an identifying chronological period.
- C. Creation of files should be restricted to authorised personnel.
- D. Ensure that a file with the same or similar subject does not already exist.
- E. Duplicate files should not be opened and where it is necessary to open one, every effort should be made to merge this file with the master file as soon as is reasonably achievable.

#### 7.6 Day-to-day Management of Files

Staff should follow the best practice principles outlined in sections 7.1 And 7.2.

#### 7.7 Opening Successor Files

- 7.7.1 Additional volume of files must be created once a file has reached a defined depth (38mm or one and a half inches).
- 7.7.2 The creator of the successor volume must be familiar with procedures for transfer of information from one record to the subsequent volume.
- 7.7.3 Once an additional volume is created, the previous volume must be marked 'closed' and dated. Current information should only be added to the latest volume.

#### 7.8 Opening Temporary Files

- 7.8.1 Temporary files may only be created for emergency situations when an original file cannot be located.
- 7.8.2 Temporary files used by the service must be consistent and easily recognisable.

- 7.8.3 Only NAS, Area or NASC H.Q. personnel have the authority to create temporary files.
- 7.8.4 The current status of temporary files must be recorded i.e. creation and closing (when merging with the original file or a new file is created).
- 7.8.5 Staff must make every effort to locate the original file and the temporary file should be amalgamated with it in a timely fashion.
- 7.8.6 If it is established that there is no existing file, then the temporary file must be converted to a permanent file.
- 7.8.7 Appropriate follow up action should be taken once the location of the original file is established i.e. who/what location was holding the file and for what reason.

## **7.9 Transportation of Records including PCR Folders**

- 7.9.1 On occasion it will be necessary to transport records or PCR files to a location other than that where it was initially stored.
- 7.9.2 In the event that records or PCR files are being transported between locations:
  - A. An authorised NAS staff member must conduct the transportation of the record or PCR File.
  - B. The staff member conducting the transfer is responsible for the record or PCR file whilst in their charge and is responsible for safe delivery.
  - C. Transported records must be carried in a storage case, box file or sealed envelope where the name on the record(s) cannot be identified.
  - D. Records must not be left unattended in an ambulance or staff car.
  - E. On arrival at the appropriate location the record should be delivered directly to the charge of the appropriate person.

## **7.10 Storing Paper Records Efficiently**

- 7.10.1 The safety and quality of records are of prime importance. Knowing how long the records will need to be kept (refer to Section 7.18) and maintained will affect decisions on storage media.
- 7.10.2 The records system must address disaster preparedness to ensure that risks are identified and appropriately addressed.

## **7.11 Deterioration and Loss**

- 7.11.1 Records must be stored in such a way that minimises the potential for deterioration and loss.
- 7.11.2 Records must be stored away from and protected from the hazards of fire, flooding, humidity, atmospheric pollution, noise and vandalism.
- 7.11.3 Records must be stored in such a way that ensures that the record remains intact and is usable throughout its lifetime.
- 7.11.4 Records must be stored in areas that are suitable for the storage of records and must comply with health and safety regulations.

## **7.12 Rapid Retrieval and Easy Access**

- 7.12.1 The location of records must facilitate the rapid retrieval and access to records and must suit the needs of the user.
- 7.12.2 Where a record is in constant or regular use, or is likely to be needed quickly, the record should be kept within the location responsible for its creation.
- 7.12.3 Storage equipment for current records should be adjacent or close to the person using the file so that the file can be easily retrieved when it is next required.
- 7.12.4 PCR Files should be scanned monthly in arrears to ensure compliance with best practice guidelines and ease of retrieval and access to information

## **7.13 Safe Retrieval**

- 7.13.1 The storage of records or PCR files must facilitate the safe retrieval of records by any authorised staff member.
- 7.13.2 Records and files must be stored at a height that can be safely reached by all staff required to do so.
- 7.13.3 Storage facilities that require the retrieval of records/files by climbing must be avoided.

## **7.14 Security and Confidentiality**

- 7.14.1 Any storage facilities used must ensure the security and confidentiality of the records or PCR Files being stored.
- 7.14.2 When a room/building containing records is left unattended, it should be locked.
- 7.14.3 Only appropriate staff should receive access to records and files.
- 7.14.4 All personnel with access to records and files must agree to meet any Confidentiality requirements. The confidentiality of the patient must be maintained at all times. Everyone who handles stores or otherwise comes across patient information has a personal common law duty of confidence to the patient and to his/her employer. This duty of confidence continues even after the death of the patient or if an employee has left the HSE.
- 7.14.5 There are measures in place to deal with any breaches in confidentiality by personnel.
- 7.14.6 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 consent of the provider of this information, subject to the terms and exemptions set out in Data Protection and Freedom of Information legislation.
- 7.14.7 Where staff access patients' records for the purposes of training or audit, they may do so only if the information is anonymised so that the individual patients cannot be identified.

## **7.15 Visual Records**

- 7.15.1 The NAS has a small collection of still photographs (which may be prints, negatives, slides, transparencies and electronic-readable images) or as moving images (video or film).
- 7.15.2 The teaching and historical value of photographs should be considered. Some of this material may be considered for permanent preservation.

## **7.16 Information Technology**

- 7.16.1 Increasingly information technology is being introduced into the NAS. This trend of producing documents electronically places new demands on managing records.
- 7.16.2 There is also an increase in the use of electronic transfer using the Intranet and Internet networks.
- 7.16.3 Management needs to be aware of and address the implications for backup copies of electronic records and security.
- 7.16.4 The principles of good record management apply equally to records created electronically and to those created in other formats. It is important to remember that it is the content or information, and not the mode of delivery that classifies a record.

## **7.17 Archiving Of Records (Post 1971)**

- 7.17.1 Healthcare records should be retained in line with the HSE Code of Practice on Healthcare Records Management.
- 7.17.2 PCR Records are recommended for retention for a minimum period of 10 years from the date of creation of the original PCR
- 7.17.3 Clinical Audit Records should be retained for a minimum period of 5 years.
- 7.17.4 Records of Serious Untoward Incidents should be retained for a minimum period of 30 years from the date of the original incident.
- 7.17.5 Records of Procurement should be retained for a minimum period of 11 years.

## **7.18 Disposing Of Unwanted Records**

- 7.18.1 No matter how desirable it is to retain a record in its original format, the reality is that there is limited resources and storage capacity available. The NAS must aim to balance the cost of indefinite storage against the costs that may arise following an action resulting from the service not having a record to support its defence.
- 7.18.2 A record, from its creation, moves through a series of phases in its lifecycle. These phases known collectively as the record 'Retention Schedule' are active, semi-active and finally inactive.
- 7.18.3 The length of the retention period depends upon the type of record, its importance and adherence to legislation. The HSE Code of Practice on Healthcare Records Management takes into account legal requirements and sets out the **minimum** retention periods.

7.18.4 It also highlights issues which need to be considered prior to the policy being implemented. These are:

- A. Recommended minimum retention periods should be calculated in line with the recommended Retention Schedule for each type of record.
- B. Local requirements/instructions must be considered before activating retention periods.
- C. Decisions should also be considered in the light of the need to preserve records, whose use cannot be anticipated fully at the present time, but which may be of value to future generations.
- D. On-going legislative requirements.

## **7.19 Who makes the Decision?**

7.19.1 There are two principle options – to destroy or to dispose. Some records have fixed retention periods, whilst others will need more careful consideration.

7.19.2 The relevant Senior Manager is responsible for making sure that all records are periodically and routinely reviewed to decide what can be disposed of in accordance with the HSE Code of Practice on Healthcare Records Management.

## **7.20 What are the Options?**

7.20.1 Disposal does not necessarily mean destruction. There are a number of options to consider before finally agreeing on a specific method.

7.20.2 These options include:

- A. Off-site storage
- B. On-site storage
- C. Computer/Digitised storage
- D. Destruction (shredding, pulping, incineration)

## **7.21 What are the Rules of Destruction?**

7.21.1 Most NAS records, even administrative ones contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method of destruction used is fully effective and secures complete illegibility.

7.21.2 The NAS is responsible for ensuring that the methods used throughout the process provide adequate safeguards against accidental loss, or disclosure of information. A record of the files destroyed should be maintained.

## 7.22 Release of Information

7.22.1 The NAS may release information from records in the following situations:

- A. Request of information for clinical purposes (PCR)
- B. Request for information for administrative, legal and quality purposes
- C. In an emergency situation
- D. For education purposes

## 8.0 IMPLEMENTATION PLAN

- 8.1 This Policy will be circulated electronically to all Managers, all Supervisors and Staff
- 8.2 This Policy will be available in electronic format in each Ambulance Station and Ambulance Control for ease of retrieval and reference
- 8.3 Each Operational Support and Resilience Manager will ensure that the Manager/Supervisor responsible for updating Policies and Procedures will return the Confirmation Form to NAS Headquarters to confirm document circulation to all staff

## 9.0 REVISION AND AUDIT

- 9.1 This Policy will remain under constant review and may be subject to change to facilitate any changes/developments in service requirements.
- 9.2 Random audits of records held at Headquarters, Control and Station level.
- 9.3 Inspections by regulatory bodies may review NAS compliance with this Policy

### Revision History:

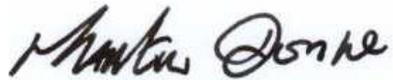
(This captures any changes that are made to a SOP when it has been revised. This may be placed at the back or close to the front of the document according to local preference.)

No	Revision No	Date	Section Amended	Approved by
1	4	03/01/2017	5.2.2	Business Manager

## 10.0 APPENDICES

### Appendix I – Document Control Forms 1-3

## 11.0 Signatures of Approval



---

National Ambulance Service Director  
On Behalf of the National Ambulance Service

Date 3<sup>rd</sup> January 2017

**Document Control No. 1 (to be attached to Master Copy)**

**NASBS010 Business Support Policy Records Management**

**Reviewer:** The purpose of this statement is to ensure that a Policy, Procedure, Protocol or Guideline (PPPG) proposed for implementation in the HSE is circulated to a peer reviewer (internal or external), in advance of approval of the PPPG. You are asked to sign this form to confirm to the committee developing this Policy or Procedure or Protocol or Guideline that you have reviewed and agreed the content and recommend the approval of the following Policy, Procedure, Protocol or Guideline:

**Title of Policy, Procedure, Protocol or Guideline:**

**NASBS010 Business Support Policy Records Management**

I acknowledge the following:

- I have been provided with a copy of the Policy, Procedure, Protocol or Guideline described above.
- I have read Policy, Procedure, Protocol or Guideline document.
- I agree with the Policy, Procedure, Protocol or Guideline and recommend its approval by the committee developing the PPPG.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Signature (Block Capitals)

\_\_\_\_\_  
Date

**Please return this completed form to:**

**Name:** Niamh Murphy  
**Contact Details:** Corporate Office  
National Ambulance Service  
Rivers Building  
Tallaght Cross  
Dublin 24  
email [niamhf.murphy1@hse.ie](mailto:niamhf.murphy1@hse.ie)

**Document Control No. 2 (to be attached to Master Copy)**

## Key Stakeholders Review of Policy, Procedure, Protocol or Guidance Reviewer Statement

**Reviewer:** The purpose of this statement is to ensure that a Policy, Procedure, Protocol or Guideline (PPPG) proposed for implementation in the HSE is circulated to Managers of Employees who have a stake in the PPPG, in advance of approval of the PPPG. You are asked to sign this form to confirm to the committee developing this Policy or Procedure or Protocol or Guideline that you have seen and agree to the following Policy, Procedure, Protocol or Guideline:

**Title of Policy, Procedure, Protocol or Guideline:**

**NASBS010 Business Support Policy Records Management**

I acknowledge the following:

- I have been provided with a copy of the Policy, Procedure, Protocol or Guideline described above.
- I have read Policy, Procedure, Protocol or Guideline document.
- I agree with the Policy, Procedure, Protocol or Guideline and recommend its approval by the committee developing the PPPG.

\_\_\_\_\_  
Name

\_\_\_\_\_  
Signature (Block Capitals)

\_\_\_\_\_  
Date

**Please return this completed form to:**

**Name:** Niamh Murphy  
**Contact Details:** Corporate Office  
National Ambulance Service  
Rivers Building  
Tallaght Cross  
Dublin 24  
email [niamhf.murphy1@hse.ie](mailto:niamhf.murphy1@hse.ie)

