Business Services Organisation

Records Management Policy

Reference No:	**BSO-CS 9**
Version:	**1.1**
Ratified by:	**BSO Board**
Date Ratified:	**August 27th 2015**
Date Equality Screened:	**July 6th 2015**
Name of Originator/Author	**Scott Stevenson**
Name of responsible committee/individual	**Information Governance Management Group**
Date Issued:	**September 4th 2015**
Review date:	**September 2018**
Target Audience:	**All BSO Staff**
Distributed Via:	**Email, Intranet, Hard Copy**

Amended by:	
Date amendments approved:	

Contents

1.0 Introduction

1.1 This policy provides for:

a. The requirements that must be met for the records of the Business Services Organisation to be considered as a proper record of the activity of the organisation, including the provision of health and social care services by or on behalf of the BSO.

b. The requirements for systems and processes that deal with records.

c. The requirements for the disposal of records

d. The quality and reliability which must be maintained to provide a valuable information and knowledge resource for the organisation.

e. Review of the policy and checking the quality of implementation.

f. An overall statement of records management policy which is supplemented by detailed procedures.

1.2 It covers records in all formats; electronic or paper, created, collated, processed used, stored and/or disposed of in the course of BSO business.

1.3 The International Standard of Managing Record 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."

1.4 This policy should be read in conjunction with the following:

- BSO policies and procedures on Information Governance
- The relevant ICT policies.
- The relevant Legislation and guidance

a. Public Records Act (NI) 1923

b. Disposal of Documents Order No 167, 1925

c. Limitation Act 1980

d. Freedom of Information Act 2000

e. International Standard on Records Management (ISO 15489)

f. Electronic Records Management: Toolkits (PRO, 2000-2002)

g. Data Protection Act 1998: A Guide for Records Managers and Archivists (PRO, PRONI, NAS, in association with ODPC, 2000)

h. Records Management Standards and Guidance (PRO, from 1998)

i. Northern Ireland Records Management Standards (NIRMS) (2002) (Public Records Office of Northern Ireland)

j. The Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information.

k. Good Management, Good Record, Guidelines for Managing Records in Health and personal Social Services Organisations in Northern Ireland, DHSSPSNI

l. Human Rights Act 1998

m. Office of the Ombudsman – The importance of good record keeping

2.0 Policy Statement

2.1 Information is a corporate asset and the records of the Business Services Organisation are important sources of patient and client information in addition to administrative, fiscal, legal, evidential 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.

2.2 In consultation with organisations that may be concerned with the management of its records, the Business Services Organisation will create, use, manage then destroy or preserve its records in accordance with all statutory requirements.

2.3 Systematic records management is fundamental to organisational efficiency. It ensures that the correct information is:

- captured, stored, retrieved and destroyed or preserved according to need
- fully utilised to meet current and future needs, and to support change
- accessible to those who need to make use of it; and
- that the appropriate technical, organisational and human resource elements exist to make this possible.

2.4 The records management systems within the constituent parts of the BSO will ensure that:

- **The record is present**

  The Business Services Organisation has the information that is needed to form a reconstruction of activities or transactions that have taken place.

- **The record can be accessed**

It is possible to locate and access the information and display it in a way consistent with initial use.

- **The record can be interpreted**

It is possible to establish the context of the record; who created the document, during which business process, and how the record is related to other records.

- **The record can be trusted**

The record reliably represents the information that was actually used in or created by the business process, and its integrity and authenticity can be demonstrated.

- **The record can be maintained through time**

The qualities of accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of formats

- **The record is made accessible to those who need to make use of it**

The record is maintained in such a way that it is available to those who need it.

2.5 All staff of the Business Services Organisation who create, use, manage or dispose of records have a duty to protect them and to ensure that any information that they add to the record is necessary, accurate and complete. The confidentiality of patient and client records must always be of primary concern to Business Services Organisation staff. All staff involved in managing records will receive the necessary training and formally acknowledge their duty of care with regard to Business Services Organisation records.

2.6 The records management policy is a specific part of the Business Services Organisation's overall Corporate Information Governance strategy and relates to other policies. The BSO Information Governance Management Group (IGMG) are responsible for maintaining the accuracy and relevance of this policy and providing assurance as to its effectiveness through a structured records management audit plan.

2.7 Electronic Records

2.7.1 Decisions to move from paper based records to electronic records will require SMT and Board agreement. Any decision to move from paper based records will require electronic systems to meet the requirement of the British Standard BS 10008. This is to ensure the authenticity of records can be demonstrated within legal proceedings.

2.7.2 Electronic based records can only be disposed of in accordance with procedures set out in GMGR and the guidance of the Public Record Office (NI).

2.8 The difference between Records and Documents

When handling any type of record, it is important to make the distinction between a record and a document. In the context of records management a document becomes a record

when it has been finalised and becomes part of an organisation's corporate information. At this point, the record should not be amended and should only be held in the corporate system in the appropriate records management system. In its simplest form a record is static and a document is live.

3.0 Accountability

3.1 The role of the **Board** is to oversee the effective record management by officers of the BSO.

3.2 The **Chief Executive** and **Directors** have a duty to ensure that the Business Services Organisation complies with the requirements of legislation affecting management of the records and with supporting regulations and codes.

3.3 The **Administrative Services Manager** on behalf of the **Director of Human Resources and Corporate Services** will be charged with Corporate Records Management responsibilities and will work closely with all Directorates 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. The ASM will co-ordinate the Information Governance Management Group. The need to establish a coordinating group specific to Records Management will be kept under review.

3.4 **Senior Managers** and **Line Managers** will ensure that records are managed effectively in each service area in accordance with this policy. They are responsible for ensuring staff members are aware of their responsibilities under this policy and local records management procedures. Specifically they will be responsible for ensuring that;

- Any policies, procedures or protocols agreed by the BSO are implemented within their area;
- Appropriate employees are designated to assist with the implementation of records management procedures within their area;
- Employees are supported in terms of training and development in their adherence to the Records Management Policy and procedures;
- Personal information is not kept longer than is necessary. (Information about individual patients may not be passed on to others without the individual's consent except as permitted under Schedule 2 and 3 of the Data Protection Act 1998) and relevant data sharing protocols issued by DHSSPS;
- Staff know what to record, how to record and why to record
- An inventory of records is maintained which shows the nature and type of records within service function, activity and directorate, is accessible to users and indicates the specific retention periods for those records; and
- Staff who record, handle, store or otherwise comes across patient information are aware that they have a common law duty of confidence to patients. Such a duty will continue even after the death of a patient;

3.5 All members of **staff** are responsible for documenting their actions and decisions in the records and for maintaining the records in accordance with good records management practice and professional guidelines and need to ensure that the:

- Records are opened and closed in accordance with local requirements
- Records can be accessed;
- Records can be interpreted;
- It is possible to establish who created the document;
- Records are processed in accordance with policies;
- Records can be trusted;
- Records can be maintained through time;
- The need for the records are regularly reviewed
- Records are disposed of in accordance with the agreed disposal schedule

"Good Management Good Records" will be made available to all staff on the Intranet and by internet access to the DHSSPS website. Requests for alternative formats will be considered.

"A guide to Good Record Keeping" (see Appendix A) will similarly be made available.

4.0 Records Registration

4.1 Records registration ensures a link between the record and its administrative roots. Each Directorate must ensure that they have reviewed all records groups held and that an appropriate and full entry is made on the Corporate Record Survey hosted on the Information Governance Share Point Site. The BSO will undertake a full review of the records survey every two years but it remains the Directorate's responsibility to ensure any on-going changes are recorded in a timely manner.

4.2 The registration of records will follow best practice in records management. It will allow for the users of the records to identify and track particular records and record collections. The registration system includes:

- Classification of the records into series that have meaningful titles and a consistent reference code.
- Setting a responsibility on individuals creating records to allocate them to an appropriate work area in the policy, case or secure file series
- Having sequences of reference numbers that can facilitate paper and electronic (where appropriate) records
- Checking that the correct records have been allocated to the sequence and that meaningful titles are used.
- Auditing lists of the references used so that the registration system makes sense and records can be found in appropriate search sequences.

- Operating an efficient file management system that is appropriate to the needs of the Directorate.

5.0 Information Governance Management Group

5.1 The Director of Human Resources and Corporate Services chairs the Information Governance Management Group (IGMG) which will monitor the application of this Policy along with compliance with the controls assurance requirements for Records Management and other Information Governance issues. The group consists of identified Information Governance Leads/Managers in each Directorate or sub-Directorate and will also take on the role of:

- Developing and maintaining a comprehensive inventory of all record systems used within the BSO
- Reviewing the listing of all Offsite Records for appropriateness
- Developing criteria for Storing Records Offsite / Security of Personal Data
- Developing procedures for Requisitioning / Retrieval / Authorisation Framework for retrieval of offsite records
- Developing a Policy on the Disposal of Offsite Records
- Recording any reported data breaches and near misses

5.2 Each Directorate will identify one person who will have a coordinating role to ensure that records and information systems in their business areas conform to this policy and to the requirements of legislation. This does not detract from the responsibilities of other managers to ensure they meet their obligation. Where appropriate this person will also take on some of the role of Personal Data Guardian who has a particular responsibility for safeguarding patients' interests regarding the use of patient identifiable information. The BSO's Personal Data Guardian is the Director of Human Resources and Corporate Services.

6.0 Disposal of Records

6.1 Records will be retained and disposed of in accordance with the guidance set out in the Good management Good Record Guidelines for Managing Records in Health and Personal Social Services organisations in Northern Ireland which can be found at www.dhsspsni.gov.uk/gmgr

7.0 Monitoring Compliance

7.1 The Business Services Organisation will follow this records management Policy within all relevant procedures and guidance used for operational activities. Interpretation of the Policy will be monitored and there will be regular planned inspections by the Internal Auditor to assess how the Policy is being put into practice. These inspections will seek to:

- Identify areas of good practice which can be used throughout the organisation
- Highlight where non-conformance to the procedures is occurring
- If appropriate, recommend a tightening of controls and make recommendations as to how compliance can be achieved

8.0 Equality Statement

8.1 This policy has been screened in accordance with the BSO's statutory duty and is not considered to require a full impact assessment.

Appendix A

A guide to good record keeping

For issue to all staff

Who's responsible?

All staff are responsible for any records, which they create or use.

Everyone working for or with the BSO who records, handles, stores or otherwise comes across patient information has a personal common law duty of confidence to patients/clients and to his/her employer. The duty of confidence continues even after the death of the patient or after an employee or contractor has left the NHS.

Personal information (e.g. about a patient) processed/kept for any purpose should not be kept for longer than is necessary for that purpose. Patient information may not be passed on to others without the patient's consent except as permitted under Schedule 2 and 3 of the Data Protection Act1998 or, where applicable, under the common law where there is an overriding public interest.

Why are records valuable?

Records are valuable because of the information they contain and that information is only usable if it is correctly and legibly recorded in the first place, is then kept up to date, and is easily accessible when needed. If it is not recorded it did not happen.

A Health Record may be called as evidence in legal proceedings or a professional misconduct hearing.

The Data Protection Act 1998 gives individuals the right to access their health record held manually or on computer.

Why good record keeping is important

You can work with maximum efficiency without having to waste time hunting for information.

There is an "Audit Trail" which enables any record entry to be traced to a named individual at a given Date/Time with the secure knowledge that all alterations can be similarly traced.

Those coming after you can see what has been done, or not done, and why.

Any decisions made can be justified or reconsidered at a later date.

Everyone who records patient's information should be aware that records are also kept because one day they may be needed:-

- By the patient applying to have access to their own health records under the Data Protection Act.
- By the patient's solicitor for a third party litigation claim.
- By the patient's solicitor for a clinical negligence claim against the Trust.
- By the patient's solicitor in support of a clinical negligence claim against another Trust.
- By you to write a report for a litigation claim.
- By you to write a report for a clinical negligence claim.
- By you to demonstrate that you have not been professionally negligent in anyway.
- By you to protect your job.
- By the BSO for managing complaints.
- By the BSO for managing audits
- By the BSO for managing issues of the Data Protection Act
- By the BSO for managing research

What is considered good practice?

- Make comprehensive notes of actions and outcomes.
- Detail all complex problems, or where more input has been required.
- Show duty of care has been honoured.
- Think about what you write, humour does not fare well in the legal arena.
- Take care when recording information regarding or given by a third party,
- Clearly state that the information has been given by a third party.
- Document clearly when discussion has taken place with a Senior Team Member.
- Record all information; it may be crucial if a complaint is made.
- Ensure the information you record is really relevant.
- Make sure you read what you have written – Does it make sense!!

Standards to be achieved

Service user and client records should:

- Be factual, consistent and accurate.
- Be written in black ink.
- Be written as soon as possible after an event has occurred
- Be written clearly, legibly and in such a manner they cannot be erased.
- Erasers, liquid paper, or any other obliterating agents should not be used to cancel errors. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment.

- Be accurately dated, timed and signed with the signature being printed alongside the first entry.
- The use of abbreviations should be kept to a minimum.
- Be written, wherever possible, with the involvement of the service user and in terms that the service user or carer will be able to understand.
- Be consecutive.
- Be bound and stored so that loss of documentation is minimised.
- Be relevant and useful
- Identify problems that have arisen and the action taken to rectify them.

Service user records should not include

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive statements.
- Personal opinions regarding the service user (restrict to professional judgments on all matters).
- The name(s) of third parties involved in a serious incident. The name should be included on the separate incident form for cross referencing.
- Correspondence generated from legal papers and complaints.

REMEMBER!!!

You are responsible for what you write!

- If it isn't recorded then there is no proof that something has been done.
- Clients have the right of access to their own Health Records under the Data Protection Act 1998 however; this is by formal application only.
- Records can be produced as evidence in legal proceedings or misconduct proceedings.
- You have a duty of confidence to ensure that any person identifiable information is only given to authorised staff and that information divulged to an unauthorised person can result in dismissal.
- If you are handling health records you are responsible for ensuring their safekeeping whilst they are in your care.

How to protect health records and the information they contain against loss, damage or unauthorised access?

If Health Records are being delivered to another location they should be enclosed in sealed envelopes or satchels and sealed for transfer. Any records that may be damaged in transit should be enclosed in suitable padding or containers.

- Packages should be marked “Private & Confidential”.
- For larger quantities, records should be boxed in suitable boxes or containers for their protection.
- Each box or envelope should be addressed clearly and marked confidential with the senders name and address on the reverse if the envelope. There are various options if records are to be mailed, such as recorded delivery, registered mail etc. When choosing options staff should consider the following carefully:-
- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
- Does the mail provider offer ‘track and trace’ options and is a signature required on delivery?

Handling & Storing Records

- No-one should eat, drink or smoke near the records.
- Clinical records being carried on-site e.g. from the archive storage to the department, should be enclosed in an envelope.
- Records should be handled carefully when being loaded, transported or unloaded.
- Records should never be thrown.
- Records should be packed carefully into vehicles to ensure that they will not be damaged by the movement of the vehicle.
- Vehicles must be fully covered so that records are protected from exposure to weather, excessive light and other risks such as theft.
- No other materials that could cause risks to records (such as chemicals or water) should be transported with records.
- Vehicles containing records should ensure that records are kept out of sight and the vehicle is locked when stationary.

Taking records off site

- Records should only ever be taken off site if absolutely essential
- Records should never be left unattended e.g. in the car. Care must be taken in order that members of the family or visitors to the client’s house cannot gain access to the records.
- If the health records cannot be returned to the BSO on the same day then the employee must ensure that they are kept securely and confidentially, not left in a car or lying around for any unauthorised persons to gain access.
- Records should be carried in a secured envelope, locked briefcase and not carried ‘loosely’, as this increases the risk of dropping the records land loss of the contents.
- The responsibility for maintaining health records in a secure place rests with the person who has use of the documents at any one time.

Confidentiality – common law duty

"All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty to support professional ethical standards of confidentiality.

Everyone working for or with the NHS who records, handles, stores or otherwise comes across information that is capable of identifying an individual patient, has a personal common law duty of confidence to patients and to his or her employer".

(The NHS Code of Confidentiality: Guidance from the Department of Health)

In all walks of life 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 the information. This duty of confidence is established in the NHS may lead to disadvantages to the patients or to that of the public in general.

> The Health Service collects and holds large volumes of confidential information about you, members of your family, friends and colleagues, although the vast majority of this information will be about strangers, most of whom you are unlikely to meet. The information we hold belongs to them and we only act as custodians. Their information should be afforded as much integrity as you would expect yourself. Handle their information with care. It is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that personal identifiable information is not made available to unauthorised persons. These principles apply equally to data about staff as well as patients.

Background to Caldicott

Following the publication of the "The Caldicott Committee: Report on the Review of Patient-Identifiable Information", published in December 1997 a senior health professional or existing member of the Board has to be identified as responsible and the Personal Data Guardian for reviewing and agreeing protocols governing the disclosure of personal information about the patients across organisational boundaries. This role is undertaken in BSO by the Director of Human Resources and Corporate Services.

There are a set of six general principles for the safe handling of patient identifiable information. These principles work hand-in-hand with the Data Protection Act 1998 and must be adhered to when collecting, transferring, or generally working with personal information. The six principles are as follows:

1. Justify the purpose.

Every proposed use or transfer of patient-identifiable information within or from another organisation should be clearly defined (and reviewed regularly).

2. Do not use patient-identifiable information unless it is absolutely necessary.

Patient-identifiable information should not be used unless there is no alternative.

3. Use the minimum necessary patient-identifiable information.

Where use of patient identifiers is considered to be essential, each individual item of information should be justified with the aim of reducing identification.

4. Access to patient-identifiable information should be on a strict need to know basis.

Only those individuals who need access to patient-identifiable information should have access to it.

5. Everyone should be aware of their responsibilities.

Action should be taken to ensure that all staff are aware of their responsibilities and obligations in respect of patient confidentiality.

6. Understand and comply with the law.

Every use of patient-identifiable information must be lawful.

What is patient-identifiable information?

“All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriately protected to safeguard confidentiality”

Items include:

Surname Forename; Initials; Address; Date of Birth; Other dates (date of death);

Postcode; Occupation; NHS Number; Ethnicity; National Insurance Number

Telephone Number; Local Identifier (e.g. hospital number)

Who is an unauthorised person?

An unauthorised person can be anyone who does not need to have access to the information. Your job role, for instance will determine what level of information you have access to either from a paper-based system or password protected computer system. Do not assume that your colleagues have the same privileges or that because they are more senior to yourself that they need to know the information. If you are in doubt as to whether you should share information with one of your colleagues, seek the advice of your manager.

It is not acceptable for you to access information about yourself, or on behalf of your relatives, friends and neighbours. There are procedures in place within the BSO for the processing of requests for access to personal information.