ORF-051, Issue 1.0, Date 14/04/14
Ref: SOP: 023/ORG

Procedure No: MP- 018

Management Procedure for:

Records Management

Originator(s) of Change:- R. Walters	**Issue No:- 7.0**
	Issued for Training/Awareness:-16/04/18
Approver(s):- M. Cheadle	**Effective Date:- 24/05/18**
Author(s):- C. Stirrup	**Date first issued:- 19/10/1993**
****** **If printed, this document becomes an uncontrolled copy** ******	

1.0 PURPOSE

To define the nature of records, the responsibilities of staff with regard to records management, to outline best practice in records management and to indicate the recommended retention times for primary records. To facilitate the creation of the necessary records to provide comprehensive, reliable and authentic evidence of the organisation's decisions and activities

2.0 SCOPE

This procedure covers the management of all records generated by the Welsh Blood Service including the operation of the system, product quality and process control.

3.0 REFERENCES

3.1 Procedure for data protection impact assessments **SOP:076/ORG**
3.2 **SOP:023/ORG** Guidelines for Controlled Documentation
3.3 Good Documentation Practice **SOP: 001/ORG**
3.4 **POL(P)-045** Data Integrity Policy and Standards
3.5 **SP-001** IT Security Policy
3.6 Procedure for the Release of Confidential Personal Information and/or removal from the database under the terms of data protection legislation **SOP: 030/ORG**
3.7 Procedure for the Release of Information Under the Freedom of Information Act and the Environmental Information Regulations - **SOP 050/ADM**
3.8 Procedure for The Release of Confidential Information to Third Parties – **SOP: 044/ADM**
3.9 Archiving Procedure – **SOP: 016/FAC**
3.10 Retrieval of Information – **SOP: 015/FAC**
3.11 Reporting of Incidents, Accidents, Near Misses or Hazards – **SOP: 025/ORG**
3.12 **IG 13** Confidentiality Breach Reporting Policy

4.0 DEFINITIONS

4.1 Senior Management: a member of the Senior Management Team who has functional responsibility for an area of activity at the WBS.

4.2 Manager: is a generic job title that can refer to any person having managerial accountability for a department or group of employees.

4.3 Any job titleholder mentioned in this procedure may appoint a designated nominee to represent the job titleholder as and when required.

ORF-051, Issue 1.0, Date 14/04/14
Ref: SOP: 023/ORG

4.4 Record: 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.

4.5 Physical records: are those records that can be touched and which take up physical space. e.g. paper records, photographs, microfiche/microfilm

4.6 Electronic records: also often referred to as digital records, are those records that are generated with and used by information technology devices (such as computers) that requires the use of the device to render it intelligible by a person e.g. database records, e-mails, video, voice recordings, text messages.

4.7 Record Media: The physical medium on which information is stored in recoverable form, such as plain paper, magnetic tapes, magnetic disks, solid state media (e.g. memory stick) or CD-ROM/R/RW

4.8 Filing System: A plan for organising records so that they can be found when needed.

4.9 Data Custodian: A Senior Manager who is responsible for authorising access to an identified database and monitoring compliance with this Management Procedure within their area of responsibility. See Attachment 6.3.

4.10 Caldicott Guardian: A Medical Consultant responsible for safeguarding and governing the uses made of confidential patient and donor information. See Attachment 6.3.

4.11 Local Records Manager (LRM): A member of staff who has the role of ensuring that best practice in records management is followed in their area of responsibility. They may be required to carry out staff training to new members of staff joining their area and refresher training as appropriate.

Note: The specific roles listed in 4.9 to 4.10 shall not normally be delegated. However, it is legally established by law that **all NHS employees** including consultants, contractors, casual and agency staff are responsible for any records that they create or use in the course of their employment.

4.12 WTAIL: Welsh Transplantation and Immunology Laboratory

4.13 WBMDR: Welsh Bone Marrow Donor Registry

5.0 PROCEDURE

5.1 Creation of records

5.1.1. A data protection impact assessment (DPIA) should be considered when a new system of record keeping is set-up and if it contains personal data (Ref. 3.1). A DPIA should also be considered when personal data is handled in new ways.

5.1.2. All GMP record templates should be prepared and controlled in accordance with the SOP (Ref. 3.2).

5.1.3. All records shall include the identity of person or equipment (pc, server etc.) Creating the record, and include the date of creation (and time if necessary).

5.1.4. All paper must be completed legibly and accurately in accordance with Good Documentation Practice and Data Integrity Principles (see references 3.3, 3.4 for details).

5.1.5. All Data Custodians shall ensure that mechanisms are in place to assure the accuracy of data entered into databases

5.1.6. Rough notes and post-it notes must not be used for recording Good Manufacturing/Distribution Practice data.

5.2 E-mails Records

E-mail information is often of little value to the organisation or has value for only for a short time. However some e-mails can be valuable records where they are used as the only means to communicate approvals, decisions or directions and advise. Consideration should be given to storing such e-mails in filing systems where they can be easily be accessed as organisational records e.g. in project folders; not in personal accounts.

5.3 Management of Social Media records

Social media is a form of communication that occurs on various platforms, such as websites and applications. Is important that the WBS keeps an accurate and authentic 'original' copy of business information posted on social media and captures it in the records management system. Different information obtained from social media has different value and purpose. More valuable social media information, such as feedback about policy,

announcements or complaints, needs to be communicated and retained appropriately.

5.4 Retention of records

5.4.1 Data Custodians shall agree with the LRM which records shall be retained and in what format. Categories of records that must be retained for a designated period include:-

- Policies and Procedures
- Strategic plans (e.g. corporate plans, business plans and related planning documents)
- Product and Process Characteristic records
- Donor/Medical records
- Patient records
- Quality System records
- IT records
- Financial records
- Personnel records
- Health & Safety records
- Business records
- Research and development papers
- Minutes, circulated papers etc. of meetings
- Reports

5.4.2 All Records must be held within filing systems where they can be easily accessed for the duration of their retention period. WBS records should not be held on personal drives.

5.4.3 When determining the minimum retention period of any of the above, reference must be made to attachment 6.1. For all record not described in the attachment, consult the IBMS The retention and storage of pathological records and specimens

https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html

or the Records Management Code of Practice for Health and Social Care 2016

https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

5.4.4 Any records placed into archive storage will not be accessible for alterations.

5.4.5 Websites information should be retained for 6 years after creation

5.5 Security & Access

5.5.1 Everyone working for or with the NHS who records, handles, stores, or otherwise comes across information has a personal common law duty of confidentiality. The Data Custodian for a database shall ensure that the database is secure, and accessed only by appropriately authorised staff.

5.5.2 All records must be held securely. They must be protected against unauthorised or unlawful access or processing and against accidental loss, destruction or damage (3.5).

5.5.3 All staff members have a duty to ensure paper records are held securely. Wherever possible staff shall adopt a "clear desk" procedure at the end of each working day and secure records and other paperwork relating to donors, patients and staff in a locked cabinet or room.

5.5.4 Donor, patients and staff have the right to access data pertaining to them that is held by the WBS. This is by a "Subject Access Request". Information has to be disclosed under other legislation. It is important that the correct procedure is followed (3.6 to 3.8) so that confidential information is not disclosed to an unauthorized party.

5.6 Storage Environment

5.6.1 All records should be stored in an environment that provides protection from direct sunlight and ultra-violet light, and is free from chemical or particulate atmospheric pollutants. The environment should not be subject to rapid fluctuations in either temperature or humidity. Records should be held in areas where there is minimal risk from ingress of water e.g. from leaking pipes, leaking roofs or floods. Areas where records are stored long term, must have an automated fire and/or smoke detection system in the area.

5.6.2 Storage areas for magnetic media should not contain large electrical devices or other equipment that may produce magnetic fields.

Media for electronic records must be store according to the manufacturer's instructions, or the guidance in the following table:

Long Term Storage (>1 year) For Electronic Media (National Archive Guide)		
Media	**Temperature**	**Relative Humidity**
Flexible Magnetic Disks	18-22ºC	35-45%
Digital Audio Tape (DAT)	5-32ºC	20-60%
Digital Linear Tape (DLT)	18-26ºC	40-60%
Ultrium Linear Tape Open (LTO)	16-32ºC	20-80%
Other Magnetic Tape Cartridges	18-22ºC	35-45%
CD-ROM/R/RW	18-22ºC	35-45%
DVD-ROM/R/+R/RAM/RW/+RW	18-22ºC	35-45%
Solid State Media	18-22ºC	35-45%

5.6.3 Where paper records contain personal information they should not be removed from the site by staff, unless authorised by the data custodian. Where possible, all such records should be held digitally on encrypted devices. Records containing personal identifiable information must not be left unattended in personal vehicles.

5.6.4 Staff must only access the records that they are authorised to do according to their job role. Unauthorised access of electronic records is illegal.

5.7 Local Records Manager Responsibilities

5.7.1. Local Records Managers are responsible for ensuring all records are recorded in the information asset register E:\All Users\Information Assets & data Protection Impact Assessments\Information Asset Database. They may be added by completing form ORF-084 and submitting it to Quality Assurance Systems.

5.7.2. Department Records Managers shall include regular reviews of records, and other paperwork held in storage, with a view to reducing records and paperwork that are no longer required.

5.8 Digitisation

It is expected that at least two (full) year's records should be maintained at all times, for trending and inspection purposes, in their original format. Following this period paper records may be converted to digital format (archived) for the remainder of their retention period (3.10, 3.11)

5.9 Copying

The copying of records shall be kept to a minimum, compatible with the needs of the Service. Where appropriate, a record of who requested a copy of a confidential record and final disposal of the copy record shall be maintained by the record holder.

5.10 Rationalisation and sharing of records

Wherever possible, and subject to the conditions of Data Protection Legislation, records shall be shared by the use of electronic means e.g. shared databases. Duplication of records should be avoided in order to reduce the possibility of transcription errors, time delays in updating the same record and storage and retrieval costs.

5.11 Disposal

5.11.1 Records at the end of their minimum retention period, may only be disposed of with the authorisation of the appropriate Data Custodian (See Attachment 6.3). Disposal may include transfer of records to a final permanent depository, but more usually destruction. Destruction of records must be authorised by the Data Custodian as it is an irreversible event. Data protection legislation require that records with personal information are held for no longer than necessary, however at the same time, unauthorised destruction of records may breach the Freedom of Information Act or other legislation requiring records to be held for minimum periods.

5.11.2 Management of the removal of computer media and mobile telephone memory prior to disposal of equipment

It is essential that computer media such as CDs, floppy disks, tapes, label printers and single pass film faxes are removed before the equipment is disposed of. Staff must return mobile phones supplied by the Welsh Blood Service to the Procurement Department, who will liaise with Network Support, IT Section of the General Services

Department, to ensure the phone memory is erased. Advice on the disposal of computer media can be obtained from Network Support

5.11.3 An electronic records management system should retain a metadata stub which will show what has been destroyed.

5.12 Training in Records Management

Each departmental LRM shall be responsible for ensuring that all current and new staff, within their area of responsibility, must receive training on the best practice in records management and that staff are familiar with the Department Records Management SOP.

5.13 Data Protection Legislation

When dealing with records management, the requirements of the legislation shall be followed.

5.13.1 All data collected about an individual must be processed lawfully and in a transparent manner.

5.13.2 All personal data collected must be for specified, legitimate purpose, and not further processed in a manner incompatible with the purpose.

5.13.3 Data collected must be adequate relevant and limited to what is necessary.

5.13.4 Data must be kept accurate and up-to-date.

5.13.5 Processing in a form that identifies data subject for no longer than necessary.

5.13.6 Held with appropriate organisational and security measure to prevent unauthorised or unlawful processing, accidental loss, destruction, or damage.

5.13.7 Medical confidentiality must be respected.

5.14 Breaches

All losses of records and other breaches of personal information must be reported (ref 3.11), and the Data Protection Officer (DPO) must be informed. The Trust policy should be consulted in determining whether a breach is

ORF-051, Issue 1.0, Date 14/04/14
Ref: SOP: 023/ORG

reportable to the Information Commissioners Office (3.12). Reportable breaches of personal data must be reported to the ICO within 72 hours of recognition, by the DPO.

6.0 DOCUMENTATION

6.1 Table of WBS Primary records and recommended retention periods
6.2 **Deleted**
6.3 Data Custodians for the WBS

Primary records and recommended retention periods:
Disposal of these records shall only be authorised by the appropriate Data Custodian.

Category of Record	Record	Period
Product and Process Characteristic Records	Laboratory Results	40 years
	Batch Release	30 years
	Product specifications	30 years
	Production History	15 years
	Calibration Records	15 years
	Apheresis Daily worksheets	30 years
Donor/Medical Information	Donor Records	30 years
	Health questionnaires	30 years
	Donation Information	30 years
	Session Reports	15 years
	Donor permanent deferrals	30 years
Patient Information	Patient Records	30 years
Other Quality System Information	Official Procedures	40 years
	Product Recalls	30 years
	Product complaints	30 years
	Other complaints	10 years[a]
	Audit paperwork (internal & external)	10 years electronic 5 years paper records
	Serious Adverse Blood Reactions and Events (SABRE)	15 years
	Document control papers	3 years
	Incident Records	40 years
IT Information	Programmer Documentation	30 years
	Software documentation	30 years
	User documentation	30 years
	Validation Logs	30 years
	Database Amendment Forms	30 years
Financial Records	Delivery notes	1.5 years
	Invoice requisitions	7 years
Personnel records–major Personnel records– minor	E.g. Personal files, letters of appointment, contract references & related correspondence. E.g. attendance books, annual leave records, duty rosters, clock cards, timesheets.	6 years[b] 2 years
Health and Safety	Risk assessments	40 years
	Health & Safety Records	40 years
Business	Management meeting minutes	30 years
	Management review minutes	5 years
	Contract Review minutes	5 years

[a] If the complaint has gone to litigation refer to legal advice on retention.
[b] 6 years after subject has left the service or until subject's 70th birthday whichever is the later. Only the summary needs to be kept to age 70; remainder of file can be destroyed.

DATA CUSTODIANS FOR THE WBS

Role	Job title
Caldicott Guardian	Medical Director
Data Custodian of confidential medical records	Medical Director
Data Custodian Directors Office	Director
Data Custodian Donor Records	Head of Collection Services
To provide cover for Donor Records Data Custodian. May authorise access in the absence of the Head of Collection Services	Donor Recruitment & Retention Manager
Data Custodian Laboratory Records	Head of Laboratory Services
Data Custodian WTAIL/WBMDR Records	Head of WTAIL
Data Custodian IT Records	General Services Manager/Deputy Director
Data Custodian Business, Personnel, Finance, Estates, Security	Director
Data Custodian Quality Systems	Head of Quality Assurance and Regulatory Compliance