

**RECORD MANAGEMENT AND LIFE CYCLE POLICY AND STRATEGY**

**Document Owner:** Dr Caroline Yates

**Developed in Consultation With:** Information Governance team

**Document type:** Policy

**Version:** 2

**Requirement:** Mandatory

**Date of ratification:** 26.03.15

**Ratified By:** The partners

**Date to be reviewed:** 3 years from ratification or sooner if any changes in legislation

HISTORY

Revisions: (Enter details of revisions below)		
Date:	Author:	Description:
<b>17.01.13</b>	<b>Becky Biddick</b>	<b>Addition to Appendix 1 – Clinical Records to be retained for 7 years from date of discharge.</b>
<b>August 2014</b>	<b>Ceri Evans</b>	<b>Section 2 of the summary page and Section 21 of the main policy. Update of policy to reflect email and text message requirements.</b>
<b>September 2014</b>	<b>Becky Biddick</b>	<b>Update of version 1 - Review of whole policy to reflect staff changes, and new information from KCCG regarding retention periods</b>

## **1. Statement of Intent**

The purpose of this policy is:

- To ensure all staff are aware of the principles and practice of record-keeping.
- To ensure all staff are aware of the principles and practice of the destruction of all records
- To document Outlook South West LLPs principles for recording, producing, updating and storing handwritten and electronic clinical records and to provide standards for staff to follow.

Outlook South West LLP's records management strategy aims to ensure:

- a planned approach to records management, covering records from creation to disposal
- greater coordination of records and storage systems through improvements in the quality and flow of information
- compliance with statutory requirements
- awareness of the importance of records management and the need for responsibility and accountability at all levels
- appropriate archiving of the company's records.

## **2. Who this document is relevant to:**

This document applies to all staff of Outlook South West LLP. This policy also applies to all organisations employed by Outlook South West LLP and all organisations contracted to Outlook South West LLP. The policy relates to all operational and administrative records held in any format by Outlook South West LLP. These include:

- all administrative records (e.g. personnel, estates, health and safety, financial and accounting records, notes associated with complaints, incidents, policies); and
- all patient health records (for all specialties and including private patients, and records held by Outlook South West LLP's subsidiaries.)

The policy covers records held in all formats, for example:

- paper records, reports, diaries and registers etc;
- electronic records;
- audio and video tapes;

- Text message communication with patients (both outgoing from Outlook South West LLP and incoming);
- Email communications with patients (both outgoing from Outlook South West LLP and incoming)

### 3. Definitions

**Records Management** is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of Outlook South West LLP and preserving an appropriate historical record. The key components of records management are:

- record creation
- record keeping
- record maintenance (including tracking of record movements)
- access and disclosure
- closure and transfer
- appraisal
- archiving
- disposal

**Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by Outlook South West LLP in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

**Information** is a corporate asset. Outlook South West LLP's records are important sources of administrative, legal, evidential and historical information. The records are vital to support the business's current and future operations (including meeting the requirements of Freedom of Information and Data Protection legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

#### Types of record

**Clinical Records** Anything which contains clinical information about a particular patient (in any media) which has been created or gathered as a result of any aspect of work undertaken for Outlook South West LLP. This includes electronic records on IAPTUS. In addition to brief session by session notes kept by therapists (Therapy Notes), these include reports, letters and formal summaries of assessments, treatments and outcomes.

**Therapy notes** Also known by some as ‘Process notes’. Therapy notes are a subset of the clinical record. These typically are in paper form, are kept by High Intensity therapists and Clinical Psychologists, and include formulation diagrams and other such notes made during a session or shortly after. Therapy notes should be signed and dated. They are kept for the duration of the therapy, and then destroyed. These notes are supplementary to the electronic record on IAPTus and/or the GP system which provide the formal Clinical Record. On discharge these writings may be used to provide a summary of assessment /treatment (which, in general, will go to the patient’s GP), and which covers assessment, formulation, treatment and therapeutic outcomes. This may augment the information already provided to the GP. This summary letter then becomes part of the clinical record. Such notes, while they are kept, can be subpoenaed by the courts.

**Content notes** These are anonymised records which are used by the practitioner as part of their learning and professional development and will draw on the clinical contacts they have with patients. Staff should ensure that their Content Notes do not contain patient identifiable information. They may contain personal information pertaining to the therapist, for example, about the therapists own reactions, and as such their disclosure may breach the confidentiality of the therapist. It must be clear that these are not patient-specific notes, and that maintaining dual records – one version for the patient and another for the use of the professional - is illegal (Pattenden, 2003:650). These notes do not form part of the clinical record..

A **Lost** record is defined as any record that cannot be located within 5 working days of the first attempt to access the record, or any record that has been stolen from a known place. This should be reported as an incident using the standard Outlook South West LLP incident reporting methods.

A record is defined as **unavailable** if it is in use elsewhere and/or cannot be retrieved in time for an appointment or within 24-hours.

#### 4. **Related Policies**

Confidentiality Code of Conduct	Request for Information policy
Untoward Incident policy	IT security policy
Information Risk Management policy	

#### 5. **Related legislation, national and local guidance**

<a href="#">Data Protection Act 1998</a>	<a href="#">The Freedom of Information Act 2000</a>
<a href="#">The NHS Confidentiality Code of Practice.</a>	<a href="#">The Common Law Duty of Confidentiality</a>
<a href="#">The Public Records Act 1958</a>	<a href="#">The Records Management: NHS Code of Practice.</a> Published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on

	current legal requirements and professional best practice.
Professional Organisations guidelines	Bond T. and Jenkins P. 2007 Access to Records of Counselling and Psychotherapy <a href="http://www.bacp.co.uk/members/info_sheets/pdf/G1_web.pdf">http://www.bacp.co.uk/members/info_sheets/pdf/G1_web.pdf</a>
British Association of Behavioural and Cognitive Psychotherapy (2009). Ethical Framework for Good Practice in Counselling & Psychotherapy: BABCP. <a href="http://www.babcp.com/">http://www.babcp.com/</a>	Health Professions Council (2009). Standards of conduct, performance and ethics.: HPC. <a href="http://www.hpc-uk.org/">http://www.hpc-uk.org/</a>
Newton, S. (2008). Record Keeping: guidance on good practice.: British Psychological Society: Division of Clinical Psychology. <a href="http://tinyurl.com/ykd9zco">http://tinyurl.com/ykd9zco</a>	Pattenden R. 2003 The Law of Professional-Patient Confidentiality: Regulating the Disclosure of Confidential Personal Information. Oxford University Press.
Scott, B. (2004). Health Records. Retrieved April 2009, from <a href="http://www.isb.nhs.uk">www.isb.nhs.uk</a>	NHS Trust Records Management Policy

6. **Equality Impact and Privacy Impact Screen / Assessment**  
Completed on 18.09.2014

7. **Communication and Training**

Outlook South West LLP recognises the importance in ensuring that all members of staff are fully aware of their responsibilities in relation to record-keeping and record management. Outlook South West LLP staff members will be made aware of their responsibilities as part of their Induction Training, Information Governance online training, at Service Update days and through generic and specific training programmes and guidance.

The Connecting For Health IG Training Tool is an online training tool focused on all aspects of learning about Information Governance (IG). The aim of the tool is to develop and improve staff knowledge and skills in the IG work area. All staff will complete appropriate modules of this training as suggested by their role prior to creating any clinical records and annually thereafter.

Effective records management involves staff at all levels. Training and guidance enables staff to understand and implement policies, and facilitates the efficient implementation of good record keeping practices.

The Record Management and Life Cycle Policy and Strategy will be communicated in the following ways:

Communication Method	Applicable to this document/policy	Frequency
<b>CONNECT E BULLETIN</b> - Document attached - Highlighting core responsibilities and / or how any	Essential	Minimum yearly

changes affect them directly.		
<b>COPIES</b> - Requests for hard copies (or electronic copies) of any policy can be made via the head office.	Essential	n/a
<b>UPDATE DAYS</b> - Consolidate this information by reminders/presentations at update day.	Desirable	n/a
<b>LINE/LOCALITY MANAGEMENT MEETINGS</b> - Consolidate this information by reminders/presentations at line management / locality meetings. - Operational Manager Responsibilities will be reinforced and checked for understanding in their line management meetings.	Essential	Minimum yearly
<b>INTRANET</b> - Updated / new policies and documents uploaded to intranet.	Essential	Minimum yearly
<b>STAFF INDUCTION</b> - Mandatory policies will be provided to all staff at induction	Essential	As required
<b>OSW WEBSITE</b> - Policies will be disseminated (when appropriate) to clients, health professionals and the general public via the Outlook South West website policies page <a href="http://www.outlooksw.co.uk">www.outlooksw.co.uk</a> .	Essential	As required
<b>DISSEMINATION CONFIRMATION</b> - The Clinical Governance Team will carry out checks to ensure the information is indeed being disseminated and reaching the employees.	Essential	Mandatory Policy; 1 month from dissemination
<b>STAFF FORUM / DOCUMENT OWNER</b> - Any comments, queries or suggestions for new policies or for amendments to existing policies can be made via the document owner or the Staff Forum.	Essential	As required

## 8. Evidence

All employees will sign the Policy and Guidance Acceptance document to confirm they have read and understood (as a minimum) all mandatory policies and guidelines.

## 9. Reporting, Monitoring, Reviewing and Audits

Monitoring and review of this policy will be co-ordinated by the Clinical Governance Team.

Progressive improvement can only be achieved through the constant development of policies, approaches to implementation and techniques of risk control.

The Clinical Governance Team shall audit the overall performance of the Record Management and Life Cycle Policy and Strategy. Reported incidents involving the policy and



- 6 Record Management Lifecycle
- 7 Records Management Systems Audit
- 8 Breaches in Security and Lost Records
- 9 Boundaries
- 10 Risk
- 11 Legibility
- 12 Communication
- 13 Information provision to patients
- 14 Clinical Governance
- 15 Accountability
- 16 Security
- 17 Openness
- 18 Practitioner-specific guidance
- 19 Recording group or educational work
- 20 Video/Audio Recording
- 21 Text Messages and Email Communication
- 22 Supervision and education
- 23 Ownership, Archiving and Destruction of Records
- 24 Procedure for dealing with missing records
- 25 Monitoring
- 26 Record Quality

Appendix 1 - Retention period for records (clinical and non clinical)

Appendix 2 - Consent for Audio/Video recording

Appendix 3 - The key elements of the record management strategy

Appendix 4 – OSW archiving plan 2014

Appendix 5 – Example of the OSW archiving log

## **1. Introduction**

The partners of Outlook South West LLP have adopted this Records Management and Life Cycle Policy and Strategy, and reiterates the organisations commitment to on-going improvement of its records management functions. Information (records) management, through proper control of the content, storage and volume of records, brings a number of organisational benefits. These include:

- better use of physical and server space;



- better use of staff time;
- improved control of valuable information resources;
- reduced vulnerability to legal challenge;
- compliance with legislation and standards; and
- reduced costs

This document also sets out a framework for records management initiatives, defining a strategy for improving the quality, availability and effective use of records within Outlook South West LLP and providing a strategic framework for all records management activities. This will enable overall coordination of all records management activities and ensure they support the company's business strategies. Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal.

As well as providing a policy and strategy for the management of records, this document provides clear guidelines for the keeping of and destruction of any records within Outlook South West LLP. Health record and communication practice standards for all healthcare professionals are essential for safe and effective practice. Existing standards relating to health record and communication practice are those given by the individual healthcare professional regulatory bodies and provide the appropriate reference point for practitioners. In addition record-keeping is governed by a legal framework including and in particular the Data Protection Act 1998. The source of information section contains a list of references to records-related advice and guidance.

## **2. Accountability and Responsibility**

It is important that all Outlook South West LLP employees appreciate the need for responsibility and accountability in the creation, amendment, management, storage of, access to and disposal of all company records. A clear chain of managerial responsibility and accountability for all records must be established by the company. This is essential for an effectively coordinated records management strategy.

All individuals are responsible for their own record keeping and for attending appropriate training as required and offered by Outlook South West LLP. Every time a member of staff accesses a record they are responsible for ensuring that all relevant documents are filed and secured with accordance with the Record Management and Life Cycle Policy and Strategy.

All members of staff who hold a responsibility for record keeping within the company will maintain an up to date awareness of legal and ethical issues concerning the subject.

### 3. The Records Management System and Strategy

Records held by Outlook South West LLP represent its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of Outlook South West LLP and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help us to deliver services in consistent and equitable ways.

*Outlook South West LLP's Record Management Strategy is to achieve systematic, orderly and consistent creation, retention, appraisal and disposal procedures for records throughout their life cycle. Record-keeping systems should be easy to understand, clear, and efficient in terms of minimising staff time and optimising the use of space for storage.*

The aims of our Records Management System are to ensure that:

1. **records are available when needed** - from which Outlook South West LLP is able to form a reconstruction of activities or events that have taken place;
2. **records can be accessed** - *To provide clear and efficient access for employees and others who have a legitimate right of access to Outlook South West LLP records, and ensure compliance with Access to Health Records, Data Protection and Freedom of Information legislation.*

Access is a key part of any records management strategy. Fast, efficient access to records unlocks the information and knowledge they contain. Records and the information within them must be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;

3. **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
4. **records 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;
5. **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
6. **records are secure** - *To provide systems which maintain appropriate confidentiality, security and integrity for records in their storage and use.*

Records must be kept securely to protect the confidentiality and authenticity of their contents, and to provide further evidence of their validity in the event of a legal challenge. Records must be secure from unauthorised or inadvertent alteration or erasure, access and disclosure is to be properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;

7. **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
8. **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.
9. **records are audited** - *to audit and measure the implementation of the records management strategy against agreed standards.*  
The performance of the records management programme will be audited.

#### **4 Record management roles and responsibilities**

##### **All Staff**

All Outlook South West LLP members of staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in Outlook South West LLP and manage those records in line with this policy and with any guidance subsequently produced. All staff must have an understanding of the key requirements of laws and guidelines concerning records, in particular those relating to confidentiality, data protection and access to information (including under the Freedom of Information Act 2000). All staff and those carrying out functions on behalf of Outlook South West LLP have a duty of confidence to patients and a duty to support professional ethical standards of confidentiality. The duty of confidence continues even after the death of the patient or after an employee or contractor has left Outlook South West LLP. Unauthorised disclosure of information may lead to a complaint against Outlook South West LLP or disciplinary action against a member of staff for a breach of confidentiality.

##### **The Partners**

The Partners have overall responsibility for records management in Outlook South West LLP. As the accountable persons, the partners are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

Outlook South West LLP has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

##### **Caldicott Guardian**

Outlook South West LLP's Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

## **Clinical Governance Team**

Outlook South West LLP's Clinical Governance Team are responsible for ensuring that this policy is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated and monitored.

## **Senior Information Risk Office (SIRO)**

The SIRO is responsible for ensuring the overall development and maintenance of health records management practices throughout Outlook South West LLP, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

## **The Information Asset Owner (IAO)**

The responsibility for local records management is devolved to the relevant IAO. Heads of Departments, other units and business functions within Outlook South West LLP have overall responsibility for the management of records generated by their activities, ie for ensuring that records controlled within their unit are managed in a way which meets the aims of Outlook South West LLP's records management policies.

## **Contractors and support organisations**

Service Level Agreements and contracts must include responsibilities for Information Governance and Records Management as appropriate.

## **Legal and Professional Obligations**

All NHS records are Public Records under the Public Records Acts. Outlook South West LLP will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice.

and any new legislation affecting records management as it arises.

## **5 Registration of Record Collections**

Outlook South West LLP will establish and maintain mechanisms through which departments can register the records they are maintaining. The inventory of record collections will facilitate:

- the classification of records into series
- the recording of the responsibility of individuals creating records

The register will be reviewed annually.

## **6 Record Management Lifecycle**

The 5 phases of the Record Management Lifecycle:

1. Creation
2. Retention
3. Maintenance
4. Use
5. Disposal

Below are details of each of these phases and Outlook South West LLP employees' obligations under this policy.

### **Creation:**

When creating information in the first instance, the following should be adhered to, the information must be:

- Available when needed - to enable a reconstruction of activities or events that have taken place
- Accessible to all members of staff that require access in order to enable them to carry out their day to day work - the information must be located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist
- Respectful - All records about a patient will be written in a respectful manner. Employees should be mindful that patients have a legal right to read their records.
- Interpretable, clear and concise - the context of the information must be clear and be able to be interpreted appropriately, i.e. who created or added to the record and when, during which business process and how the record is related to other records
- Trusted, accurate and relevant - the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant
- Secure - the information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required/retained
- Scanning - for reasons of business efficiency, or in order to address problems with storage, consideration should be given to the option of scanning into

electronic format, records which currently exist in paper format. Where this is proposed, the factors to be taken into account include:

- a) the costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept
- b) the need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created
- c) the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

In order to fully realise the benefits of reduced storage requirements and business efficiency, the information owners should consider disposing of paper records that have been copied into electronic format and stored in accordance with appropriate standards.

Employees should consider the following when creating information:

- what they are recording and how it should be recorded
- why they are recording it
- how to validate information (with the patient or carers or against other records) to ensure they are recording the correct data
- how to identify and correct errors and how to report errors if they find them
- the use of information; staff should understand what the records are used for and
- therefore why timeliness, accuracy and completeness of recording is so important
- how to update information and how to add in information from other sources

The **retention** period varies dependant on the type of information being stored. Please see Appendix 1 for details.

All information needs to be **maintainable** through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in the format.

The use of standardised filenames and version control methods should be applied consistently throughout the life of the information.

#### **Use:**

All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the SIRO.

- Disclosure - only the specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. The key statutory requirements can be found in Annex C of the Records Management: NHS Code of Practice (Part 1) available via:

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_4131747](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747)

Outlook South West LLP's Caldicott Guardian or senior clinician acting on behalf of the Caldicott Guardian will be involved in any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.

- Transfer – The mechanisms for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The SIRO can advise on appropriate safeguards. Guidance can also be found within the Information Governance Toolkit on the CFH website:

<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security>

- Closure – Information held in records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records, or folder of electronic records, has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the information is created. The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files

### **Disposal:**

It is particularly important under Freedom of Information legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by Outlook South West LLP and which are enforced by properly trained and authorised staff.

- Disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of information with archival value. Information lifecycle management is the responsibility of all staff and therefore managers are

responsible for ensuring weeding exercises to review information held within departments are undertaken on a regular basis.

- Destroyed appropriately – records can contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Any records that have been identified for destruction must be destroyed as soon as possible after they are eligible.

Outlook South West LLP has adopted the retention periods set out in the Records Management: NHS Code of Practice (see Appendix 1). .

## **7 Records Management Systems Audit**

Outlook South West LLP will regularly audit its records management practices for compliance with this framework.

The audit will:

- Identify areas of operation that are covered by Outlook South West LLP's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to Outlook South West LLP partners and Information Governance team.

## **8 Breaches in Security and Lost Records**

Any incident or near miss relating to a breach in the security regarding use, storage, transportation or handling of records must be reported using the Outlook South West LLP's Untoward Incident report form. Additionally the Information Governance Team should be made aware of breaches in security.



A serious breach of security e.g. major theft or fire must be managed in accordance with the Untoward Incident Policy. A lost record is defined as any record that cannot be located within 5 working days of first attempt to access the record or any record that has been stolen from a known place, for example, the boot of a car. Any suspected thefts must be reported to the Police.

Outlook South West LLP's Caldicott Guardian must be informed immediately of any loss or misplacement of any document that is used to record patient information, including diaries, or Outlook South West LLP business. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of all actions including:

- When and where the record was last seen, with date known
- If stolen, from where and Police Incident Number
- Actions taken to locate file

## **9 Boundaries**

The record's primary purpose concerns the patient difficulties, the therapeutic approach and outcomes. Sometimes difficulties the patient has, involve other people. Under these circumstances care should be taken to only record what is absolutely necessary about third parties, and even then being mindful about the need for anonymity for third parties.

References to third parties (the patient's partner, relatives and so on) should only be recorded under the following circumstances:

1. Information about third parties is included in administrative documentation e.g. IAPTus for example, where there is necessary contact information with the permission of the parties involved.
2. In notes and genograms or similar factual information reference to third parties should be by relationship, initial or other method which does not identify the individual by name.
3. Information obtained from third parties about the patient where significant levels of risk are involved.

## **10 Risk**

Guidance on risk issues can be found in the Risk Management Policy. Documentation of risk is a key role of the clinical record.

## **11 Legibility**

All handwritten paper records must be legible, signed and abbreviations defined.

## **12 Communication**

It is good practice to provide a written update to the GP on each occasion the patient is seen. GP practices currently have different requirements/agreements on what is either desirable or permitted. Details of Outlook South West LLP minimum requirements are in the standardisation documentation. Any variation from the Outlook South West LLP standard requirements should be agreed with the relevant Operational Manager. Arrangements for communication with other agencies may be required on a patient by patient basis.

### **13 Information provision to patients**

Patients must be informed at the outset of their treatment about records kept about their care via the 'Use of Patient Information' document (available on the intranet) and provide their explicit consent. This will usually happen at the beginning of the first assessment appointment. The document is also published on the Outlook South West LLP website.

### **14 Clinical Governance**

Good record keeping is one of the ways we can assure that the service is delivering good care. This will be partly monitored through regular audits by supervisors and case managers.

### **15 Accountability**

Standards of record keeping set by professional bodies, good practice guidance from public agencies and legal frameworks provide an accountability framework for clinical staff. These are used to inform this policy.

Outlook South West LLP considers it an ethical imperative to keep clinical records. Where the therapists considers there to be good and sufficient reason not to keep records, this must be brought to the attention of their supervisor and operational manager.

### **16 Security**

The security of all records is a high priority for Outlook South West LLP since we deal with highly sensitive personal information. Information concerning security can be found in the various Confidentiality and Security policies and Codes of Conduct.

### **17 Openness**

Outlook South West LLP's general principle supports an approach to the therapeutic relationship and process that is collaborative between the patient and the therapist. Therefore the records will be as accessible by the patient as possible.

However there may be occasions where a request for access to records may be denied if granting access is considered likely to cause serious harm to the physical or mental health or condition of the patient and that opinion has been endorsed by an appropriate health professional, such as a doctor involved in the treatment of the patient concerned. This

exception is restricted to records containing information about the data subject's physical or mental health.

All requests for access to view a record or for a copy of a record should be put in writing and sent to the head office. For further information, please refer to the Request for Information Policy.

## **18 Practitioner-specific guidance**

Practitioners will differ in the way they keep records, primarily as a consequence of their job role. Guidance on minimum requirements and appropriate clinical record keeping will be covered in Induction and via the in house Record Keeping Training.

## **19 Recording group or educational work**

Models of group work provided by Outlook South West LLP may vary and are likely to at least cover a range of approaches including educational at one end of the dimension to those which depend on group processes at the other. For each group activity written information describing the approach should be made available to the participants explaining how the data will be recorded and that they provide consent by the designated method for that course. If consent is not provided, then data will be stored separately so it is not processed for secondary purposes. Consent / declining should be documented on IAPTus.

Since groups are held in a variety of settings away from therapy bases, records of activity will need to be transported (see security section below). For the more educational work like Stress Buster, some questionnaire data will be collected. For other group work it will depend on the type of group and there will be a degree of clinical judgement about what records are appropriate. These should be written up and stored at a therapy base and ideally should not be taken to other sites, even if the groups are held elsewhere. A summary of the group should be stored on IAPTus when it finishes which will include any information which will be needed for audit or reporting, and the records destroyed.

## **20 Video/Audio Recording**

### **Reasons for Recording**

Therapists are required to continuously develop their professional experience and skills. To help ensure high standards of practice it is common practice to audio-tape therapy sessions.

Audio and Video recording can only take place with the patients' prior consent. They must sign the 'consent for Audio / Video Recording form' – Appendix 2, this also provides information to both the therapist and patient on the use of the recordings.

The recordings must be stored in a confidential manner and will usually be destroyed as soon as the recording has been used for its expressed purpose e.g. supervision, training portfolio.

The patient has the right to withdraw their consent at any time, without giving a reason. This would not affect your continuation of sessions with them.

## **21 Text Message and Email Communication**

Whilst text messages have been referred to in this policy, this is not generally an acceptable method of communication to be initiated or used by staff for communicating with colleagues or patients. This is due to the difficulties in ascertaining if the message has actually been received. Where text messaging is used for communication, a written record of the content of the text message, sent and received, should be made in the patient's health record.

Appropriate measures should be put in place to ensure that the message has been received.

## **22 Supervision and education**

### Content notes

All clinical staff in Outlook South West LLP are required to have regular supervision as part of our evidence-based approach to delivering psychological therapies. The process of supervision involves the supervisor having access to all the material which has been obtained during the course of therapy with particular patients.

### Case reports

The use of case material in educational settings or as part of accreditation processes will be covered by the relevant professional body and Higher Educational Institute (HEI)

## **23 Ownership, Archiving and Destruction of Records**

Outlook South West LLP also has a responsibility for archiving and destruction of records that belong to them. This is in accordance with the Data Protection Act 1998 and in collaboration with the following guidelines;

*The Data Protection Act 1998 (effective from 1 March 2000) governs access to the health records of living people.*

*The Access to Health Records Act 1990 governs access to the health records of deceased people.*

Once you have discharged a patient, the records should be forwarded to the head office (FAO the Archive team), so that we can log and archive the records. Records ready for archiving should not be kept for longer than they are required in any GP surgery or Outlook South West LLP locality office. **As a guide, the majority of clinical records are archived for a period of 20 years.** For further information on destroying records, please refer to the Acceptable Use policy and to the archiving guidance document in **Appendix 3**.

## **24 Procedure for dealing with missing records**

Outlook South West LLP has set out the following procedure that staff must follow, when records are mislaid or missing.

Records are legal documents and as such can be required as evidence before:

- A Court of Law
- The Parliamentary Proceedings Committee
- The Professional Conduct Committee of the United Kingdom
- The General Medical Council
- Other statutory regulatory bodies

When a staff member becomes aware that a record is lost they should report the missing record to their Information Asset Owner, as soon as possible. The Information Asset Owner should ensure that a thorough search takes place, using tracking and patient contact history (dependent on the type of record), including initiating a search in the Outlook South West LLP archives, if applicable.

The event must be logged via an untoward incident report, with a copy forwarded to the Senior Information Risk Officer.

In the case of clinical records, a temporary record should be created, clearly marked as a temporary record, populated with all relevant information available for the patient. A temporary record should be set up and tracked. When the original records are located the missing record log should be updated with the details of where/how the original record was located, and the two folders should be merged.

## **25 Monitoring**

The Information Asset Owner should send a copy of the missing records log to the Senior Information Risk Officer on the last day of each month with appropriate supporting information.

The Senior Information Risk Officer will report quarterly to the Information Governance Team. This should include information on the number of records logged as missing, observed trends and remedial action recommended or taken.

## **26 Record Quality**

*To create and keep records which are adequate, consistent, and necessary for statutory, legal and business requirements.*

Outlook South West LLP's records should be accurate and complete, in order to facilitate audit, fulfil the company's responsibilities, and protect its legal and other rights. Records

should show proof of their validity and authenticity so that any evidence derived from them is clearly credible and authoritative.

## Appendix 1

### Records Management – Retention Periods for clinical and non-clinical records (Long Version)

Based on the NHS Code of Practice – Types of records that maybe relevant to Outlook South West LLP have been extracted and listed below (regardless of the media on which they are held, including paper, electronic, images and sound)

Type	Details	Minimum Retention period
Clinical	All clinical records including video/audio recordings, clinical health records and reports, supervision notes, diaries, patient letters/correspondence, referral letters,	Retain for 20 years
	Scanned records relating to patient care	Retain for the period of time appropriate to the patient/specialty, eg children’s records should be retained as per the retention period for the records of children and young people; mentally disordered persons (within the meaning of the Mental Health Act 1983) 20 years after the last entry in the record or 8 years after the patient’s death if patient died while in the care of the organisation. NB Providing the scanning process and procedures are compliant with BSI’s BIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically once the case notes have been scanned the paper records can be destroyed under confidential conditions.
Financial	Financial Records, including expenses	7 years

	Accounts – annual (final – one set only)	30 years
	Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (eg waiting list initiative, private finance initiative)	6 years after end of financial year to which they relate
	Contracts – financial Approval files	15 years
	Approved suppliers lists	11 years
	Contracts – non-sealed (property) on termination	6 years after termination of contract
	Contracts – non-sealed (other) on termination	6 years after termination of contract
	Contracts – sealed (and associated records)	Minimum of 15 years, after which they should be reviewed
	Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (eg waiting list initiative, private finance initiative)	6 years after end of financial year to which they relate
	Payroll (ie list of staff in the pay of the organisation)	6 years after termination of employment
Personnel	Job applications (successful)	3 years following termination of employment
	Job applications (unsuccessful)	1 year
	Job descriptions	3 years



Leavers' dossiers	6 years after individual has left. Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time. The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans
Letters of appointment	6 years after employment has terminated or until 70th birthday, whichever is later
Pension Forms (all)	7 years
Personnel/human resources records –major (eg personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained)) NB Includes locum doctors	6 years after individual leaves service, at which time a summary of the file must be kept until the individual's 70th birthday. Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time. The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans
Personnel/human resources records – minor (eg attendance books, annual leave records, duty rosters (i.e. duty rosters held on the individual's record not the organisation or departmental rosters), clock cards, timesheets (relating to individual staff members)) NB Includes locum doctors	2 years after the year to which they relate
Study leave applications	5 years

	Training plans	2 years
Quality	Complaints	action– Files closed annually and kept for – 6 years following closure.
	Accidents and Incidents – including report forms and investigation notes/reports and accident register (Reporting of Injuries, Diseases and Dangerous Occurrences register	10 years
	Serious Incident files	30 years
	Annual reports, including IG reports, Quality reports etc	3 years
	Audit records ((e.g. Organisational Audits, Records Audits, Systems Audits) – Internal & External in any format (paper, electronic etc)	2 years from the date of completion of the audit
	Freedom of Information requests	3 years after full disclosure;10 years if information is redacted or the information requested is not disclosed
	Health and safety documentation	3 years
	Subject Access Requests, (excluding Freedom of Information requests)	6 years after last action
	Statistics (including contract minimum data set, statistical returns to DH, patient activity)	3 years from date of submission
Communication	Patient information leaflets	6 years after the leaflet has been superseded

& Media	Patient Surveys (re access to services etc)	2 years
	Press cuttings	1 year
	Press releases	7 years
Locality Management	Locality office files, including details of building work, town and planning records, maintenance logs and logs of equipment.	30 years
	Inspection reports (eg boilers, lifts)	Lifetime of installation. If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely
	Leases – the grant of leases, licences and other rights over property	Period of the lease plus 12 years
	Maintenance contracts (routine)	6 years from end of contract
	Property acquisitions dossiers	30 years
	Property disposal dossiers	30 years
General	Diaries (office)	1 year after the calendar year to which they refer
	Meeting minutes and agendas	
	Receipts for registered and recorded mail, post books	2 years following the end of the financial year to which they relate
	Records documenting the archiving, transfer to public records archive or destruction of records	30 years

	<p>Project files (over £100,000) on termination, including abandoned or deferred projects</p> <p>Project files (less than £100,000) on termination</p>	<p>6 years</p> <p>2 years</p>
	<p>History of organisation or predecessors, its organisation and procedures (eg establishment order)</p>	<p>30 years</p>
	<p>Manuals – policy and procedure (administrative and clinical, strategy documents)</p>	<p>10 years after life of the system (or superseded) to which the policies or procedures refer</p>
	<p>Papers of minor or short-lived importance not covered elsewhere, eg: advertising matter – covering letters – reminders– letters making appointments – anonymous or unintelligible letters– drafts– duplicates of documents known to be – preserved elsewhere (unless they have important minutes on them)indices and registers compiled for – temporary purposes routine reports– punched cards– other documents that have ceased to be of – value on settlement of the matter involved</p>	<p>2 years after the settlement of the matter to which they relate</p>

Electronic records are supported by audit trails, which record details of all additions, changes, deletions and viewings. Typically, the audit trail will include information on:

- ■ who – identification of the person creating, changing or viewing the record;
- ■ what – details of the data entry or what was viewed;
- ■ when – date and time of the data entry or viewing; and
- ■ where – the location where the data entry or viewing occurred.

1. Audit trails are important for medico-legal purposes as they enable the reconstruction of records at a point in time. Without its associated audit trail, there is no reliable way of confirming that an entry is a true record of an event or intervention.
2. NHS Connecting for Health is considering the impact of the retention of audit trail data, eg whether it should be retained for at least the same period as the data to which it relates. There is also an unresolved issue regarding the association of audit trail data with electronic GP records transferred between practices.
3. Advice and guidance specific to audit trails will be issued in due course on the Department of Health website (<http://www.dh.gov.uk/PolicyandGuidance/OrganisationPolicy/RecordsManagement/>). In the meantime, NHS organisations are advised to retain all audit trails until further notice.

## **Appendix 2**

### **Consent for Audio / Video recording**

#### **Reasons for Recording**

All therapists are required to continuously develop their professional experience and skills. To help ensure high standards of practice it is common practice to audio-tape therapy sessions.

The recordings are reviewed by your therapist and their clinical supervisor with the goal of fine-tuning the treatment you receive.

Recordings will be used only for your therapist's supervision and professional development and will not be used for training others, for research or any other purpose without further consent being obtained.

You may listen/view the recordings if you wish

The recordings will be stored in a confidential manner and will be destroyed 7 years after your date of discharge. You may request that the recordings be destroyed earlier if you wish.

You may withdraw your consent at any time without giving a reason and this would not affect your continuation of sessions.

You can also ask that the recording be paused at any time if there are parts of a session you prefer not to be recorded.

**Please take your time to consider these points and ask your therapist if you have any additional queries or concerns.**

**Thank you**

**Consent for Audio / Video recording**

I have read the information on Reasons for Recording and have had time to think about it.

I have been informed that the tapes may be listened to or view by my therapist and their clinical supervisor to monitor and fine tune the treatment I am receiving.

Recordings will be used only for supervision and my therapist’s professional development and will not be used for training others, for research or any other purpose.

I consent to my sessions being taped.

I understand the recordings will be treated as confidential documents, that they will be stored securely and they will be destroyed 7 years after my date of discharge.

I am aware I may listen to or view the recordings if I wish.

I have been informed that I may withdraw my consent at any time without needing to give a reason and that this will not affect my continuing with sessions

I understand that I can ask for the recording to be paused at any time if there are parts of the session I do not want recorded.

**Patient**

Signature \_\_\_\_\_ Print \_\_\_\_\_ Date \_\_\_\_\_

**Therapist**

Signature \_\_\_\_\_ Print \_\_\_\_\_ Date \_\_\_\_\_

### Appendix 3

#### The key elements of the record management strategy.

The key elements of this strategy will be implemented as follows:

Strategic Goal	Objective	Action	Responsibility	Target Date
<b>Responsibility and Accountability</b>	To provide a clear system of accountability and responsibility for records	<b>Level 1: Essential</b>		
		Establish a records management strategy and framework to enable the implementation, ongoing monitoring and review of records management	Partners and Senior Compliance Manager	
		Identify a Partner to hold overall accountability for records management.	Partners	
		Identify a qualified Records Manager to be responsible for co-ordinating and advising on Record Managements issues, reporting to the accountable Partner.	Partners	
		Identify key staff with responsibilities for Records Management, each of whom will be responsible for a records/information set, and will work with the Records Manager to implement the Records Management Strategy.	Records Manager	
		Ensure the induction training for all new staff includes records management and information issues	Records Manager	
		<b>Level 2: Desirable</b>		
		Identify an Archives Officer to be responsible for the archiving and destruction of records, as indicated by the Local Records Officers	Partners & Records Manager	
		Ensure that job descriptions for all roles within the company (both clinical and admin) outline individual record keeping responsibilities. Any key roles with additional responsibilities for Records	Records Manager & Personnel Records Officer	



		Management should have this outlined in their job description.		
		Produce a framework of competencies to outline the knowledge and skills required for records and information management	Records Manager	
		Undertake regular reviews of record management training needs	Records Manager	
<b>Record Quality</b>	To create and keep records which are adequate, consistent, and necessary for statutory, legal and business requirements	<b>Level 1: Essential</b>		
		Develop good practice guidelines for each area of record management to establish appropriate standards of record creation and record keeping within the company, taking into account current Data Protection and Freedom of Information legislation	Local Records Officers	
		Identify all records vital to the continuation of the business in the event of disaster and make provision for their protection (cross-reference with the Risk Management Strategy)	Partner and Records Manager	
		<b>Level 2: Desirable</b>		
		Review the individual good practice guidelines for each area of records management to establish common and consistent standards within the company	Records Manager	
		Reduce the duplication of records to improve information sharing, reduce cost and save space	Local Records Officers	
		Develop procedures to ensure the authenticity of electronic records	Local Records Officers	
<b>Management</b>	To achieve systematic, orderly and consistent creation, appraisal, retention and disposal procedures for records during their lifecycle	<b>Level 1: Essential</b>		
		Undertake an inventory of all company records, both patient clinical records and corporate records held in either hard copy or electronically. Identify all record/information sets, the quantity and where/how they are stored.	Local Records Officers	
		Review existing records management practices to establish what needs to be done to comply with the 'Records Management: NHS Code of Practice'	Local Records Officers	

		Produce a central schedule of records retention that outlines how long each type of record should be kept for. This should be consistent with the Retention and Disposal schedules detailed in the ' <i>Records Management: NHS Code of Practice</i> '	Records Manager & Local Records Officers	
		Produce and maintain an Archive Log that documents what type of record is being archived (a title and description), the archive date, where the archive will be held, any risks associated with the destruction of the record, and the date and way in which the document can be disposed of	Local Records Officers	
		Produce and maintain a log of records which have been destroyed, showing the type of record (a title and description), and the method and date of destruction	Archives Officer	
		<b>Level 2: Desirable</b>		
		Document the procedure for determining when records need to be archived, where they should be archived	Local Records Officer	
		Produce and maintain a central Archive Log that collates each record/information set	Records Manager	
		Establish procedures for the continuous monitoring of the records management process to ensure that legal and statutory requirements are met and new types of records have a lifecycle determined at the point of creation	Records Manager	
<b>Security</b>	To provide systems which maintain appropriate confidentiality, security and integrity for records in their storage and use	<b>Level 1: Essential</b>		
		Develop and disseminate policies and procedures to protect records from unauthorised access, maintaining adequate audit trails	Local Records Officers	
		Implement secure safe, storage arrangements for confidential and sensitive information and documents, allowing access by authorised personnel only.	Local Records Officers	
		Conduct a risk assessment of storage arrangements to decide	Local Records Officers	

		whether the information is safe from fire, flood and theft and unauthorised access		
		Organise the relocation of records into secure and safe archive storage when they are no longer required, to await destruction	Local Records Officers & Archive Officer	
		Develop appropriate Information Sharing Protocols for the exchange of confidential and personal information	Partner & Records Manager in consultation with PCT	
		Ensure that standards for the safe and secure transportation of records are strictly applied	Records Manager & Archives Officer	
		<b>Level 2: Desirable</b>		
		Collate the risk assessments of storage arrangements	Local Records Officers	
		Develop and implement and full and tested business contingency or recovery plans	Partner	
<b>5 Access</b>	To provide clear and efficient access for employees and others who have a legitimate right of access to Trust records, and ensure compliance with current Data Protection and Freedom of Information legislation	<b>Level 1: Essential</b>		
		Implement audit trails where necessary, while still ensuring information can be retrieved when required	Local Records Officer	
		Assess systems to determine any unnecessary access restrictions at the point of records creation	Local Records Officer	
		Implement Freedom of Information procedures, as outlined in the Confidentiality Policy	Records Manager	
<b>6 Audit</b>	To audit and measure the implementation of the records management strategy against agreed standards.	<b>Level 1: Essential</b>		
		Provide advice and support for Operational Managers in meeting agreed standards	Records Manager	
		<b>Level 2: Desirable</b>		

		Monitor the compliance with the records management standards (e.g. response to requests for information, FOI requests, record keeping etc)	Records Manager	
<b>7 Training</b>	To provide training and guidance on responsibilities and good practice for all staff involved with records.	<b>Level 1: Essential</b>		
		Provide relevant procedural instructions and good practice guidelines to all staff.	Local Records Officer & Records Manager	
		Develop training plans for all staff, and more detailed training for those with responsibilities for Records Management	Records Manager & Partner	
		Provide specific training and instruction of Data Protection and Freedom of Information legislation	Records Manager & Partner	

## Appendix 4

### OSW Archiving Plan 2014

#### Summary

All the historical paper work in the OSW archives that relates to patients discharged up to and including 31.12.2013 is kept in **paper format** only in an archive store.

Everything that relates to a patient discharge from 01.01.2014 onwards will be **uploaded to IAPTus** and the paper record will be destroyed. This should take place on a regular (possibly daily basis) and be part of routine work.

The bulk of the administration for this task is carried out by the Compliance Administration Manager and members of the Clinical Admin team at the head office.

There are different steps associated with the task so that if something has been missed / done in error at step 2, the person at step 3 will notice records filed in an incorrect location. Therapists should forward via the NHS courier (or hand deliver) to the head office any records for archiving. Records should not be stored in locality offices or GP surgeries for longer than they are required (once a patient has been discharged, the records should be archived).

#### THE PLAN

##### **Step 1**

A box file with the archived paper work for a year is to be collected by the Compliance Administration Manager from the Archive store and brought to the head office. These boxes will be securely stored once at the head office.

##### **Step 2 (Person A)**

All the paper work is to be removed from the box and 26 suspension files are to be placed in the empty box with tabs labelled A-Z on each suspension file.

The pile of paper work is then to be sorted through and filed in the suspension files by the surname of the patient.

Date of discharge should have already been noted on the cover page of the paper archives – it should be noted if this is correct to the relevant year of discharge that the box refers to. If it is different, it should be placed to one side and passed to the Compliance Administration Manager to put in the correct year of discharge box.

##### **Step 3 (Person A or B)**

Once all of the paper work has been sorted alphabetically, you should then go through each suspension file and staple together the paper work that relates to the same patient (if this has not already been done).

**Step 4 (Person B)**

Take the box of records that have been sorted alphabetically. Take the first suspension file with records in and add the relevant details to the Archive Database. Once you have added the details, place a red **A** on the first page to indicate that the record has been added to the archive database, with the date this was done.

Once the whole box has been added to the database it should be passed to the Compliance Administration Manager so that it can be taken back to the Archive room for storage.

**NOTHING SHOULD BE SHREDDED WITHOUT DISCUSSION WITH THE COMPLIANCE ADMINISTRATION MANAGER OR THE SIRO FIRST**

Appendix 5

Example of the OSW archiving Log (log saved at I:\Quality\Archives\Outlook South West Archives\Archive Master Log)

AS MUCH INFORMATION AS IS AVAILABLE SHOULD BE ADDED TO THE LOG.

Archive Box Number	Date archived under 2014 procedures	IAPT us #	Forename	Surname	DOB	Surgey	NHS #	Date of Discharge from service	Brief description of what is being archived	To be destroyed date	Actual date of destruction	By whom	Method of destruction
2005 box 1	10.08.14	12345	Smith	John	01/01/1901	Branel	123456789	12.12.05	Referral letter, session notes	31.12.2025			

## Equality Impact Assessment Form

### Stage 1 – Initial Assessment

Name of Individual completing assessment	Becky Biddick	Locality	Company wide
Name of the function, policy, practices, service	Records Management & Life Cycle Policy	Is this a new or existing policy?	Existing
Date policy was implemented	TBC	Who does the policy affect?	Patients, third parties and staff.
Communication	Staff Induction, Operational Management Meetings, Connect E Bulletin Copies, Update Days, Website		

Equality Group	Positive Impact	Negative Impact	No Impact	Reasons for decision
Age			X	
Disability			X	
Marriage & Civil Partnership			X	
Pregnancy & Maternity			X	
Race			X	
Religion & Belief			X	
Gender			X	
Sexual Orientation			X	
Gender Reassignment			X	

Following completion of the stage 1 assessment, is stage 2 (Full Assessment) necessary?

Yes  No

Date completed: 18<sup>th</sup> September 2014

Sign by member of staff completed assessment : B Biddick  
Records Management and Life Cycle Policy\_Version 1



**Privacy Impact Assessment Form**

**Stage 1 – Initial Assessment**

	<u>Yes/No</u>	<u>Comments</u>
<p><b><u>Technology</u></b></p> <p>1. <u>Does the development or revision of this policy apply new or additional information technologies that have substantial potential for privacy intrusion?</u></p>	Yes	Email records, text message records, audio/video recordings
<p><i>Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.</i></p>		
<p><b><u>Identity</u></b></p> <p>2. Does the development or revision of this policy involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?</p>	Yes	Re use of existing identifiers – for example <u>within the Archive master log</u>
<p><i>Examples of relevant development or revision of this policy features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence development or revision of this policy risk.</i></p>		
<p>3. <u>Might the development or revision of this policy have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?</u></p>	No	<u>Anonymous records / locked records can still be held, with limited staff members having access as required.</u>
<p><i>Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.</i></p>		

<p><b><u>Multiple organisations</u></b></p> <p>4. Does the development or revision of this policy involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?</p>	<p>No</p>	
<p><i><u>Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of development or revision of this policy s involving multiple organisations. Compensatory protection measures should be considered.</u></i></p>		
<p><b><u>Data</u></b></p> <p>5. <u>Does the development or revision of this policy involve new or significantly changed handling of personal data that is of particular concern to individuals?</u></p>	<p>No</p>	
<p><i><u>The Data Protection Act at s.2 identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings. There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft. Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.</u></i></p>		
<p>6. <u>Does the development or revision of this policy involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?</u></p>	<p><u>Yes</u></p>	<p><u>The commencement of the archiving project which involves therapists securely transporting patient records from their locations to the head office for central archiving. The handling is still only within OSW though.</u></p>
<p><i><u>Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.</u></i></p>		
<p>7. <u>Does the development or revision of this policy involve</u></p>	<p><u>No</u></p>	

<p><u>new or significantly changed handling of personal data about a large number of individuals?</u></p>		
<p><i>Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.</i></p>		
<p>8. <u>Does the development or revision of this policy involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?</u></p>	<p><u>No</u></p>	
<p><i>This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.</i></p>		
<p><b>Exemptions and exceptions</b></p> <p>9. <u>Does the development or revision of this policy relate to data processing which is in any way exempt from legislative privacy protections?</u></p>	<p>Yes</p>	<p>Records can include court orders, safeguarding reports</p>
<p><i>Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.</i></p>		
<p>10. <u>Does the development or revision of this policy 's justification include significant contributions to public security measures?</u></p>	<p><u>No</u></p>	
<p><i>Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.</i></p>		
<p>11. <u>Does the development or revision of this policy involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?</u></p>	<p><u>No</u></p>	
<p><b>Evaluation</b></p> <p>12. <u>In light of the questions above,</u></p>	<p><u>No</u></p>	

is a privacy impact assessment needed?		
13. <u>Will the scope of the PIA be wide-ranging, or focused on particular aspects of the development or revision of this policy?</u>	<u>n/a</u>	
14. <u>Is privacy law compliance checking recommended?</u> <u>If yes then conduct a privacy law compliance check</u>	<u>n/a</u>	
15. <u>Is Data Protection Act compliance checking recommended</u>	<u>Yes</u>	<u>The record management and lifecycle within OSW complies with the Data Protection Act and includes links to the main principles.</u>
16. <u>Do the activities involve the handling of 'personal data'? If yes then conduct a data protection compliance check</u>	<u>Yes</u>	

Date completed	18 <sup>th</sup> September 2014
Signature of person completing this assessment	B Biddick