NHS
Wandsworth
Clinical Commissioning Group

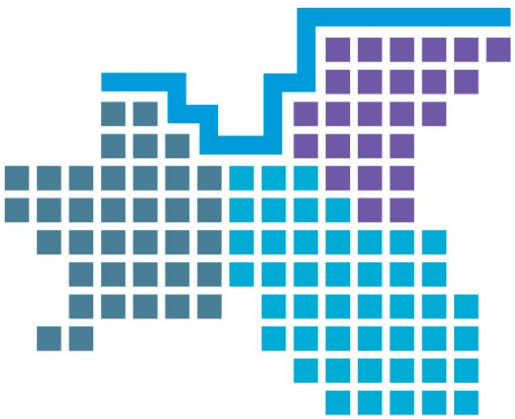
Information Life Cycle Management Protocol

Version - Final

Date for Review: 1 December 2017

Lead Director: Performance, Quality and Corporate Affairs

NOTE: This is a CONTROLLED Document. Any documents appearing in paper form are not controlled and should be checked against the server file version prior to use.



DOCUMENT CONTROL AND AMENDMENT RECORD

Document Name:	Information Life Cycle Management Protocol
Consultation:	SIRO &IGSG and IGC
Approved by:	IGSG & Integrated Governance Committee(IGC)
Description:	A Protocol for the management of the Information Lifecycle from Creation through Use to ultimate Retention or Destruction.
Audience:	All Staff
Contact details:	IG Manager
Supersedes	Information Life Cycle Management Protocol 2012-2014

Change History

Version	Date	Author	Approver	Reason
0.1	Oct-14	IG manager		Initial Draft
0.2	Oct-14	SIRO		Review
0.3	Nov 2014	IG manager	IGSG	Approval
0.4	Dec-14	IG manager	IGC	Approval

CONTENTS

1. Introduction

This document sets out the information management principles for the organisation at each stage of the information's lifecycle. Furthermore, it aims to outline the responsibilities of all staff for the proper management of information.

The organisation must ensure that it manages information throughout its lifecycle and as it flows internally and externally with partners.

The protocol applies to all stages of the lifecycle; it sets out the minimum requirement for staff at each stage of information processing. These must be met alongside the provision of security, confidentiality and the use of information to discharge the functions of the organisation.

It intends to set out:

- Best Practice guidelines for information and records management across all formats
- To reflect the NHS Records Management Code of Practice
- To maintain the accessibility, integrity and availability of information
- To support the information and records management strategy and review
- The requirements for ongoing monitoring, reviews and regular audits of information and records

2. Information Lifecycle Stages

The protocol applies to all stages of information and records management lifecycle, from the initial identification of a requirement through to its ultimate disposal:

- System Design
- Creation
- Use
- Maintenance
- Disposal

Detailed information of the stages of the Information lifecycle is contained in section below

2.1 Types of Information

The following is a list of information and systems within the scope of this protocol, the list is not exhaustive:

- digital or hard copy patient health records (including GP medical records);
- digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);
- digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
- digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, and other internal and external media compatible with NHS information systems);

- computerised records, including those that are processed in networked, mobile or standalone systems;
- portable communications devices such as mobile phones, Blackberry's, Personal Digital Assistant (PDA) etc.;
- email, text and other message types;

3. Information Lifecycle

3.1 System Design

One of the key elements of Information Lifecycle management is the design of systems to capture information and records. It is important that the procurement, commissioning or system design process completes a thorough analysis of:

- What information will be gathered and recorded
- How will standards of data quality be supported and maintained
- How will these standards be aligned with broader strategic and information objectives (for example performance) within the organisation
- How will information be secured
- Is it intended to transfer or share this information with third parties or external agencies and has this received the correct approval from the Caldicott Guardian or nominated deputy
- How will the Organisation ensure information is accessible throughout its lifecycle
- What metadata or context will need to be captured in the information creation process and how the system will meet these requirements
- The information risks associated with the requirements and system, the systems put in place for the management and mitigation of them

For more information see the Information Governance Framework

3.2 Creation

Information when created must be **authentic, accurate, accessible, complete, compliant, effective** and **secure** and its integrity must be protected over time.

Within a records management environment these highlighted terms have a specific meaning which is defined in Annex D.

3.3 Information Asset Register

The Information Asset Register entry must be maintained for all information assets within a Director's remit. The entry must also account for historic data sets, those that have been superseded

3.4 Validation or confirmation

Different types of information, especially clinical elements, as a part of creation require a validation or confirmation. This must be done in a timely and efficient manner by an appropriate member of staff.

3.5 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 their line manager and the Information Governance manager.

Evidential weight relies upon a clear audit trial and the ability to demonstrate that the context and content of information can be relied upon.

3.6 Retrieval

A key component of information lifecycle management is that information can be retrieved throughout its life. Retrieval must always be by staff with appropriate access and be supported by access controls.

Retrieval times must be measured by the Organisation; coverage for records especially for clinical records should be across 24 hours, 7 days a week.

Retrieval is supported by naming conventions (for files, folders and systems), version control and for databases by the use of appropriate reference systems.

3.7 Storage

Storage of all information must be systematic and consistent. Individual systems are required for different formats of records and information but they must all meet these standards. Further details are provided in the policies and procedures for the relevant systems. However, storage must always:

- Meet security standards (across physical and electronic media)
- Document produced by services on access controls and supporting documentation around who is permitted to have access
- Be registered as either a record collection or an information asset (as required)
- Meet Health and Safety requirements (contact the Health and Safety team for more details)
- Recorded – what is held in storage by each service: the extent, the type of files and location must be registered with the Information Governance team in addition to being held locally.

3.8 Information Flows

All Flows of personal identifiable information must be in accordance with legal, regulatory and department requirements. Routine flows of information with partners require an Information Sharing Agreement or Framework that outlines the basis of information sharing and obligations on each party.

Every directorate must record all flows of patient identifiable data or information both internally and externally, and the associated risks. All routine flows must be accompanied by procedures.

A review of information flows will be undertaken on an annual basis and in response to any significant organisational change

3.9 Maintenance

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 organisation and the life of the information.

3.10 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 and the Freedom of Information 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. Where appropriate, details of the disclosure must be kept as part of the record. The key statutory requirements can be found in Annex C of the Records Management: NHS Code of Practice (Part 1).

The organisation's Caldicott Guardian and any nominated delegates or support staff must be involved in any proposed disclosure of confidential patient information. Further details are available from the Information Governance manager. This process is informed by the Department of Health publication Confidentiality: NHS Code of Practice.

3.11 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 Information Governance Manager can advise on appropriate safeguards.

3.12 Disposal

Disposal is defined as the management intent for a record once it is no longer required for the conduct of current business. There are a number of stages in the disposal phase of a corporate record.

3.13 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.

3.14 Retention

The retention period varies dependant on the type of information being stored. For other types of information the specific retention periods should be checked in the documents detailed below. The information must be relevant, fit for the purpose it was intended and only retained for as long as it is genuinely required.

Details are set by the Department of Health; NHS Code of Practice Records Management (Part 2), a local version is available on the intranet along with a form to highlight any queries or concerns.

3.15 Destruction

All information and records must be destroyed appropriately. This applies across all media and to the systems that hold information (such as servers and encrypted memory sticks). For confidential, clinical and corporate information there is a destruction process through approved suppliers that produces certificates of destruction. It is the responsibilities of services and their staff to ensure that all records that contain personal information (whether patient or staff) are managed through to destruction.

3.16 Archiving

Upon the end of a retention period, information must be assessed for whether it is requires archiving or destroyed. Guidance is provided by the Department of Health and the process is managed within the Information Governance team as part of the Records Management function. More details are held in the Records Retention Schedules.

Any service that takes over legacy records must manage their disposal. Those that find records within their remit or office space must; locate the originating department, register the collection with the information governance team and ensure that it is managed appropriately.

3.17 Scanning

An important element in meeting the requirement for accessibility and completeness of records is considering which records should be scanned. This is a process that will be addressed on a case by case basis given the expenses involved. However, it is the objective to ensure all records are in one format (e.g. no hybrid paper – electronic records) especially as it relates to patient care

4. Safe Haven Principles

Within the organisation there are three standards of Safe Havens. These principles apply to all three, Safe Haven, Enhanced Safe Haven and New Safe Haven.

4.1 Principles for Safe Haven Procedures

The following principles represent the minimum requirements which must be articulated in any safe haven procedure or procedure for information transmission:

When sending information:

- Contact details must be confirmed before information is dispatched
- The information must be clearly identified as private and confidential
- A return or contact point must be included in the transmission
- Contact details must be checked before dispatch
- Those receiving the information must be informed to expect it
- Receipt of the information should be sought or provided by the process (in the case of electronic transmission)

In addition, before sending any information, all staff are required to ensure that only the minimum information is being provided, that there is a legal basis for the disclosure of information and that there is an agreement in place on the use of the information with the receiving party.

When receiving information:

- Up-to-date contact details must be maintained with all information partners. Routine reminders and up-dates should be sent.

4.2 Enhanced Safe Haven Arrangements

The highest standard of Safe Haven is a designated safe haven location. To achieve this standard, in addition to working procedures and practice to the principles articulated above:

- Access to the area or equipment **must be** controlled and locked to all non-authorised staff
- Access to the area or equipment **must** follow an authorisation process
- Any staff with access to the area or equipment **must be** authorised and trained to deal with any personal information or the transmission of personal information
- The equipment can receive safe haven transmissions in the absence of staff and hold them securely until authorised staff access the equipment
- The equipment **must be** monitored on a routine basis
- Procedures **must be** in place that outline the management of personal information and supporting guidance **must be** available for the area or equipment

Examples of Safe Haven Locations

- An area with key-code access
- An office that is routinely locked when staff are not present with a secure post box

4.3 New Safe Havens (NSH)

Department of Health policy to support the secure, restricted access and appropriate use of personal data is the use of de-identified or pseudonymous data. This led to the requirement for New Safe Havens within the areas responsible for working with data sets and databases of patient data.

All patient information systems and databases must be within areas of restricted access and should have login details that are unique to each user, in addition to network authentication. An authorisation process is required and a register of those authorised to access must be maintained by the relevant Information Asset Owners.

4.4 Registration of Safe Havens

The organisation maintains an entry on the national register of safe havens and an internal register to support the transmission of information internally.

The details required and recommended are detailed in Annexe E

4.5 Department of Health Register of Safe Havens

The Department of Health maintains a register of Safe Havens for Organisations in England and is updated on a monthly basis. For details on the register and procedure for updating details see the Information Governance Framework.

Annexe A - Useful Definitions

Personal Confidential Data **Acronym:** PCD	This is information about a person which would enable the person's identity to be established. This can be explicit such as the name and address or different items together which combined could reasonably be considered to identify the individual. For more information see the Data Protection Protocol
Sensitive Personal Information	There is a precise definition of sensitive information within the Data Protection Act 1998 for Personal Data. It includes information about the health of an individual; within the NHS it is safe to assume that most information about patients can be considered sensitive if it includes any details of health conditions or treatment. For more information see the Data Protection Protocol
Sensitive Information	This is information such as financial or security information that should be considered sensitive. Access to this information needs to be controlled and restricted to specific post holders.
Protected Personal Data Category A	This is information if wrongly released or lost could cause harm or distress to individuals. These need to be afforded the highest protection and most restricted access. Category A – Any information that links one or more identifiable living person with information about them which, if released, would put them at significant risk of harm or distress. See Information Governance Toolkit Requirement 308 for more background information

Protected Personal Data Category B	Any information about 21 or more identifiable individuals, other than information sourced from the public domain. This is a minimum standard, information on a smaller number of individuals will warrant protected personal data status because of the nature of the individuals or source of information, for example vulnerable adults or children.
Safe Haven	A ”Safe Haven” is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves, or is transmitted within the organisation by any means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven protocol and relevant procedure.

Category A – Protected Personal Data

Group 1: one or more of the pieces of information which can be used along with public domain information to identify an individual	combined with	**Group 2:** information about that individual whose release is likely to cause harm or distress

Name / addresses (home or business or both) / postcode / email / telephone numbers/driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data Protection Act 1998: racial or ethnic origin political opinions religious beliefs or other beliefs of a similar nature membership of a trade union physical or mental health or condition sexual life the commission or alleged commission of any offence or Any proceedings or sentencing relating to any offence committed or alleged to have been committed. Sensitive personal data will also include: DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / employment record / school attendance or records / material relating to social services including child protection and housing.
These are not exhaustive lists. Sensitive Data should be clearly identified in the Information Asset Register entry for the information set.		

Annexe D - Records Quality Criteria

Authentic –

It must be possible to prove that a record is what it purports to be by keeping a record of its management through time.

Accurate –

It must be possible to trust the content of a record as a reliable representation of the transaction to which it attests.

Accessible –

It must be possible to locate, retrieve, render and interpret a record and understand the sequence of activities in which it was created and used for as long as such evidence is required.

Complete –

It must be possible to protect a record against unauthorised alteration and to monitor and track any authorised annotation, addition or deletion.

Compliant –

Records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.

Effective –

Records must be maintained for specific purposes and the information contained in them must meet those purposes.

Secure –

It must be possible to ensure the integrity of the record and the record keeping system in which it is kept.

Annex E – DH Safe Haven Requirements

Department of Health Safe Have Requirements		Local Nominations Requirements	
ODS Code	Organisation Data Service code, this is set by the Department of Health and is the organisations unique identifier for connection to the N3 network and other data processing.		
Organisation Name	This is the legal title of the organisation	**Directorate or Site Name**	This is the legal title of the organisation
Safe Haven Contact – Title of Post	The contact point for the Safe Haven. Note this must be a post title not an individual's name	**Safe Haven Contact – Title of Post**	The contact point for the Safe Haven. Note this must be a post title not an individual's name
Address Line 1	The first line of the postal address of the Safe Haven	**Address Line 1**	The first line of the postal address of the Safe Haven
Address Line 2	The second line of the postal address of the Safe Haven	**Address Line 2**	The second line of the postal address of the Safe Haven
Town	As described	**Town**	As described
County	As described	**County**	As described
Post Code	The postcode for the Safe Haven	**Post Code**	The postcode for the Safe Haven
Tel		**Tel:**	
Fax	The Fax number for the Safe Haven. This must be a Safe Haven Fax in a secure located. If none is available this entry should be left blank.	**Safe Haven Fax:**	The Fax number for the Safe Haven. This must be a Safe Haven Fax in a secure located. If none is available this entry should be left blank.
Email (nhs.net)	Not required for the Directory currently but should reflect either the named Posts email address or the Safe Haven email address	**Email (nhs.net)**	Required for the Directory currently but should reflect either the named Posts email address or the Safe Haven email address
		Safe Haven Area	Does the area meet the requirements of a **Safe Haven Area**? Is it locked and access routinely restricted?