NHS
England

Corporate Document and Records Management Policy

NHS England Information Reader Box	
Directorate	**Trans. & Corp. Ops.**
Publications Gateway Reference:	**01767**
Document Purpose	Guidance
Document Name	Document and Records Management Policy v4.0
Author	Sarah Graham Jan Gavin
Publication Date	16 May 2017
Target Audience	CSU Managing Directors, NHS Trust Board Chairs, NHS England Regional Directors, NHS England Directors of Commissioning Operations, All NHS England Employees
Additional Circulation List	N/A
Description	Advice and guidance to all NHS England staff with regards to the creation, management, storing and disposal of records.
Cross Reference	N/A
Superseded Docs (if applicable)	Document and Records Management Policy v3.0
Action Required	N/A
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	Sarah Graham
	Records Manager, Corporate Information Governance
	Transformation and Corporate Operations
	4th Floor West, Quarry House
	Quarry Hill, Leeds, LS2 7UE
	07860 179022

Corporate Document and Records Management Policy

Version number: 4.0

First published: April 2013 v1
February 2014 v2
June 2014 v3
May 2017 v4.0

Prepared by: Corporate Records Manager

Contents

Contents 3
1 Introduction 4
2 Background 5
3 Scope 6
4 Roles and Responsibilities 6
5 Corporate Level Procedures 7
5.6 Records and Information Life Cycle Management...8
5.7 Record Retention Schedule...9
5.8 Records involved in Investigations, Litigation and Legal Holds 10
5.9 Record Naming and Good Practice..10
5.10 Record Maintenance 12
5.11 Record Access 12
5.12 Record Disclosure 12
5.13 Record Closure 13
5.14 Record Appraisal...13
5.15 Record Transfer 13
5.16 Record Disposal..14
5.17 Scanning 14
5.18 Records Security: Work Base, Home Working, Agile Working.....................15
6 Distribution and Implementation... 16
7 Equality Impact Assessment…………………………………………………… 16
8 Monitoring Compliance with the Policy... 17
9 Associated Documentation.. 17
Appendix A: Records Management Co-ordinator roles and responsibilities............. 19
Appendix B: Records Management Glossary of Abbreviations and Acronyms 20
Appendix C: NHS England Electronic Document Naming Convention..................... 22
Appendix D: Protective Marking Scheme………………………………………25
Appendix E: Glossary of Terms.. 29
Appendix F: Disposal Certificate …………………………………………………32
Version Control Tracker... 33

1 Introduction

1.1 All NHS England staff members must ensure they are familiar with the contents of this policy, which describes the standards of practice we require in the management of our corporate records. It is based on current legal requirements and professional best practice.

1.2 All organisations need to keep some records, and patients and the public would rightly expect that NHS England maintains records on its activities and decisions that affect their health service in an exemplary way.

1.3 Records and Documents are different. Documents consist of information or data that can be structured or unstructured and accessed by people in NHS England. Records provide evidence of the activities of NHS England's functions and policies. Records have strict compliance requirements regarding their retention, access and destruction, and generally have to be kept unchanged. Conversely, all records are documents.

1.4 A record can be in various formats including email, paper, digital, social media, videos and telephone messages.

1.5 Records are created to provide information about what happened, what was decided, and how to do things. Individuals cannot be expected or relied upon to remember or report on past policies, discussions, actions and decisions accurately all of the time. So, as part of their daily work they keep a record – by updating a register or database, writing a note of a meeting or telephone call, audio recordings of customer interaction or filing a letter or email – which ensures that they and their successors have something to refer to in the future.

1.6 Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality evidence-based healthcare. Information has most value when it is accurate, up-to-date and accessible when it is needed. An effective records management function ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required.

1.7 Records management is about controlling records within a framework made up of policies, standard operating procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the organisation benefits from effective management of one of its key assets, its records.

1.8 A records retention schedule is a control document. It sets out the classes of records which NHS England retains and the length of time these are retained before a final disposition action is taken (i.e. destruction or transfer to The Archives). It applies to information regardless of its format or the media in which it is created or might be held. All staff members should be familiar with this records retention schedule and apply retention periods to records.

1.9 A records management policy is a cornerstone of effective management of records in an organisation. It will help to ensure NHS England keeps the records it needs for business, regulatory, legal and accountability purposes.

1.10 The purpose of this policy is to establish a framework in which NHS England's records can be managed, and to provide staff members with a high-level overview of the legal obligations that apply to NHS records.

2 Background

2.1 NHS England will take actions as necessary to comply with the legal and professional obligations set out for records, and in particular:

- Public Records Act 1958
- Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act 2000
- Records Management Code of Practice for Health and Social Care 2016
- NHS Information Governance: Guidance on Legal and Professional Obligations
- General Data Protection Regulations (due in May 2018)

a. The Public Records Act 1958 is an Act of Parliament to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.
b. The Data Protection Act 1998 is an Act of Parliament which regulates the processing of personal data relating to living individuals, including the obtaining, holding, use or disclosure of such information. Access to the health records of living patients is governed by this Act.
c. The Freedom of Information Act 2000 is an Act of Parliament that makes provision for the disclosure of information held by public authorities or by persons providing services for them. The Lord Chancellor's Code of Practice on the management of records is issued under section 46 of this Act.
d. The Access to Health Records Act 1990 is an Act of Parliament that regulates access to the health records of a deceased person.
e. The Regulation of Investigatory Powers Act 2000 which permit the 'interception' of communications. Such interception must be proportionate to the needs of the organisation, society and the users of the communication system.
f. The Records Management Code of Practice for Health and Social Care 2016 was published by the Information Governance Alliance in July 2016. It is a best practice guide for the management of records for those who work within or under contract to NHS organisations in England. They are based on legal requirements and professional best practice.
g. NHS Information Governance: Guidance on Legal and Professional Obligations provides guidance on the range of legal and professional obligations that affect the management, use and disclosure of information.

2.2 Failure to comply with the regulations stated in paragraph 2.1.could result in reputational damage to NHS England and carries financial penalties of up to £500,000 imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

3 Scope

3.1 Staff of the following NHS England areas are within the scope of this document:

- Central Teams
- Regional Teams
- All Commissioning Support Units
- NHS Improving Quality
- Strategic Clinical Networks
- Offices (e.g. Chairs, Professional Committees)
- Staff working in or on behalf of NHS England (this includes employees, contractors, temporary staff, secondees, and honorary appointees).
- Sustainability and Transformation Partnerships

4 Roles and Responsibilities

4.1 The Chief Executive through the Executive Management Team is accountable for Records Management within NHS England.

4.2 The National Director of Transformation and Corporate Operations Directorate has the lead responsibility for Records Management and for ensuring this policy is implemented and becomes an active document within NHS England.

4.3 The Corporate Records Manager has operational responsibility for the Records Management Policy and is responsible for the overall development and maintenance of the Records Management Framework and for ensuring this policy complies with legal and regulatory edicts. They are also responsible for providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness.

4.4 The Corporate Records Manager is responsible for developing and supporting a culture of high quality records management practice across NHS England to deliver associated organisational benefits. They are also responsible for knowing what records NHS England holds and where they are, by conducting regular stock-takes of records.

4.5 The Corporate Records Manager is responsible for ensuring that records created by NHS England are stored securely and that access to them is controlled.

4.6 The Director of HR is responsible for the application of this policy in respect of ensuring effective employee records management and for managing access requests for those records made under the Data Protection Act 1998.

4.7 Information Asset Owners are responsible for ensuring the asset they ‘own’ is managed in accordance with this policy, and also for maintaining adequate records within the context, both legal and regulatory, of the business area the asset operates. For example, Estates and Facilities must be able to demonstrate how they comply with current Health and Safety legislation.

4.8 Information Asset Administrators are responsible for assisting the Information Asset Owners in the management of the records that they ‘own’, in accordance with point 4.7.

4.9 Records Management Coordinators within each business area will champion records management from a local level supporting their team in records management matters. Roles and responsibilities are outlined in Appendix A.

4.10 All staff are responsible for keeping a record of any significant business transaction conducted as part of their duties for NHS England. The record should be saved appropriately, a retention period assigned and access controls applied if necessary.

5 Corporate Level Procedures

5.1 This Policy covers the management of both documents and records in NHS England. The policy sets in place the strategic governance arrangements for all documents and records produced and received by NHS England in accordance with agreed best practice as well as the principles established in ISO 15489 (the International British Standard for Records Management).

5.2 This policy is mandatory and applies to all information in all formats. It covers all stages within the information lifecycle, including create/receive, maintain/use, document appraisal, declare as a record, record appraisal, retention and disposition.

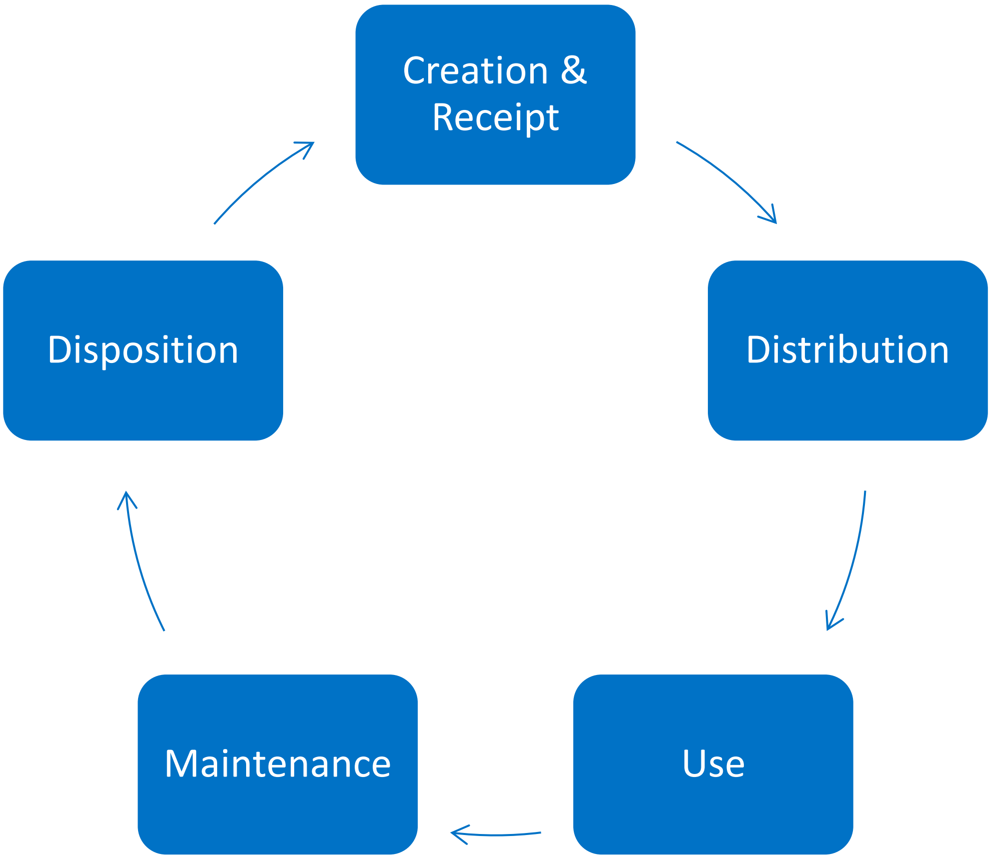
5.3 Staff members must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000 or the Data Protection Act 1998.

5.4 Staff members are expected to manage records about individuals in accordance with this policy irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status.

5.5 Where records contain any abbreviations or acronyms which are not listed in the Records Management Glossary of Abbreviations and Acronyms please contact the Records Management department to ensure your abbreviation is added. Please see Appendix B.

5.6 Records and Information Life Cycle Management

5.6.1 Records and Information Management plays an integral role within NHS England as it underpins effective information sharing within our organisation and externally to patients and suppliers. The law requires certain records to be kept for a defined retention period; however records are used on a daily basis for internal purposes to help make decisions, provide evidence, etc. Using the diagram below, you can learn more about each of the 5 steps in the Records Life Cycle.



- Stage 1: Creation and Receipt
  This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source and it is complete and accurate.

- Stage 2: Distribution
  Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used.
- Stage 3: Use
  This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other NHS England operations. It is also considered the Active Phase.
- Stage 4: Maintenance
  Maintenance is when records are not used on a day to day basis and are stored in the Records Management system. Even though they are not used on a day to day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a Records Management system; the information should be copied and tracked to ensure no amendments were made.
- Stage 5: Disposition
  Disposition is when a record is less frequently accessed, has no more value to NHS England or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to NHS England will be retained for 20 years and sent to the National Archives, where they will be kept for the future of the organisation and may never be destroyed. This is the final phase of a records lifecycle. . If you are unsure whether your records have historical value, please get in touch with the Corporate Records Management Team.

5.7 Record Retention Schedule

5.7.1 Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the Data Protection Act 1998 (DPA) and/or the Freedom of Information Act 2000. Moreover, compliance with these acts means that, for example, personal data must not be kept longer than is necessary for the purposes for which it was collected (Principle 5 of the DPA).

5.7.2 Records should only be destroyed in accordance with the NHS England Corporate Records Retention and Disposal Schedule. It can be a personal criminal offence to destroy requested information under either the Data Protection Act (Section 61) or the Freedom of Information Act (Section 77). Therefore, NHS England needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures.

5.7.3 The Code of Practice on Records Management, issued under Section 46 of the Freedom of Information Act 2000, requires that records disposal 'is undertaken in accordance with clearly established policies that have been formally adopted'. The NHS England Corporate Records Retention and Disposal Schedule is a key component of NHS England's information compliance and allows it to standardise its approach to retention and disposal.

5.7.4 The recommended retention periods shown on the NHS England Corporate Records Retention and Disposal Schedule apply to the official or master copy of the records. Any duplicates or local copies made for working purposes should be kept for as short a period of time as possible. Duplication should be avoided unless absolutely necessary. It should be clear who is responsible for retaining the master version of a record and copies should be clearly marked as such to avoid confusion.

5.7.5 Some types of records which may be created and kept locally are the responsibility of the local department, but may be found under a different function on the retention schedule: for example where recruitment is carried out by departments, the department shall be responsible for ensuring the disposal of the records relating to unsuccessful candidate, this type of record is listed under Human Resources in the retention schedule.

5.8 Records involved in Investigations, Inquiries, Litigation and Legal Holds

5.8.1 A Legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation or inquiry. Organisations have a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated. Staff must immediately notify the Records Manager if they have been notified of a Litigation, Investigation or Inquiry or have reasonable foresight of a future Litigation, Investigation or Inquiry as this could result in records being held beyond their identified retention period.

5.8.2 The Corporate Records Manager will use this information and log details of the records which have been placed on hold.

5.8.3 The Legal Hold decision will be determined by Senior Management.

5.8.4 When a Legal Hold is terminated, Records previously covered by the Legal Hold should be retained in accordance with the applicable retention period under this policy without regard to the Legal Hold, and retained Non-Records or Records not previously subject to retention may be destroyed.

5.9 Record Naming and Good Practice

5.9.1 Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of NHS England to aid in the management of records.

5.9.2 Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

5.9.3 The NHS England standard naming convention, see Appendix C, must be used for the filename of all electronic documents created by NHS England staff members from the implementation date of this policy.

5.9.4 The re-naming of old documents is optional but new documents must follow the standard naming convention.

5.9.5 Version Control is the management of multiple revisions to the same document. Version control enables us to tell one version of a document from another. For more guidance on this, refer to Appendix C of this Policy.

5.9.6 Where records contain person identifiable data or corporate sensitive information it is a legal requirement that such data is stored securely. You must ensure that you adopt one of two approaches:

- Store the data within the Secure drive (S:drive) and have the correct protective marker applied. Please see Appendix D
- Contact the ATOS Service Desk on openservice@atos.net and ask for the folder containing the data to be password protected and access only allowed for specific, named personnel

5.9.7 Documents must be held within the SharePoint Office 365 platform, in Team Working Areas. This ensures that documents are easily accessible even in the document owner's absence. Corporate records must then be transferred to the Electronic Records Management System (ERMS), which is available here:

https://nhsengland.sharepoint.com/sites/records/default.aspx

The ERMS home page provides guidance on how to declare a record on the system but more advice and guidance can be sought from the Corporate Records Management Team.

5.9.8 Good record keeping should prevent record duplication. Staff members should ensure team members have not previously created a record prior to initiating a new document.

5.9.9 Good record keeping requires information to be recorded at the same time an event has occurred, or as soon as possible afterwards.

5.9.10 Staff members should ensure their handwriting is legible when making entries on paper records.

5.9.11 Staff members should ensure records are relevant including their opinions about individuals, as the individual has the right gain access to their records via a Subject Access Request under the Data Protection Act 1998.

5.9.12 Be aware when redacting Microsoft Word documents electronically by using the black highlight text tool as this process is reversible. A Microsoft Word file converted into PDF can be easily read merely by copying if from PDF back into Word. Best methods of redaction include cover up tape, specific blacking pen or scalpel.

5.10 Record Maintenance

5.10.1 Electronic documents and records should be maintained in accordance with this Document and Records Management Policy and the overarching Information Management Strategy and Delivery Plan.

5.10.2 At the present time there is no national external data storage organisation for paper records. To keep costs low, and in accordance with our aim to move to become a largely paperless organisation by 2020, NHS England staff are encouraged to save in electronic format wherever applicable. Records which need to remain in paper format are often 'Sealed' contract records which are usually identified by an embossed stamp and are executive level.

5.10.3 The movement and location of paper records should be controlled to ensure that a record can be easily retrieved at any time. This will enable the original record to be traced and located if required and must be held in a shared location.

5.10.4 Paper file storage must also be safe from unauthorised access and meet fire regulations.

5.10.5 Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of NHS England.

5.10.6 Records held in electronic format within the ERMS have regular back-up copies scheduled and undertaken on a daily basis via the Corporate ICT Team.

5.11 Record Access

5.11.1 There are a range of statutory provisions that give individuals the right of access to information created or held by NHS England such as a data subject access request, Freedom of Information request and correspondence on how a decision was made. The Data Protection Act 1998 allows individuals to find out what personal data is held about them. The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities.

5.12 Record Disclosure

5.12.1 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.

5.12.2 Only certain staff members have the authority, which is dictated by their role, to disclose records. Staff members with this authority should make a record of any copies of records they have disclosed, and to whom.

5.13 Record Closure

5.13.1 Records should be closed, for example, made inactive and transferred to secondary storage as soon as they have ceased to be in active use other than for reference purposes, in the case of paper corporate records. Electronic corporate records should be stored in the ERMS and retention applied.

5.13.2 NHS England has a Records Retention and Disposal Schedule, saved within the ERMS, which will help you apply timescales to your records to ensure records are not kept longer than necessary.

5.13.3 If a record is deleted / destroyed once its retention period has been reached, then a Records Disposal Certificate must be completed and saved in order to prove that the record existed, met its retention and was then disposed of. See Appendix F for a copy of the Record Disposal Certificate. Records from August 2016 onwards should be held within the ERMS and this system creates a Record Disposal Certificate automatically when a record is deleted from the system by its owner.

5.14 Record Appraisal

5.14.1 Appraisal refers to the process of determining whether records are worthy of permanent archival preservation, as certain records created by NHS England may be of historical interest to The National Archives.

5.14.2 The purpose of the appraisal process is to ensure the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.

5.14.3 Appraisal should only be undertaken after consultation with NHS England's Corporate Records Manager.

5.14.4 It is the responsibility of the staff member who is leaving their current post or the organisation, and their Line Manager, to identify as part of the exit procedure specific records that should be retained in line with NHS England's Record Retention and Disposal Schedule. These records should then be transferred securely to the ERMS and any non-work related records disposed of.

5.15 Record Transfer

5.15.1 Records selected for archival preservation and no longer in regular use by NHS England should be transferred to an archival institution, for example a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities.

5.15.2 Following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, non-active records are required to be transferred no later than 20 years from the creation date of the record, as required by the Public Records Act 1958.

5.15.3 The Corporate Records Manager will identify NHS England's Place of Deposit and assist in the transfer of those records identified.

5.16 Record Disposition

5.16.1 Disposal is the implementation of appraisal and review decisions and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.

5.16.2 Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records consumes time, space and equipment use, therefore disposal will aid efficiency. Staff members must regularly refer to NHS England's Record Retention and Disposal Schedule saved within the ERMS.

5.16.3 Unnecessary retention may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Act 1998. If NHS England continues to hold information which we do not have a need to keep, we would be liable to disclose it upon request. The Data Protection Act 1998 also advises that we should not retain personal data longer than is necessary.

5.16.4 The accounts (mailbox and personal folder) of staff members who have left employment with NHS England will be deleted immediately unless there are extenuating circumstances, for example, an Employment Tribunal claim or litigation case. This will ensure best utilisation of server space, as well as to ensure that records are not held in excess of their retention period. It is the Line Manager's responsibility to notify the ICT Service Desk of accounts that should not be deleted.

5.16.5 Staff members must seek specialist advice from the Information Governance team when considering destruction of the organisation's records through a commercial third party.

5.16.6 Staff members must seek specialist advice from the Corporate Records Manager when considering off-site storage of the organisation's records with a commercial third party.

5.16.7 Short-lived documents such as telephone messages, notes on pads, post-its, e-mail messages, texts, etc do not need to be kept as records. If they are business critical they should be transferred to a more formal document which should be saved as a record and placed within the ERMS.

5.17 Scanning

5.17.1 For reasons such as business efficiency and/or to address problems with storage space, staff may consider the option of scanning paper records into electronic format. Large scale scanning can be a very expensive option and should only be undertaken after approval of a Business Case by their National Director. Further scanning guidance can be found on the Records Management page of the intranet here:

https://nhsengland.sharepoint.com/sites/records/default.aspx

5.17.2 Staff members involved in a process to scan paper records into electronic format with the purpose of discarding the original paper file, should understand the principles of information management encapsulated in Code of Practice BIP0008 to conform to the provisions of the Records Management Code of Practice and/or seek advice from the Corporate Records Manager.

5.17.3 By virtue of the Freedom of Information Act 2000, NHS England is required to conform with the Code of Practice 'BIP 0008-1:2008: Evidential weight and legal admissibility of information stored electronically.

5.18 Records Security: Work Base, Home Working, Agile Working

5.18.1 All person identifiable data or commercially sensitive data must be saved with appropriate security measures. Staff should contact openservice@atos.net to request a secure folder.

5.18.2 Staff must not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of NHS England.

5.18.3 Removable Media must be NHS England owned and encrypted by Corporate ICT services. Ideally, person sensitive data should not be stored on any removable media, however if there is no other option ensure this data is stored on a corporate encrypted device and deleted once transferred to identified secure area folder.

5.18.4 When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

5.18.5 NHS England has a Safe Haven procedure in order to ensure that staff are aware how to receive personal information in a secure manner at a protected point.

5.18.6 In non-clinical areas, each department should have at least one designated safe haven contact point. Ideally, all information transmitted to the organisation should pass to these contact points. Clinical environments should operate in accordance with safe haven principles and the organisation should operate safe haven procedures for all flows of person identifiable information.

5.18.7 When transferring data, ensure security measures and precautions have been actioned by the sender and receiver. A robust contract or Service Level Agreement should be in place detailing responsibilities if the information is being transferred to a third party. Please contact the Information Governance team for more advice.

5.18.8 Never leave your computer screen open when unattended. Always lock it using the keys Control + Alt + Delete and then click on 'Lock This Computer'.

5.18.9 For further guidance on Agile working please refer to the Agile Working Policy.

6 Distribution and Implementation

6.1 Distribution Plan

6.1.1 This document will be made available to all Staff via the NHS England intranet site and made available at induction.

6.1.2 A global notice will be sent to all Staff notifying them of the release of this document.

6.1.3 A link to this document will be provided from the Information Governance, Records Management intranet site.

6.2 Training Plan

6.2.1 The Records Management training course is a recommended aspect of the Information Governance training programme for all staff.

6.2.2 The Records Management training course is a mandatory aspect of the Information Governance training programme for all Records Management Coordinators.

6.2.3 Information Governance Training guidance is provided on the staff intranet at the following location:

https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Pages/Information-Governance-Training.aspx

7 Equality Impact Assessment

7.1 Equality and diversity are at the heart of NHS England's values. Throughout the development of the policies and processes cited in this document, we have given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who share a relevant protected characteristic (as cited in under the Equality Act 2010) and those who do not share it.

7.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

8 Monitoring Compliance with the Policy

8.1 Compliance with the policies and procedures laid down in this document will be monitored via the Records Manager team together with independent reviews by both Internal and External Audit on a periodic basis.

8.2 The Corporate Records Manager, in conjunction with the Head of Corporate Information Governance is responsible for the monitoring, revision and updating of this document.

9 Associated Documentation

9.1 The following documents will provide additional information:

Publication Date	Title	Version
April 2013	Freedom of Information Policy	1.0
June 2016	Information Governance Policy	3.0
June 2016	Confidentiality Policy	3.0
June 2014	Data Protection Policy	2.0
June 2016	Information Security Policy	3.0
June 2016	Information management strategy and delivery plan 2015-17	V1.1
TBC	Acceptable Use of ICT and User Obligations Guidance	Unable to find this on the Intranet! Version 1.1 from Sept 2015 seems to have gone.
Various dates	Records Management Procedures and Guidance – available on the intranet at: https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Pages/RecordsManagement.aspx	NA
July 2016	Records Management: Code of Practice on Health and Social Care 2016 issued by the Information Governance Alliance	v1.0

	https://digital.nhs.uk/information-governance	

Appendix A: Records Management Co-ordinator roles and responsibilities

NHS England has already identified RMCs at a local level, who work with NHS England’s records management team and senior managers within their teams to appraise their records and meet the operational needs and legal and regulatory requirements of the organisation
Responsible for promoting document and records management (DRM) policies, procedures and best practice to team members
Liaison with line/team managers to ensure new starters are aware of DRM policies, procedures and best practice within 10 working days of joining the section. Referring them to Records Manager if required
Referring to their line/team manager or the records management team, any problems which they cannot resolve e.g. appropriate retention periods
Communicating changes in DRM policies and procedures to other members of their team/business area
Reviewing and quality assuring (from a business perspective) DRM policies, processes, procedures and guidance
Ensuring continuity of the RMC role, in conjunction with the team manager
First point of contact for uploading records to the ERMS at team level by liaising with the requester / record owner
Liaise with information asset owner / administrator i.e. the person who has requested the upload when records come up for review and disposal

Appendix B: Records Management Glossary of Abbreviations and Acronyms

Please check the Records Management section of the intranet at https://nhsengland.sharepoint.com/TeamCentre/TCO/infogov/Pages/RecordsManagement.aspx
for the latest copy of this acronym list.

AOB	Agreement of Balances
AQP	Any Qualified Provider
BPPC	Better Payment Practice Code
CAMHS	Child and Adolescent Mental Health Service
C&B	Choose and Book
CEO	Chief Executive Office
CCG	Clinical Commissioning Group
CCG Council	Clinical Commissioning Group Council
CiC MH	Care in the Community Mental Health
Comms & Engagement	Communications & Engagement
DOLS	Deprivation of Liberty Safeguards
FOI	Freedom of Information
FIMS	Finance Information Monitoring Systems
FMR	Finance Monitoring Report
FSD	Finance Skills Development
GP	General Practice/Practitioner
GPCEC	GP Commissioning Executive Committee
HC Contracting	HealthCare Contracting
HR-Workforce	Human Resources-Workforce
ICT	Information Communication Technology
IFR-PA	Individual Funding Requests - Prior Approval
IG	Information Governance
IRC	Immigration Removal Centre
ISFE	Integrated Single Finance Environment
JSNA	Joint Strategic Needs Assessment
KPI	Key Performance Indicator
LD Cont Care	Learning Disabilities Continuing Care
PFT	Partnership Foundations Trust
SCB	Safeguarding Children's Board

LTC	Long Term Conditions
SCG	Specialist Commissioning Group
MH	Mental Health
MOGP	Markers of Good Practice
NCA	Non Contract Activity
Non HC Contracting	Non Health Care Contracting
OHPs	Overhead Presentations
PBC	Practice Based Commissioning
PFI	Private Finance Initiative
PH	Public Health
Pract Perform & Development	Practitioner, Performance & Development
Prim Care Contracts	Primary Care Contracts
SAAF	Self-Assessment Assurance Framework
SCR	Serious Case Review
SHA -DH	Strategic Health Authority-Department of Health
Sec Care Contracts	Secondary Care Contracts
SSG	Safeguarding Steering group
TCS	Transforming Community Services
WCC	World Class Commissioning
WPs	Working Papers

Appendix C: NHS England Electronic Document Naming Convention

All electronic documents and records should be named according to the following format;

Date (in format YYYYMMDD)_File Title / Description_ Version (in format v1.0, v1.1 etc…)
For example: 20170210_Board minutes_v2.0

Elements of the file title

In constructing a title it is necessary to decide how best to describe the informational content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title.

Common elements of a title:

- Date
- Subject
- Version number

Date

The date element is essential as this will allow retention to be applied to the document or record. Using the format YYYYMMDD means that electronic files will be stored in date order.

Dates should be included to understand the content of the document e.g. minutes of meetings. (20131013_Programme_Board_Minutes_v1.0)

Subject

Where possible give your files meaningful names. This assists both yourself and other members of staff in managing and retrieving files. Always make the name of a folder or record descriptive of its content or purpose.

- Enter the subject term. This may be from a controlled acronym glossary or else use natural language
- Do not name the file after the person whose work it contains
- Do not use terms such as ‘general’ or ‘miscellaneous’
- Always ensure the title is: specific, consistent, sensible, understandable and helpful to others

Version Number

In order to effectively control different versions of a document it is necessary to have documented procedures. Consistent naming of different versions can be used to support version control and is useful for documents which have a number of contributors which are in various stages of development before the final version is complete. Use whole numbers (e.g. v1.0, v2.0, v3.0 etc…) to indicate finalised versions; use v0.1, v1.1, v1.2 etc…to indicate that the version is a draft and not finalised yet.

Length of a title

Keep file paths on Microsoft packages under 255 characters (216 for Sharepoint) or the information may become scrambled. Titles should contain enough information in order to properly describe the contents of the document or folder. However, keeping titles a reasonable length, but under 255, (216 for Sharepoint) will help users quickly identify and retrieve accurate information.

Redundant terms

The use of redundant terms should be avoided in order to keep titles as brief as possible.

Do not use conjunctions such as ‘and’, ‘on’, ‘of’ unless they add meaning to the description e.g. Freedom_of_Information or FOI

Author

Do not use the document creator’s name in the title unless this information genuinely adds to a description of the content. This information can be added directly in the document or accessed in the document or folders Properties.

- Do not use – ‘Jan Gavin’s meeting papers’
- Only use if acronym is added to glossary - ‘RM Meeting Papers’
- If file path characters allows use - ‘Records_Manager_Meeting_Papers

Acronyms & Abbreviations

Due to the 255 characters rule abbreviations and acronyms may need to be used. Do not use obscure abbreviations or acronyms as they often become obsolete over a period of time and can often have more than one meaning. If you use a new acronym contact the Records Management Team to ensure it is added to the glossary of acronyms.

Emails

All the advice and guidance that apply to documents and folders also apply equally to naming emails, but there are other things that should be considered. Email titles must accurately describe their content.

- You must change the title of the email if it does not accurately reflect the content (right click then rename)
- You do not need to include ‘email’ as part of the title, as the Object type icon shows it is an email.
- Save all emails with their attachments
- Save all emails as Outlook Email Format (File, Save as)

Appendix D: Protective Marking Scheme

Classification of NHS Information - Marking Guidance for NHS England

ALL information NHS England collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works within NHS England (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any NHS England information or data that they access, irrespective of whether it is marked or not.

New Government Security Classifications (published April 2014) have been implemented to assist you in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The new levels are;

OFFICIAL
Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. NHS England will operate exclusively at this level including the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

SECRET
Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat actors and highly serious organised crime groups.

TOP SECRET
Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

There is no need to apply the new classification procedure retrospectively.

This simplified procedure will make it easier and more efficient for information to be handled and protected. The new procedure places greater emphasis on individuals taking personal responsibility for data they handle.
All information used by NHS England is by definition ‘OFFICIAL.’ It is highly unlikely NHS England will work with ‘SECRET’ or ‘TOP SECRET’ information.
Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.
2. A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL

classification tier, but should have additional measures applied in the form of OFFICIAL-SENSITIVE.

3. This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
4. In additional to the marking of OFFICIAL-SENSITIVE further detail is required regarding the content of the document or record, i.e.:

> OFFICIAL – SENSITIVE: COMMERCIAL
>
> Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to NHS England or a commercial partner if improperly accessed.
>
> Or
>
> OFFICIAL – SENSITIVE: PERSONAL
>
> Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Such documents/records should be marked with the caveat 'OFFICIAL-SENSITIVE: COMMERICAL or SENSITIVE' in capitals at the top and bottom of the page.
In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

NHS Confidential

NHS England has adopted the new government classification scheme for corporate information as it is an expectation from the DH for all Arms Length bodies (ALBs) to comply with. Our approach will satisfy any corporate communications with DH, other departments and ALBs. In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

How to handle and store OFFICIAL information;

EVERYONE is responsible to handle OFFICIAL information with care by:

- Applying clear desk policy
- Information sharing with the right people
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

How to handle and store OFFICIAL – SENSITIVE information;

All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, OFFICIAL-SENSITIVE:

PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules
- Always question whether your information may need stronger protection
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains, etc
- Only print sensitive information when absolutely necessary
- Send sensitive information by the secure email route or use encrypted data transfers
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control
- Store information securely when not in use and use a locked cabinet/drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details
- Do not send to internet email addresses e.g. Gmail, Hotmail, etc.
- Only in exceptional cases, where a business need if identified, should sensitive information be emailed over the internet, in an encrypted format, to the third parties. Contact the Corporate IG team for further advice
- The use of pin code for secure printing is both widely available and preferable way to manage the printing process

Table 1 – Descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL

Category	Definition	Marking
Appointments	Concerning actual or potential appointments not yet announced	OFFICIAL-SENSITIVE: COMMERCIAL
Barred	Where • there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or • disclosure would constitute a contempt of Court (information the subject of a court order)	OFFICIAL-SENSITIVE: COMMERCIAL
Board	Documents for consideration by an organisation's Board of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way	OFFICIAL-SENSITIVE: COMMERCIAL

Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL-SENSITIVE: COMMERCIAL
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date	OFFICIAL-SENSITIVE: COMMERCIAL
Management	Concerning policy and planning affecting the interests of groups of staff (Note: Likely to be exempt only in respect of some health and safety issues)	OFFICIAL-SENSITIVE: COMMERCIAL
Patient Information	Concerning identifiable information about patients	OFFICIAL-SENSITIVE: PERSONAL
Personal	Concerning matters personal to the sender and/or recipient	OFFICIAL-SENSITIVE: PERSONAL
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published)	OFFICIAL-SENSITIVE: COMMERCIAL
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff	Concerning identifiable information about staff	OFFICIAL-SENSITIVE: PERSONAL

Appendix E: Glossary of Terms

Term of Abbreviation	What it stands for
Assembly	A collection of records. May be a hybrid assembly meaning where electronic and paper records are contained in one folder.
Class	Class is a subdivision of an electronic classification scheme by which the electronic file plan is organised e.g. subject area. A class may either be sub-divided into one or more lower level classes. A class does not contain records. See folder.
Classification	A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.
Data Quality	Data Quality refers to the procedures and processes in place to ensure that data is accurate, up-to-date, free from duplication (for example, where two or more different records exist for the same individual), and free from confusion (where different parts of a individuals records are held in different places, and possibly in different formats).
Declaration	Declaration is the point at which the document (i.e. record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.
Disposition	Manner in which a record is disposed of after a period of time. It is the final stage of record management in which a record is either destroyed or permanently retained.
Document	The International Standards Organisation (ISO) standard 5127/1 states “Recorded information which can be treated as a unit in a documentation process regardless of its physical form and characteristics.”
Electronic Document	Information recorded in a manner that requires a computer or other electronic device to display, interpret, and process it. This includes documents (whether text, graphics, or spreadsheets) generated by a software and stored on magnetic media (disks) or optical media (CDs, DVDs), as well as electronic mail and documents transmitted in electronic data interchange (EDI). An electronic document can contain information as hypertext connected by hyperlinks.

Electronic record	An electronic record is an electronic document which has been formally declared as a corporate record. A typical electronic record consists of both electronic content (one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.
Electronic Records Management System	A system which is designed for the storage and retrieval of Corporate Records.
End Users	This group comprises those, at all levels of the organisation, who generate and use records in their daily activities. The end user group is the source of much of the material which constitutes the record. Since records systems tend to devolve control to end users at the time of record capture, sound advice and guidance to this group is critical for the maintenance of quality and accountability.
File plan	The full set of classes, folders and records together make up a file plan. It is a full representation of an organisation, designed to support the conduct of the business, and meet records management needs.
Folder	A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable). Folders are allocated to a class.
Information Asset Owner (IAO)	Is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance requirement that all Information Assets are identified and that the business importance of those assets is established.
Information Asset Administrator (IAA)	Is usually an operational manager who is familiar with information risks in their business area. Their primary role is to support the IAO to fulfil their responsibilities and ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.
Information Lifecycle Management	Information Lifecycle Management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction. Record management policies and procedures form part of the Information Lifecycle Management, together with other processes, such as for example, a records

	inventory, secure storage, records audit etc.
Metadata	Metadata can be defined as data about data. Metadata is structured, encoded data that describes characteristics of a document or record to aid in the identification, discovery, assessment and management of documents and records. Examples of metadata: title, dates created, author, format, etc.
Naming Convention	A naming convention is a collection of rules which are used to specify the name of a document, record or folder.
Place of Deposit	A Place of Deposit is a record office which has been approved by the National Archives for the deposit of public records in accordance with the Public Records Act 1958.
Protective marking	Protective marking is a metadata field applied to an object to show the level of security assigned to the object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the file plan hierarchy.
Record	A record in the records management terminology may not be the same as a record in database terminology. A record for the purposes of this document is used to denote a “record of activity” just as a health record is the record of activity of a patients NHS contact. A record may be any document, email, web page, database extract or collection of these which form a record of activity. A record of activity for a database extract may therefore include a collection of health records. A formal definition is “information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business.” (BS ISO 15489.1 Information and Documentation. Records Management
Safe Haven	Safe Haven is the term used to explain an agreed set of arrangements that are in place in an organisation to ensure person identifiable, confidential and/or sensitive information can be received, stored and communicated safely and securely.

Appendix F: Record Disposal Certificate

NHS England

Record Disposal Certificate

Disposal of Records				
Section:	**Name:**		**Date:**	
Title of Record (list all):				
Format (electronic/ paper):				
Reason for disposal:				
Legal hold not placed upon these records:	None			
Method of disposal: (tick relevant box)	Destruction		Transferred to archive	
If destroyed, method of destruction:				
Date of disposal:				
Authority:				
Not subject to current information request: (tick once checked)				

Please complete the form and retain a copy. Send a copy to england.ig-corporate@nhs.net

Version Control Tracker

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
1.0	Apr 2013	Information Governance Senior Manager	Approved	New policy
2.0	Feb 2014	Records Manager	Approved	A review of current policy
3.0	June 2014	Records Manager	Approved	Updated appendix D highlighting the changes to reflect the new Government Classification Scheme since April 2014
4.0	May 2017	Records Manager	Draft	Updated to remove reference to sub regions and area teams. Section 1.5 updated to include audio recordings Updated Section 2.1f to note that the Codes of Practice are under review. Section 2.1 updated to include GDPR Section 3.1 updated to include Sustainability and Transformation Partnerships Updated Section 5.8.1 to include inquiry records, in the light of inquiries such as Goddard. Updated Section 5.9.7 to refer to ERMS for storing electronic records and the guidance available on the home page with regards to declaring records,~~.~~ Updated Section 5.10.1 to reflect links to Information Management Strategy Plan and dates of the plan removed Updated Section 5.10.2 to refer to the date that paperless NHS is aiming to – i.e. 2020. Updated Section 5.10.06 to refer to the forthcoming ERMS for NHS England. Updated Section 5.13.1 to refer to

Version Number	Date	Author Title	Status	Comment/Reason for Issue/Approving Body
				the forthcoming ERMS Section 5.13.3 added in to reflect the need to have a Records Disposal Certificate for deletion. Section 9.1 on associated documentation has been updated and a new table included. Updated amendments to sections with regards to Safe Haven and S Drive. Appendix A amended to reflect new RMC roles and responsibilities in relation to ERMS. Appendix B amended to show the link to the Records Management intranet page. Plus various smaller highlights in red. Appendix F Record Disposal Certificate added.

First published April 2013
Published to NHS England, in electronic format only.