



Information Management

Policy V0.7

Document revision history

Date	Version	Revision	Comment	Author
21/08/2018	V0.1	Draft GDPR compliant document created		Head of IG, NEL
15/09/2018	V0.2	Review		Head of FOI and IG Compliance
27/09/2018	V0.3	Review		SME Manager
18/10/2018	V0.4	Review		Compliance Manager
15/11/2018	V0.5	Review		Merton CCG
08/12/18	V.06	Review		IGSG Meeting/Merton CCG

Document approval

Date	Version	Revision	Comment	Approver
31.12.18	V.07	FINAL	Information Governance Steering group Meeting	Caldicott Guardian/Senior Information Risk Owner Merton & Wandsworth CCG.

Contents

.....	1
1.0 Introduction.....	5
2.0 Scope.....	7
3.0 Definitions	8
4.0 Responsibilities	8
5.0 Information Management	8
Principle 1.....	8
Principle 2.....	8
Principle 3.....	8
Principle 4.....	9
6.0 Objectives.....	9
7.0 Legislative and Regulatory Environment	9
Legislation.....	9
Best Practice Standards.....	10
8.0 Information Asset Register	10
9.0 Electronic Filing Structure.....	11
10.0 Paper Filing Structure.....	11
11.0 Record Disposal and archiving	11
12.0 Monitoring and Compliance	12
13.0 Equality Analysis.....	14
14.0 Review	14
Appendix A: Definitions.....	15
Appendix B: Classification Marking of NHS Information.....	18
Appendix C: Applying a Classification.....	23

1.0 Introduction

This policy sets out the intentions of Merton & Wandsworth CCGs (hereafter referred to as the CCGS) to manage all the information within its remit to the standards required by law and regulations. In doing so, it supports high quality commissioning and healthcare through accurate, accessible and appropriately governed information. The CCGS have put this policy in place to ensure members of staff are fully aware of their information management responsibilities.

This document uses definitions provided by the Cabinet Office. The Cabinet Office defines data as *'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation'* and information as *'output of some process that summarises interprets or otherwise represents data to convey meaning'*. All reference to information in this document encompasses information and data. This includes information which is personal, financial or falls within any other category.

Information is a corporate asset and as such, is an important source of administrative, financial, legal, evidential, and historical information, it is vital to the organisation's future operations, for the purposes of accountability and for an awareness and understanding of its history. Information is the corporate memory of the organisation.

Information supports the formulation of policy, managerial decision-making, protects the interests of the organisation and the rights of patients, staff, and members of the public. Information supports consistency, continuity, efficiency and productivity and helps deliver services in reliable and equitable ways. It is important to ensure information and records are:

- Available when needed so that events or activities can be followed through and reconstructed as necessary;
- Accessible, located and displayed in a way consistent with their initial use, with the original or current version being identified where multiple versions exist;
- Able to be interpreted and set in context: who created or added to the record and when, during which business process, and how the record is related to other records;

-
- Trustworthy and hold integrity, reliably recording the information that was used in, or created by, the business process;
 - Maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy;
 - Secure from unauthorised or inadvertent alteration or erasure, with access and disclosure being properly controlled with audit trails tracking use and changes;
 - Held in a robust format which remains readable for as long as the information is required;
 - Retained and disposed of appropriately using documented retention and disposal procedures, which include provision for retrieving and permanently preserving records with particular archival value.

The CCGs are committed to ensuring that information, in whatever its context, is processed as determined by prevailing law and best practice. Compliance with all organisational policies is a condition of employment. A breach of policy may result in disciplinary action.

NEL, the information governance service provider is hosted by NHS England. All policies and associated documentation of the organisation are aligned to those of NHS England.

This policy outlines the legal, regulatory and best practice information framework that the CCGs work to and the methods used to deliver and maintain this policy. This policy and commitment extends to the services the CCGs are commissioned to provide, ensuring the appropriate use and control of information to deliver high quality healthcare to support patients and the organisation.

Where the CCGs create an official “record”, it is expected that staff follow: The Records Management: NHS Code of Practice published by the Department of Health, which is 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. The Code of Practice is based on current legal requirements and professional best practice.

The Records Management Code of Practice states that *‘information and records are the corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations’*. Consequently, it requires all NHS bodies to adopt a systematic and planned approach to the management of information and the determination of where a record has been created, from the moment the need for information is identified to when a record is created, through the information life cycle (creation to destruction).

The CCGs recognise that effective information management is fundamental to good administration and operational effectiveness and is an enabler to the achievement of its strategic objectives.

This policy is part of the suite related to information governance which set out the expected standards and controls around its use. They are: Information Governance, Information Quality, Information Management and Information Security. The overarching document which sets out the approach to Information Governance is the Information Governance Framework. The concepts and standards throughout the suite of policies are interrelated. It is important to consider all of the obligations and intentions across the suite of policies.

2.0 Scope

This policy applies to all information (paper, electronic or in other formats) that is received, created, or held in the course of the business by its employees. It must be adhered to by all permanent, contract, interim and temporary staff and any organisation or body acting as agents or on behalf of the CCGs.

The CCGs are committed to ongoing improvement of its information management systems as it believes that it will gain a number of organisational benefits from doing so. These include:

- Using cloud-based technologies to make better use of, and reduce the need for physical server space;
- Provide a paperless and clear desk environment (see the policy statement below), where paper records are held by exception, out of sight and locked away when not in use, with a justification for holding hard copies of documents;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards;
- Reduced costs.

The CCGs believe that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of information management as a designated corporate function.

3.0 Definitions

A list of key information management definitions is contained in Annex A.

4.0 Responsibilities

Information Governance responsibilities are outlined within the Accountability and Governance Structure section within the Information Governance Framework.

5.0 Information Management

The CCGs utilise four main principles in the management of information:

Principle 1

The CCGs will create, capture, use, manage, store and destroy or preserve its records in accordance with all statutory, business and historical requirements. It will ensure that the appropriate technical, organisational and human resource elements exist to make this possible. The primary location for the information will be the Blue Network.

Principle 2

Information will be created once, stored in one place and will be accessible in a timely fashion to those who need to use the information across the organisation and externally to stakeholders. This will take into account the need for effective security and appropriate confidentiality.

Principle 3

Information management will be embedded within operational procedures and activities. All staff that create, use, manage or dispose of information have a duty to protect the information and ensure that any information that they add is accurate, complete and necessary. This includes identifying where an official record is created, as defined in Annex A.

Principle 4

The risk to effective information management will be assessed corporately and managed appropriately at strategic and operational levels. Compliance with this policy and associated procedures will be subject to a programme of audit and assurance.

6.0 Objectives

The key objectives of this policy and supporting guidance are to:

- Facilitate and effectively record all the operations, business and policy decisions;
- Model best practice in information management and record-keeping, including operating a Clear Desk Policy (see below);
- Demonstrate compliance with relevant legislation;
- Raise the minimum standard of records management practice in the CCGS to the specified standard in the Data Security and Protection toolkit;
- Ensure that records are protected, complete, accessed and managed in line with information classification and handling arrangements;
- Ensure official records of historical and evidential significance are identified and held securely;
- Define clear responsibilities for managers and staff (as listed above).

7.0 Legislative and Regulatory Environment

All NHS official records are Public Records under the Public Records Act 1958. The CCGS will take actions as necessary to comply with all legal and professional obligations in particular those contained in:

Legislation

- The Public Records Act 1958;
- Data Protection Act (2018);
- The common law duty of confidentiality;

- Human Rights Act 1998;
- Freedom of Information Act 2000;
- The Protections of Freedoms Act 2012;
- The Re-use of Public Sector Information Regulations;
- General Data Protection Regulations 2018;
- Environmental Information Regulations 2004;
- NHS Act 2006;
- Health and Social Care Act 2012;
- Care Act 2014.

Best Practice Standards

- ISO 15489 - Records Management Standard;
- ISO 27001 – Information Security Standard;
- Department of Health Records Management NHS Code of Practice;
- Department of Health Records Management Roadmap;
- Confidentiality NHS Code of Practice;
- Information Security NHS Code of Practice;
- Lord Chancellor's Code of Practice on the Management of Records Issued under (s.46) of the Freedom of Information Act;
- The National Archive: Essential Records Management;
- NHS Information Governance Toolkit Standards.

8.0 Information Asset Register

The CCGS will establish an inventory of information. The inventory of information will facilitate:

- The classification of information into series; and
- The identification of information asset owners and administrators.

All records created by the CCGS will follow national guidance on protective marking; see Annex B - Classification Marking of NHS Information.

9.0 Electronic Filing Structure

Electronic information held by the CCGS will be maintained in on the Blue Network which follows the principles of functions, activities and transactions of the CCGS and matches the organisational structure. Some teams within the CCGS further operate within the Blue Network which maintains the same file structure.

The Blue Network has permissions to enable cross directorate working. The responsible owner of each team site is the Accountable Partner responsible for the service. Team managers will have responsibility for the management of their team information.

Authorisation for access to each team folder will be managed within each team, with assistance from ICT where required.

The name applied to any file must reflect the file content in terms of the CCGS function, activity or transaction it applies to, but must **not** replicate any tags already applied in the name of the file, i.e. date, name/initials of the author, version number or the tags you are prompted to add before it is uploaded.

10.0 Paper Filing Structure

By exception, where paper information is held, with a justification for holding hard copies of documents; records held by the CCGS will be maintained in a file structure which follows the principles of functions, activities and transactions of the CCGS. This will match the organisational and the electronic file structure which staff in the department can easily navigate to locate files quickly.

11.0 Record Disposal and archiving

Disposal is defined as *'the decision on the management intent for a record once it is no longer required for the conduct of current business'*.

It is a fundamental requirement that all the official records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the business functions.

The CCGS will adhere to the retention schedules aligned to the Records Management: NHS Code of Practice.

Disposal schedules will be the subject of regular review to identify any exceptions the CCGS wishes to make to the national standard retention periods, subject to justification and approval by the Information Governance Group and ratification by the Integrated Governance Committee.

Archiving is defined as *'paper or electronic records, when they are no longer required to be retained either as active or semi active records within normal working locations, but are not allowed to be destroyed'*.

The CCGS will ensure it has an appropriate and secure location for the storage of records that have an adequate process for retrieval.

The decision to archive an official record must meet the above definition and be approved by the Information Asset Owner of the service requesting to archive records.

Archiving of records may only occur on an annual basis for each service.

The process for archiving is available in the creation, storage, transportation and disposal of records procedure.

12.0 Monitoring and Compliance

This policy and the associated controls will be monitored through the risk management system for the CCGS. The risk register will be reviewed on a monthly basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Control Audit and Monitoring Table

<p>Monitoring requirements:</p> <p>What in this document is monitored?</p>	<p>The management of information risks</p> <p>Compliance with the law</p> <p>Compliance with the Data Security and Protection Toolkit</p>
--	---

	<p>Incidents related to the breach of this policy</p>
<p>Monitoring Method</p>	<p>Information risks will be monitored through the risk register management system.</p> <p>Compliance with law will be monitored through audit, work directed by the Data Security and Protection Toolkit and as directed by information risk management Policy.</p> <p>The Data Security and Protection Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the toolkit will be audited by the organisation's internal audit function before the annual submission.</p> <p>Incident reporting and management requirements.</p>
<p>Monitoring prepared by</p>	<p>Information governance function and Information Governance Group.</p> <p>Incident reports will be produced by the nominated investigation officer.</p>
<p>Monitoring presented to</p>	<p>Information Governance Group.</p> <p>Senior Information Risk Owner (SIRO).</p> <p>Caldicott Guardian (CG).</p>
<p>Frequency of Review</p>	<p>Monthly updates will be provided to the SIRO and the CG</p> <p>Relevant information risks will be added to the corporate risk register and reported in line with the risk management system.</p> <p>Annual (as a minimum) updates to the Internal Assurance Group will be provided, including the internal audit report on DSPT performance.</p>

	Incident reports will be reviewed at every meeting of the Information Governance Group and escalated to the Integrated Governance Committee, as appropriate.
--	--

Further monitoring will be undertaken through the change control process.

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance they are individually responsible for. Failure to maintain these standards can result in criminal proceedings against the individual.

13.0 Equality Analysis

This document demonstrates the organisation's commitment to creating a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership, in addition to offending background, trade union membership or political affiliation.

Merton and Wandsworth CCG acknowledges its obligations to comply with the Human Rights Act 1998 to promote positive practice and value the diversity of all individuals and communities.

14.0 Review

Review will take place every three years or earlier until the policy is rescinded or superseded, due to legal or national policy changes.

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available in the policy register for the CCGS. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Appendix A: Definitions

Records Management - as defined by ISO 15489

‘The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records’.

Record - For the purposes of this policy the definition of a record used by the CCGs are:

Documentary evidence, regardless of form or medium, created, received, maintained and used by the CCGS in pursuance of its legal obligations or in the transaction of business.

This definition draws a distinction between a record and a document – a record is a final version that may be retained, while a document can be changed and will not normally be retained except for audit trail purposes where necessary. The purpose of a record is to preserve information in a form that is trustworthy and, once declared, should not be changed.

Person Confidential Data (PCD):

E.g. patients’ clinical records, patient confidential data, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies. This includes patient demographic details that might identify people who have had a GP contact/hospital appointment within a particular timeframe or who may have a particular condition.

Information Lifecycle

System Design

One of the key elements of Information management throughout the lifecycle of information 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, including a Data Protection Impact Assessment.

Creation

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

At the point of creation, the relevant metadata (breakdown details of the data) needs to be captured to ensure its on-going value and evidential weight.

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 function.

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

The following are key components of use:

- **Retrieval** – information must be accessible throughout its lifecycle for staff with authorised access and in line with access controls;
- **Naming Conventions** – a clear, systematic and consistent standard for naming information is required;
- **Version Control** – a clear, systematic and consistent method of controlling version of information is vital for effective management and efficient working;
- **Storage** - all information must be stored in systematic and consistent to be of use. Storage must also be secure. Further details are provided in the Information Security Policy and the policies and procedures for the relevant systems;
- **Mapped Information Flows** - All flows of personal confidential data (PCD) must be in accordance with legal, regulatory and organisational requirements. Routine flows of information within the organisation and with external bodies will be mapped, ensured as lawful and the risks involved understood.

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.

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 of the CCGS to ensure all records are in one format (e.g. no hybrid paper – electronic records) with appropriate reference to relevant NHS strategies.

Disposal

Disposal is defined as the management intent for a record once it is no longer required for the conduct of current business. Data and information, not classified as a record, may be destroyed once its business value is concluded.

There are a number of stages in the disposal phase of a corporate record, these include:

- **Closure** - records are made inactive and transferred to secondary storage;
- **Retention** - the retention period varies dependent on the type of information being stored;
- **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);
- **Archiving** - upon the end of a retention period, information must be assessed for whether it requires archiving or destroyed.

Any service that takes over legacy records must manage their disposal. Those that find records within their remit or office space must:

- Register the collection with the Information Governance HUB Team and inform the relevant senior manager for their function to ensure the appropriate Information Risk Owner is identified; and
- Ensure that it is managed appropriately.

Appendix B: Classification Marking of NHS

Information

Person-identifiable clinical information should always be held confidentially (*Confidentiality*: NHS Code of Practice). Therefore, the marking NHS CONFIDENTIAL should be used for that kind of information (e.g. patients' clinical records, patient identifiable clinical information, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies). This will include patient demographic details that might identify people who have had a GP contact or hospital appointment within a particular timeframe or who may have a particular condition.

NOTE: In order to safeguard confidentiality, the term "NHS Confidential" should never be used on correspondence to a patient.

The endorsement NHS CONFIDENTIAL should be included at the top centre of every page of the document. Documents so marked should be held securely at all times. That is, they should be stored in a locked room or within secured electronic systems to which only authorised persons have access. They should not be unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed containers and not unattended at any stage. Documents marked NHS CONFIDENTIAL not in a safe store or transport should be kept out of sight of visitors or others not authorised to view them.

Other uses of NHS CONFIDENTIAL:

The endorsement NHS CONFIDENTIAL should also be used to mark all other sensitive information. That is, material the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;

- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information; or
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

A paper, printout or report etc. marked NHS CONFIDENTIAL may also be endorsed with a suitable descriptor indicating the reason for the classification e.g. “NHS CONFIDENTIAL – PATIENT INFORMATION” or “NHS CONFIDENTIAL – COMMERCIAL”.

The endorsement should be included at the top centre on every page of the document. NHS CONFIDENTIAL documents should be stored in lockable cabinets or equivalently secured electronic systems.

Information may be classified NHS CONFIDENTIAL in the light of the circumstances at a particular time. The classification should be kept under review and the information de-classified when the need for this protection no longer applies. NHS use of an equivalent classification for “restricted” is unnecessary when NHS CONFIDENTIAL is used.

NHS PROTECT

Across Government, a new marking of “PROTECT” was recently introduced. This discretionary marking may be used in order to avoid unauthorised access to information. It establishes basic principles to handle with care, take relevant precautions and dispose of properly. In the NHS context, it is possible for NHS organisations to adopt and use an equivalent NHS PROTECT marking with or without descriptors. This is beneficial for information that requires protection below that of NHS CONFIDENTIAL and where care in handling is still necessary. NHS organisations that choose to adopt NHS PROTECT must ensure their staff and business partners are aware of the different expectations and arrangements that apply for the protection and assurance of NHS CONFIDENTIAL and NHS PROTECT marked information.

Freedom of Information

When classifying NHS documents, regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to an inappropriate decision not to disclose information that would later be embarrassing to the organisation. For example, where there was an appeal against non-disclosure or the Information Commissioner became involved. Protective

markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemption, such as that for drafts of documents that are intended for publication.

Further information about the Act and its exemptions (including the application of the “public interest” test) is available on the website of the Information Commissioners Office (<https://ico.org.uk/>).

Principal	<p>Information assets (in any format) will be protectively marked according to the NHS classification. A fundamental of the classification is that protective marking should wherever possible be restricted to information that would be exempt from disclosure under the terms of the Freedom of Information Act 2000.</p> <p>A note of exemptions that are relevant to protective marking is contained in Appendix A.</p>
Creation	<p>Wherever possible, document marking will take place at creation through the use of standard templates. However, where this is not possible, markings can take a number of different forms such as: a stamp, a handwritten annotation or an entry on the container or file cover.</p>
Document Marking	<p>Protective marking classification to be bold and in BLOCK CAPITALS within the footer of a document or record.</p>
Classification	<p>The NHS does not have a requirement for the full range of protective marking used in the Government Protective Marking Scheme (GPMS). Consequently, the CCGS will adopt the two classifications recommended by the NHS information governance programme.</p> <p style="text-align: center;">NHS PROTECT</p> <p style="text-align: center;">NHS CONFIDENTIAL</p>

	<p>The use of UPPERCASE characters is to identify the term is being used in a protective marking context.</p> <p>Any document or record not carrying a protective marking classification will be considered unclassified.</p> <p>Where is it considered appropriate to positively identify and unclassified document the preferred term is NONE.</p> <p>There are two classifications above CONFIDENTIAL in the GPMS -</p> <p style="text-align: center;">SECRET</p> <p style="text-align: center;">TOP SECRET</p> <p>NHS staff are not routinely cleared to handle SECRET or TOP SECRET documents. Any member of staff whom receives material marked with these two classifications should immediately contact the information governance team:</p> <p>NELCSU.information-governance@nhs.net</p>
<p>Unclassified</p> <p style="text-align: center;">NONE</p>	<p>Information which is routinely placed in the public domain or general information which requires no access restrictions.</p>
<p style="text-align: center;">NHS PROTECT</p>	<p>Information which requires controls to be put in place in order to prevent unauthorised access or misuse.</p>
<p style="text-align: center;">NHS CONFIDENTIAL</p>	<p>Information which due to the sensitivity of its content or due to its condition requires to be handled in line with specially devised and tailored secure arrangements.</p>
<p style="text-align: center;">Handling</p>	<p>Detailed handling arrangements for the four protective marking classifications in general use within the NHS are contained in the Annexes to this document.</p>

Review	<p>It is recognised that the classification for records is capable of changing over time and will be the subject of periodic review to ensure that the marking applied remains appropriate.</p> <p>It is further recognised that within filing systems a collection of records may be marked NHS CONFIDENTIAL (e.g. patient records) but the classification may not apply to the entire contents of the container or file cover.</p>
Sensitive Personal Information	<p>Until such time that the CCGs captures the protective marking classification of documents or records at creation any document or records that contains personal or sensitive information, the document should be considered NHS CONFIDENTIAL and be handled and stored appropriately.</p> <p>The CCGs define sensitive information as:</p> <p>Information that must be protected because its unauthorised disclosure, alteration, loss or destruction will cause damage to someone or something.</p> <p>The CCGs define personal information as:</p> <p>Information about an individual whose identity is apparent or can be ascertained from his/her information.</p> <p>It is recognised that the classification for non-clinical records is capable of changing over time and will be the subject of periodic review to ensure that the marking applied remains appropriate.</p>

Appendix C: Applying a Classification

The following tables have been created to provide CCGS staff with a number of questions that they should ask and the appropriate protective marking based upon the response to the question and the assessed risk.

Table 1 – Freedom of Information Act exemptions

NHS CONFIDENTIAL	S40 Personal Information (may be subject to public interest test)
NHS PROTECT	S22 Intended for future publication (including drafts) S30 Investigations and proceedings S31 Law enforcement S38 Endanger health and safety (public interest test) S43 Commercial Interest (public interest test) S44 Legal Prohibitions on disclosure

Table 1 – Risk Assessment of security breach involving a document or records

Question	NHS PROTECT	NHS CONFIDENTIAL
Will it affect any member of the public?	Single person up to 50	Over 50
Will a breach cause embarrassment or distress to a member of the public?	Distress for an individual	Prolonged distress for a number of citizens

Will someone suffer financial loss?	Up to £10,000	Over £10,000
Will it impact upon the utilisation or provision of a public service?	Disruption to Service	Service Failure
Will it impact upon judicial proceedings?	Low level criminal proceedings	Serious Crime
Is there a risk to personal safety?	Low to Medium	High
Is there a reputational risk to the organisation	Low to Medium	High

The level of protective marking applied to a document or a record will be the highest level achieved in response to the 7 questions above.

Protective Marking – Handling Matrix			
	Classification		
Activity	UNCLASSIFIED	NHS PROTECT	CONFIDENTIAL
Document marking (at creation)	Protective marking classification to be bold and in BLOCK CAPITALS within the footer of a document or record.		

Hard Copy Storage	General storage no specific barriers required	One barrier in place e.g. stored in locked cabinet	Two barriers in place. e.g. stored in locked cabinet in locked room.
Clear Desk Policy	Documents can remain on desk in in-trays etc.	All documents to be locked out of sight when desk is not attended.	
Internal Distribution Services	Transit envelopes	Sealed envelope showing NHS PROTECT	Sealed envelope showing. NHS CONFIDENTIAL
External Postal Services and Couriers	Sealed envelope	Sealed envelope: Seal can be initialled	Double envelope both fully addressed. CONFIDENTIAL and return address on inside envelope only.
Email	No restriction	Can be used subject to the usual security checks or encryption is used	Not to be sent.

Email - NHS Net	No restriction	Can be used subject to the usual security checks	Can be sent if with encryption.
Telephone - Landline	No restriction	Can be used subject to the usual security checks	Not to be used.
Disposal of Protectively Marked Material	Refer to the Department of Health and NHS Retention and Destruction Schedule.		