Derby and Derbyshire
Clinical Commissioning Group

NHS Derby and Derbyshire Clinical Commissioning Group

Records Management Policy

(Policy on the Retention and Destruction of Records)

KEY POLICY MESSAGES	
1.	Records are essential to evidence the business decisions and activities of the CCG
2.	Records are corporate records and are owned by the organisation no by individuals
3.	Information Asset owners are accountable for the use and protection of records in their directorate

VERSION CONTROL

Title:	Records Management Policy
Supersedes:	• IG04 - Information Lifecycle Management Policy • IG05 - Records Management Policy • IG06 - Information Asset Register Procedure • IG08 - DPIA Guidance Document • IG81 - Data Quality Policy • IG19 - Information Risk Policy • IG22 - Safe Haven Procedure
Description of Amendment(s):	Version 1.0 – Initial Draft Version 2.0 – January 2020. Version 3.0 – Version number updated following approval at Governance Committee November 2020. Version 3.1 – Compliance statement added to Target Audience.
Financial Implications:	Not Applicable
Policy Area:	Corporate Delivery
Version No:	Version 3.1
Author:	IG Team (Ruth Lloyd, Information Governance Manager & Emma Holt, Information Governance Assistant)
Approved by:	SIRO and Governance Committee, 12 November 2020
Effective Date:	November 2020
Review Date:	November 2022
List of referenced policies	N/A
Key Words section (metadata for search facility online)	Records Retention Destruction Timescales Compliance Organisational Memory Information Governance
Reference Number	IG03
Target Audience	CCG approved policies apply to all employees, contractors, volunteers, and others working with the CCG in any capacity. Compliance with CCG policy is a formal contractual requirement and failure to comply with the policy, including any arrangements which are put in place under it, will be investigated and may lead to disciplinary action being taken.

CONTENTS

1. AIM OF POLICY

1.1 All NHS records held by the CCG are public records under the Public Records Act 1958. Under the Act, the Secretary of State for Health and Social Care and all NHS organisations have a duty to safeguard this information throughout its lifecycle, including the eventual disposal of all types of records. Furthermore, the destruction of records is irreversible and could have serious consequences that could be detrimental to the reputation of the CCG and the delivery of care in the local area.

1.2 By enforcing a written policy on Records Retention and Destruction, the CCG can:

1.2.1 help to protect itself against liability for the actions of its staff;

1.2.2 protect the reputation of the CCG, its staff and the NHS;

1.2.3 ensure statutory and regulatory compliance;

1.2.4 make clear to staff whom they should contact about any aspect of records management.

1.3 This policy provides a clear and easily understood framework for the CCGs management of records, including:

1.3.1 creation, maintenance, review and destruction of records (Lifecycle management);

1.3.2 retention and Destruction timescale guidance;

1.3.3 access controls;

1.3.4 the Role and function of Information Asset Owners;

1.3.5 Data Protection by design and default principles – and the implementation of Data Protection Impact Assessments and sign off;

1.3.6 the importance of Data Quality within the CCG;

1.3.7 the management of information risk- including Information flow mapping;

1.3.8 the creation and management of Privacy Notices;

1.3.9 safe haven processes adopted within the CCG;

1.3.10 management of Subject Access Requests.

2. SCOPE AND APPLICABILITY

2.1 This policy governs the use of and retention of all records processed (Held, Obtained, Recorded, Used and Shared) by the CCG.

2.2 This policy applies to all records held in digital or paper format, and all Information Asset Owners have received training on the appropriate management of records for which they have accountability.

2.3 This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff and volunteers) of the CCG, referred to in this policy collectively as 'staff'. Third Parties with whom the CCG may agree information sharing protocols will be governed by the associated information sharing agreements and will be made aware of this policy. All staff are responsible for the safe management of the information and records they process (any information Held, Obtained, Recorded, Used, or Shared) as part of their role.

2.4 Adherence to this policy forms part of the employee's employment contract, and as such any breach of this policy can be considered within disciplinary procedures.

3. LEGAL ACTS AND DEFINITIONS

3.1 Legal Acts

The law which provides the framework for the management of the above includes:

- General Data Protection Regulation;
- Data Protection Act (DPA 2018);
- Freedom of Information Act 2000;
- Environmental Information Regulations;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2012;
- Human Rights Act 1998.

3.2 Definitions

"Appraisal"

is a process to determine how long a record should be kept (the retention period) and the method of disposal at the end of the retention period;

"Destruction"

means the process of deleting records beyond possible reconstruction. The information in the record, whether paper, images or electronic, must become completely indecipherable;

"Disposal"

is the implementation of appraisal and review decisions, including the destruction or transfer of custody. It includes transferring paper records to electronic formats;

"Retention"

is the continued storage and maintenance of records until a determined date of disposal when the record is no longer needed.

4. SUPPORTING DOCUMENTS

- NHS Information Governance: Guidance on Legal and Professional Obligations
- NHS Code of Confidentiality
- Information Security Management: NHS Code of Practice April 2007
- Caldicott Guardian Manual 2017
- NHS Information Risk Management
- NHS Records Management Code of Practice 2016
- Data Security and Protection Toolkit
- Caldicott Reports

5. RECORDS MANAGEMENT IN PRACTICE

5.1 Creation, maintenance, review and destruction of records (Lifecycle management)

5.1.1 Record creation is one of the most important processes in records management and all staff within the organisation should aim to create good records that can be easily accessed and used in an effective manner.

5.1.2 Records captured or filed in a corporate filing system must be regarded as authentic or reliable – all staff must understand that a DOCUMENT – is a plan of what is to be done and can be subject to change – whereas a RECORD is created when something has been done – and cannot be subject to change. For example – meeting minutes which are approved are a RECORD of that meeting - a project plan which is in the development stages (prior to approval) is a document.

5.1.3 Records management, and the effective referencing of records means that the CCG can: Demonstrate decision making processes; provide assurance of our activities; make decisions based upon accurate records; and be assured that records are referenced and available where required.

5.1.4 A clear and logical filing structure that aids the retrieval of records must be used. The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. If this is not possible the names allocated to files and folders should allow 'intuitive filing'.

5.1.5 Final versions of appropriate documents will be circulated or placed onto the local Intranet or Internet to ensure that all staff can have access to the approved versions of policies and procedures. Where CCG decisions are recorded – these are usually in the form of Committee minutes, and these are published to the

internet on a routine basis. Policies should also be made available on the internet / intranet dependent upon their content.

5.1.6 Version control including the identification of the approving committee and date of approval must be part of records created. The review date must also be specified where required. This is reflected in the Policy Format adopted by the CCG.

5.1.7 The CCG has in place electronic systems for groups of records which identify patients. Examples of this are BluTec for the administration of Individual Funding Requests, and DATIX for the processing of PALS enquiries and complaints. Within any system in place for the management of identifiable information, individual login is provided, and the accesses undertaken by individuals can be audited.

5.1.8 Information Classification and handling is detailed below.

5.1.9 Different types of information carry varying degrees of sensitivity and need to be handled accordingly. The proper classification of information assets is vital to ensure appropriate and proportionate controls to keep information secure.

5.1.10 The CCG has a defined approach to demonstrate good practice in marking records for all types of information which may be handled, shared, stored, and disposed of, in all media, by the CCG. This includes; ICT systems; paper records, telephone and voice conversations, photographs; recording tapes, CCTV footage; entry passes and medical records.

5.1.11 Under the NHS Code of Practice all patient information is to be treated as CONFIDENTIAL. All documentation is held to be OFFICIAL; consequently, there is no requirement to explicitly mark routine information with the OFFICIAL classification.

5.1.12 In addition, the NHS Code of Practice defines descriptors applicable to data produced by, or relevant to, the conduct of NHS business and activity, as follows:

“Commercial”

to identify market-sensitive information, including that which is subject to statutory or regulatory obligations that may be damaging to the CCG;

“Personal”

to identify Personal Data (defined under the Data Protection Act 2018), the release or loss of which could cause harm, distress or detriment to the individual(s) to whom it relates; and

“LOCSEN”

to identify information which is locally sensitive to the CCG itself or to a recipient CCG or other organisations within the NHS.

5.1.13 All items considered under 'confidential' sessions of CCG meetings will be considered as a minimum as LOCSEN, and held securely.

5.1.14 Key controls shall be applied in accordance with the sensitivity of the information and in keeping with the Information Asset Owner's adherence to the requirements of Information Risk Management. Controls may be physical, procedural or technical. IAOs shall set the appropriate data classification and access as well as retention details for each set of corporate records under their control. This is undertaken as part of information flow mapping.

5.1.15 All Employees must respect and abide by the relevant statutory obligations and protections, including the Data Protection Act 2018, GDPR, Freedom of Information Act 2001, the Official Secrets Acts, and the Public Records Act. Access to information is limited to a need to know basis in line with the Caldicott Principles.

5.1.16 All Employees who handle sensitive assets must understand the impact of these legal frameworks and how it relates to their role.

5.1.17 Best practice on the provision of document referencing is included at appendix 5.

5.2 Retention and Destruction Timescale Guidance

5.2.1 Effective records management ensures that information is properly managed and is available whenever and wherever there is a justified need for information, and in whatever media:

(a) to support the rights of service users, staff and members of the public;

(b) to support policy making and managerial decision making, as part of the knowledge base for NHS services;

(c) to meet legal requirements and assist in audit;

(d) to ensure any decisions made can be justified or reconsidered at a later date;

(e) to help commission services in consistent and equitable ways.

5.2.2 Records must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails should track all use and changes. Records must be held in a robust format, which remains readable for as long as records are required. The CCG must have records management procedures in place that cover the creation, filing, location, retrieval, appraisal, archive and destruction of records.

5.2.3 The CCG is adopting the retention/disposal procedure and the retention schedules detailed within the: Information Governance Alliance (IGA) Records Management Code of Practice for Health & Social Care 2016. This is available here: https://digital.nhs.uk/data-and-information/looking-after-information/data-

security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016 and lists all the nationally agreed retention periods for specified groups of records.

5.2.4 Records selected for archival preservation that are no longer in use by the CCG are to be transferred as soon as possible to an archival institution e.g. a Place of Deposit.

5.2.5 Records selected for archival preservation that are no longer in use by the CCG are to be transferred as soon as possible to an archival institution e.g. a Place of Deposit.

5.2.6 All NHS records are public records under the terms of the Public Records Act 1958 sections 3 (1)–(2). The Secretary of State for Health and all NHS organisations have a duty under the Public Records Act to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

5.2.7 Where the CCG has identified that a record is nearing or has exceeded its retention period in line with the guidance in (b) above, where no business reason can be identified for its continues retention, it will be securely destroyed. This will be undertaken following a review of the record content, and a completion of records destruction form. The form is available here: http://intranet.derbyandderbyshireccg.nhs.uk/staff-area/governance/records-management/

6. ACCESS CONTROLS

6.1 The CCG must ensure that all information assets that hold or process personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data.

6.2 There should be formal information security risk assessment and management programme and operating systems under the organisations control must support appropriate access control functionality. Generally within the CCG this is achieved by the control of the CCGs advice directory – the control of access to the CCGs network, which has the NECS CSU as the gatekeeper, connected to the CCG starters and leavers process.

6.3 As a minimum the completion of the information flow mapping generates a risk assessment of the flow of information into and out of the CCG, and each Information Asset Owner is asked to confirm the access controls in place for each information asset. The requirements of the IAO's are confirmed in section 7.4.

7. THE ROLE AND FUNCTION OF INFORMATION ASSET OWNERS

7.1 As part of an EU General Data Protection Regulation (GDPR) compliance work, all organisations are required to map their data and information flows in order to assess their privacy risks.

7.2 Mapping of information flows is considered the cornerstone of evidence that an organisation understands what information it holds, its lawful basis for doing so, an how that information is appropriately protected. This is the basis upon which the CCG develops and maintains its privacy notice. Without this in place and evidenced, should the CCG be subject to an information breach, a fine would be likely if we cannot demonstrate that both organisational and technical security measures are in place for each of our information assets. Completion of our information flows mapping also dovetails into effective business continuity planning with CCG and ICT colleagues, and assurance of Data Protection by Design and Default where new information processes are introduced.

7.3 CCG responsibilities for Information Flow Mapping is described below:

7.3.1 to ensure we meet our statutory obligations we need a robust structure of Information Asset Owners (IAOs) across all directorates who are responsible for formally reviewing the risks to the confidentiality, integrity and availability of their information assets, identifying flows into and out of their areas;

7.3.2 Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. This is affirmed on an annual basis via the ISO statement to the SIRO included at appendix two;

7.3.3 as a result they are able to understand and address risks to the information, and ensure that information is processed within the law. Information Asset Administrators (IAAs) are the deputies for the IAOs and are usually Department Managers. The IAA ensures that staff adhere to policies and procedures which ensure the Confidentiality, Integrity and Availability of data in use in the CCG, and that any changes to processes within the department are reflected in the information flows mapping;

7.3.4 the IAA must consult their IAO on any potential or actual risks to the asset and ensure that information asset registers are accurate and up to date;

7.3.5 annually as a minimum, the IAO must affirm to the Senior Information Risk Owner (SIRO) that the processing they are undertaking is mapped, and risk assessed, with appropriate mitigations to any risks identified in place.

7.4 **Information Asset Owner Responsibilities**

7.4.1 Understand which ‘assets’ are in use by their staff / departments which they own.

7.4.2 Lead and foster a culture that values, protects and understands the importance of information.

7.4.3 Know what information the asset holds, and what enters and leaves it and why.

7.4.4 Know who has access and why, and ensure their use of the asset is monitored.

7.4.5 Understand and address risks to the asset, and provide assurance to the SIRO.

7.4.6 Ensure processes are in place for Subject Access where this is applicable.

7.4.7 Ensure identification and training of sufficient Information Asset Administrators to ensure that the process of control of information assets is in place across the IAO work responsibilities.

7.5 **Communication with Information Asset Owners in May 2019:**

7.5.1 The following statement was issued to all IAOs in May 2019, and this expectation will be re-iterated to all IAOs on an annual basis as the Information Flow Mapping return is requested:

(a) you have accountability as an Information Asset Owner. This means that for the information assets in use in your area of work, you affirm that these assets are all accessed securely, and that a record of processing activities (the information flows mapping) is complete, risk assessed and maintained as up to date to evidence this. The template for information flows mapping is attached;

(b) our reporting deadlines are that a complete and risk assessed Information Flows mapping report is required as part of the assurance work for the CCGs, and must be presented within each financial year to the SIRO;

(c) given than you have a window of opportunity to complete the attached, please can you provide a completed copy of your information flows to ddccg.igteam@nhs.net by the end of September 2019;

(d) this deadline is set to allow for a formal review of the legal basis for each information flow, and for exception reporting for those who have not returned information flows to be reported to the Directors Group at the beginning of December 2019;

(e) you will be invited to attend face to face training in order to further understand your role, however you must complete as a minimum, a list of the information assets in use in your department, within the described timescales;

(f) may I take this opportunity to remind you of the role of the Information Asset Owner, in that you are accountable for the data which is processed in your area, and that I am available to discuss approach, and advise on facilitating flows mapping with your teams;

(g) to confirm, should the CCGs have an information breach or fail to comply with national expectations of data security, where this is in your area, you will be asked immediately for your information flows mapping, the process of risk assessment undertaken and confirmation of who has access to data within your work areas.

7.6 Identification of information assets

7.6.1 Information Assets (IA) are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. Information assets are likely to include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data. Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

7.6.2 Information Assets should be documented in a CCG asset register. The approach of the CCG is to ask that IAOs and IAAs complete the information flow mapping, detailing the assets in use in their work areas. The process of completing the information flow mapping generates a risk assessment for each identified flow of information. The Information Governance Team will then create the Information Asset register, and where appropriate, develop privacy notices with the relevant IAO.

7.6.3 The IAO will lead on the development of Data Protection Impact Assessments for their work areas, ensuring that new processing of data is included in their Information Flow Mapping.

7.6.4 The IAO provides assurance as a minimum on an annual basis to the SIRO that the extent of the information processing in their work area is reflected in the information flow mapping, and that the risks identified within processing are effectively mitigated.

7.6.5 The IAO is responsible for ensuring that any actions required to mitigate the risks of processing are undertaken and implemented across the area of responsibility. The IAO is also responsible for ensuring that any incidents which happen in their work area are reviewed against the identified information asset, and process revision considered where confidentiality, integrity or availability issues are identified for that data set.

8. DATA PROTECTION BY DESIGN AND DEFAULT PRINCIPLES – AND THE IMPLEMENTATION OF DATA PROTECTION IMPACT ASSESSMENTS AND SIGN OFF

8.1 A Data Protection Impact Assessment (DPIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. DPIA's are a legal requirement under the GDPR to support Privacy by Design principles.

8.2 The DPIA template is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project, building data protection compliance in from the outset rather than bolting it on as an afterthought. This document details the process for conducting a Data Protection Impact Assessment (DPIA) through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated.

8.3 A DPIA must be carried out whenever there is a change that is likely to involve a new use or significantly change the way in which personal data is handled, for example a redesign of an existing process or service, or a new process or information asset being is introduced. A key factor is to ensure application of data minimisation principles, reduce the amount of data processed to comply with the principles of GDPR.

8.4 There are three stages to a Data Protection Impact Assessment which are described in Appendix 1.

9. THE IMPORTANCE OF DATA QUALITY WITHIN THE CCG

9.1 The CCG recognises that all of their decisions, whether health care, managerial or financial, need to be based on information which is of the highest quality. Data quality is crucial and the availability of complete, accurate, relevant and timely data is important in supporting patient/service user care, governance, management and service agreements for health care planning and accountability.

9.2 The CCGs responsibilities with regard to data quality extends to all data sets in use, which includes patient/service user information, staff information, minutes of meetings and commissioning data sets.

9.3 The CCG recognises that the data sets it uses are supplied by other organisations and in order to make sound and informed decisions the quality of the data must be verified wherever possible.

9.4 The responsibilities for Data Quality are set out below:

9.4.1 the Accountable Officer / Chief Executive Officer of the CCG has overall responsibility for ensuring that data quality is valued within the CCG;

9.4.2 all system managers (Information Asset Owners) must ensure that procedures to validate and endure data quality are in place for each personal confidential data system;

9.4.3 it is the responsibility of line managers to ensure staff compliance with data quality procedures and to ensure that staff comply with good practice in data quality.

9.5 Data quality is a measure of the degree of usefulness of data for a specific purpose. Data should be:

9.5.1 complete (in terms of being captured in full);

9.5.2 accurate (the proximity of the figures to the exact or true values;

9.5.3 relevant (the degree to which the data meets current and the potential user's needs);

9.5.4 accessible (data must be retrievable in order to be used and in order to assess its quality;

9.5.5 timely (recorded and available as soon after the event as possible);

9.5.6 valid (within an agreed format which conforms to recognised standards – either national or local);

9.5.7 defined (understood by all staff who need to know and reflected in procedural documents);

9.5.8 appropriately recorded (in either paper or electronic format).

9.6 The CCG recognises the importance of differentiating between those data which the CCG has direct control of, for example where CCG staff input directly into their own systems and to ensure the quality of data is maintained those data where the CCG is the recipient under the requirements of a contract, for example the supply of retrospective health events data for its patients treated at a hospital or aggregate data provided to summarise delivery of a performance standard.

9.7 Where the CCG is in direct control of data entry:

9.7.1 that process should be well-defined;

9.7.2 the structure of data designed to reduce the risk of errors either through the data model or through the design of the user interface;

9.7.3 regular spot checks should be undertaken by staff members; which involve analysis of a random selection of records against source material, if available;

9.7.4 spot checks should be done on an on-going basis (defined by the Information Asset Owner) to ensure the quality of data is maintained and where necessary, improved;

9.7.5 the CCG routinely receives activity information from its service providers. This information is used to monitor the performance of contracts and to contribute to the service planning and development process. Sufficient and appropriate checks are made by the service providers to ensure that the information received is accurate and complete. Where data falls outside anticipated ranges a more detailed evaluation and validation is undertaken.

9.8 Where the CCG receives data from other organisations it should:

9.8.1 encourage a culture of routine data validation comparing counts of new data against old ones, ensuring no missing cohorts by age, gender, etc.;

9.8.2 cross-check data against alternative sources.

9.9 When presenting data:

9.9.1 highlight discrepancies when interpreting data e.g. by including confidence intervals;

9.9.2 prefer standardised data (balancing age and gender and where possible deprivation) to raw rates;

9.9.3 clarify the source of data (e.g. does A&E data refer to ED, eye casualty, WICs);

9.9.4 highlight missing data; and

9.9.5 take care to rule out known biases e.g. due to seasonality, regression to the mean when analysing well performing or poorly performing cohorts over time.

9.10 On submission of data returns, Information Asset Owners will be responsible for developing and implementing procedures to ensure the completeness and validity of the data sets used. This can be done by comparing to historical data sets, looking at trends in the data and also by cross checking the data with other staff members.

9.11 The CCG will endeavour to ensure that timescales for submission of information are adhered to and that the quality and accuracy of such submissions is of the highest standard. Internal deadlines for the completion of data sets, to ensure national timescales are achieved, will be explicit and monitored.

9.12 The CCG will document the processes for data validation as Standard Operating Procedures and ensure relevant staff use and maintain these. Validation should be accomplished using techniques that are in line with the legal powers of the CCG or using services provided by the CCG's DARS (Data Access Request Service) information sharing agreement with NHS Digital (which is held by the CCG Information Governance Manager.

10. THE MANAGEMENT OF INFORMATION RISK - INCLUDING INFORMATION FLOW MAPPING

10.1 The CCG needs to have a framework to ensure that new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements. Additionally it needs to ensure that existing processes and procedures remain compliant relevant security and confidentiality legislation and codes of practice.

10.2 The CCG must also be able to demonstrate that appropriate technical and organisational security measures have been undertaken with regard to the processing of information within the CCG as part of GDPR compliance.

10.3 All employees have an important role to play in order to ensure that risks are minimised and when encountered appropriately managed. It is important to remember that risk management is not about apportioning blame, but about promoting a fair and responsible culture, which contributes to learning and improvements when mistakes may occur, but that the consequences of failure to manage information risks adequately can be both corporate and individual.

10.4 The policy requirements for effective information risk management are:

10.4.1 protect the CCG, its staff (and board members) and its patients from information risks where the likelihood of occurrence and the consequences are significant;

10.4.2 provide a consistent risk management framework in which information risks will be fully considered and addressed during key approval, review and control processes;

10.4.3 encourage a pro-active approach to managing risks, rather than a re-active risk management method;

10.4.4 provide structure, transparency and assistance to improve the quality of decision making throughout the organisation;

10.4.5 meet all legal or statutory requirements;

10.4.6 assist in adequately safeguarding the CCG's information assets.

10.5 Information risk is inherent in all administrative and business activities and everyone working for, or on behalf of the CCG must effectively manage information risks for which they are responsible. The Governing Body recognises that the aim of information risk management is not to eliminate risk, but rather to provide a structured approach to accurately identify, prioritise and manage the risks involved in all CCG related activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

10.6 The principal objectives of the Risk Management function are:

10.6.1 to assist with the identification of all reasonably foreseeable risks, particularly which may have potentially adverse effects on the quality of care, confidentiality of patient information, safety of patients, staff and visitors (Risk Identification);

10.6.2 to assist and support in the assessment of risks in terms of likelihood and severity (Risk Assessment);

10.6.3 to ensure risk ratings are applied to identified risks (Risk Quantification);

10.6.4 to identify the appropriate level of management to be responsible for the risk (Risk Owner);

10.6.5 to take positive action to eliminate or reduce risks to as low as is reasonably practicable and continually review these actions (Risk Treatment);

10.6.6 IG Working Group, Governing Body and Senior Management appraised of the significant risks present across the CCG (principally via the Risk Register and Risk reports);

10.6.7 to create an escalation and accountability framework to help ensure satisfactory risk mitigation processes and Risk Owners are encouraged and supported in their task;

10.6.8 to adequately protect transfers/flows of information, the CCG will identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with the CCG's Safe Haven Procedures and relevant legislation (e.g. Principle 7 of the Data Protection Act 2018 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data);

10.6.9 where significant risks are highlighted by the mapping exercise, immediate action will be taken to either suspend the transfer of information until remedial action can be taken, or to transfer the information by another, more secure method;

10.6.10 the outcomes of the information mapping and identified risks will be used to develop guidance for staff on appropriate and secure methods of transferring personal and sensitive information in any format (hardcopy and electronic);

10.6.11 where a new Information Assets is acquired by the organisation the IAO will ensure, as part of the PIA process that the Information Flow Mappings are mapped and the CCGs Information Flow Mapping Mapping Register is updated.

11. MANAGEMENT OF SUBJECT ACCESS REQUESTS

11.1 Under the General Data Protection Regulation (GDPR), an individual has a number of rights in respect of the information held by the CCG which include the:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

11.2 These rights are qualified rights, and not all are applicable to public records. For example, the processing of records for the purpose of providing healthcare, would not normally be erased at the request of the data subject. Should any queries be received with regard to individual's rights under the GDPR these should be directed to the Information Governance Manager via email to ddccg.igteam@nhs.net

11.3 The subject access procedure for the CCG can be found here: https://www.derbyandderbyshireccg.nhs.uk/privacy/

12. CONFIDENTIALITY AUDIT

12.1 The CCG has control mechanisms in place to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints and alerts.

12.2 The Data Security and Protection Toolkit requires that CCGs ensure access to confidential personal information is monitored and audited locally, and that the results of the confidentiality audit, with supporting actions are received at the Information Governance Assurance Forum, which reports into the CCG's Governance Committee.

12.3 The CCG will ensure that confidentiality audits are undertaken in line with the organisation's Confidentiality Audit checklist included at appendix One. The SIRO and Caldicott Guardian (CG) will be updated with the findings of any confidentiality audits and will ensure that appropriate action is taken.

13. SAFE HAVEN PROCEDURE

13.1 'Safe Haven' is a term used to cover an agreed set of administrative procedures to ensure the safe and secure handling of personal confidential data and/or sensitive information.

13.2 All NHS organisations require a Safe Haven Information procedure in order to maintain the privacy and confidentiality of personal confidential and/or sensitive data. The safe haven procedure is included as an appendix to this policy.

14. EQUALITY AND DIVERSITY

14.1 The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

14.2 This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of

their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

14.3 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

15. DUE REGARD

15.1 The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. The document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to socio-economic status, immigration status and the principles of the Human Rights Act.

15.2 In carrying out its function, the CCG must have due regard to the Public Sector Equality Duty. This applies to all activities for which the CCG is responsible, including policy development, review and implementation.

16. REFERENCES

- General Data Protection Regulation (GDPR)
  https://gdpr-info.eu/
- Data Protection Act 2018
  https://www.legislation.gov.uk/ukpga/2018/12
- Freedom of Information
  www.opsi.gov.uk
- IGA Records Management Code of Practice for Health & Social Care 2016
  http://systems.digital.nhs.uk/infogov/iga/resources/rmcop

Appendix 1 – Data Protection Impact Assessment

Stage 1 - The initial screening questions

This document is to be completed by the IAO or Project lead responsible for delivering the proposed change.

The purpose of the screening questions is to ensure that a further DPIA assessment is required and ensure that the investment in the organisation is proportionate to the risks involved. If a response to any of the questions is "yes" then a Data Protection Impact Assessment should be considered.

A meeting with the CCG Information Governance Lead should be arranged to review the responses and discuss whether a stage 2 assessment should be completed. The IG Manager will support this process as requested by the CCG Information Governance Lead.

Stage 2 – Data Protection Impact Assessment

To be completed by the IAO or project lead responsible for delivering the proposed change. The completed form will be assessed by the Information Governance Lead / IG Manager. The project lead will be advised if further detailed information or supporting documentation such as fair processing notices, consent form etc. is required.

It is essential that the data mapping section of the DPIA is completed in as much detail as possible. This step is a key part of any DPIA process and a thorough assessment of privacy risks is only possible if the organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk.

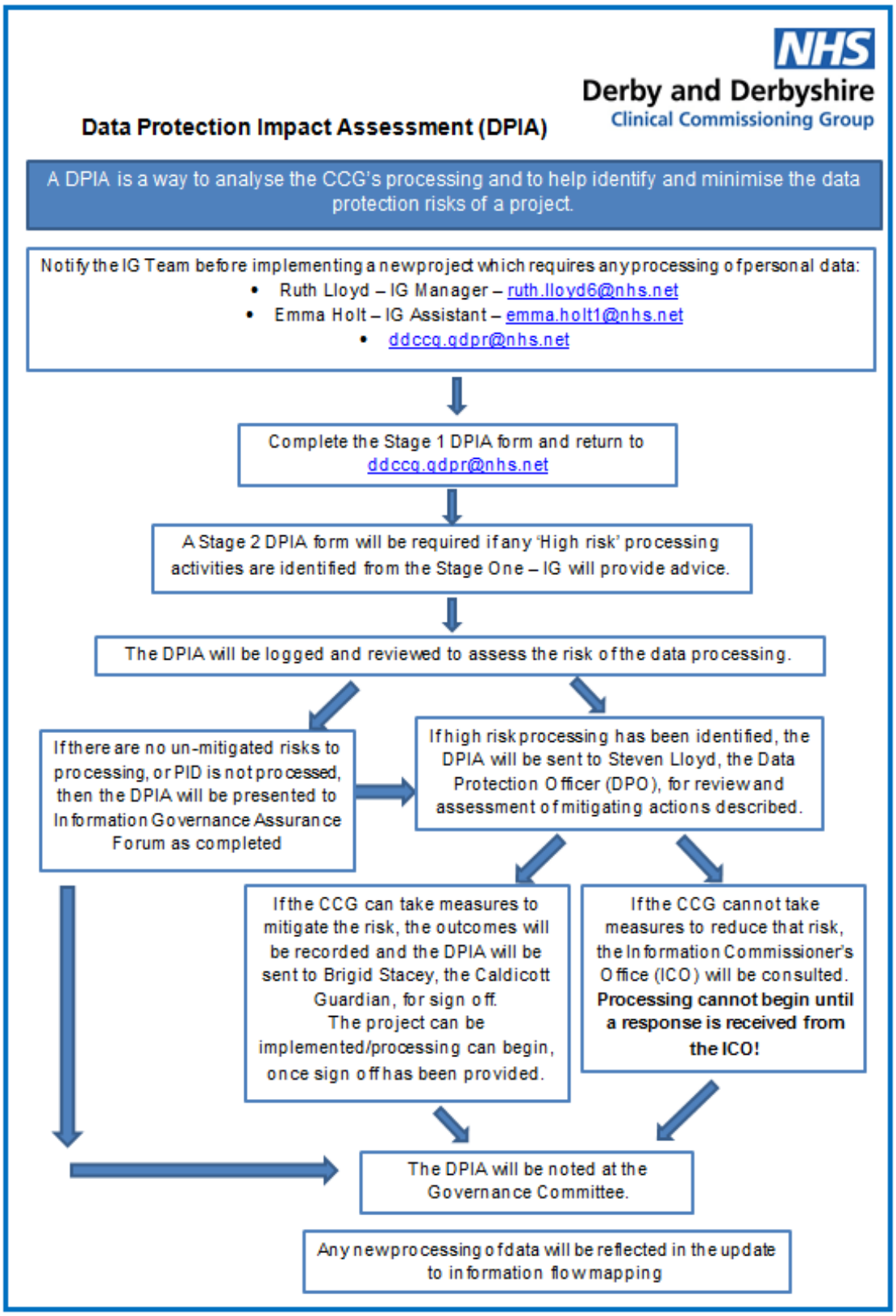
Stage 3 – Compliance Assessment/DPO Sign-Off

The completed DPIA will be assessed against the compliance checklist which includes the General Data Protection Regulations, Article 29 Working Group checklist, Caldicott Guidelines, NHS Digital guidance, Data Protection Act, Common Law Duty of Confidentiality and the Human Rights Act for example. The IG Lead/ IG Manager will also consider if other pieces of legislation or best practice guidelines are applicable.

Any risks will be noted and solutions put forward, these will be agreed by the project lead and signed off by the CCG SIRO. Where the DPIA discovers complex or several IG risks these need to be raised with the Information Commissioners Office. If this is apparent the IG Manager and or DPO must be consulted and will provide advice on the next step.

The DPIA is a dynamic document and should be reviewed regularly throughout the project lifecycle.

The DPIA Process flow diagram is included below:



Appendix 2 - Information Asset Owner (IAO) Annual Assurance Statement to SIRO

This report covers the period From_____ to _____

I can confirm that the following activities relating to my role as an IAO and to the use of my information asset(s), have been conducted/are in place during the period indicated above:

1. I am up to date with my information risk management training (e-learning or equivalent) requirements.

2. I ensure those who have access to my information asset(s) are up to date with their information risk awareness training (e-learning or equivalent) requirements.

3. I ensure all Directorate information asset(s) for which I am owner are recorded on the CCG's Information Asset Register and the entries are up to date.

4. I keep records of the access controls (which adhere to the 'need to know' principle) to my information assets. For my information assets that contain personal data I keep a record of individuals that have access to or handle that personal data. System and user access is granted to individuals or groups / teams on a role specific basis and is regularly reviewed to ensure only those with a specific need are granted access rights

5. I approve and keep a record of instances where my information assets have been saved on a removable media device.

6. I only allow Personal Data contained in my asset(s) to be transferred to personally owned ICT in exceptional circumstances and only when it has been agreed in advance by me or my SIRO.

7. I only allow Personal Data contained in my asset(s) to be transferred to non-encrypted removable media devices in exceptional circumstances and only when it has been agreed in advance by me or my SIRO.

8. Any disposal of information assets is in accordance with the organisation's Information Lifecycle Management Policy.

9. I consider the risks to my information assets; any significant information risks are escalated as set out in the Information Risk Policy. The CCG Risk Register is updated as necessary.

10. I report any misuse, theft or loss of my information asset(s) to the appropriate team.

11. I ensure that any personal data in my information assets is handled in accordance with the Data Protection Act 2018 and data sharing agreements are in place where required.

12. I ensure that Privacy Impact Assessments are undertaken where there is a proposal to change how information is shared and used.

Signed _____ Date _____

Position _____

Appendix 3 – Confidentiality Audit Spot Check

NHS
Derby and Derbyshire
Clinical Commissioning Group

On _____ the CCG undertook a review of Information Governance / data & physical security within the building.
Room number and location:

A review of your workstation identified:

No Issues	☐
Unattended PC with screen unlocked	☐
Written down passwords	☐
Unattended Smart card	☐
Unprotected patient details	☐
Unprotected confidential information	☐
Valuables left unattended	☐
Other	☐

Observations and any further comment:

A summary report on the findings of this spot-check will be reported to the Senior Management Team and Governance Committee. Please ensure you are up to date with your Information Governance training. There are additional modules available on the Health and Social Care Information Centre (HSCIC) website covering password protection, secure transfer of personal data, secure handling of confidential information and information security. **Security Check 2019/2020**

Appendix 4 – Safe Haven Procedure

- It is mandatory that secure points for the transfer of personal confidential data and sensitive information are available in order to ensure that the CCG meets its duty of confidentiality.
- Access controls and registered access levels to these secure receiving points should be restricted to those needing to access the information in order to perform their role and all staff members must be made aware of their own responsibility for ensuring the protection of personal information received in to a safe haven.
- The term 'Safe Haven' can also be considered to be a location within an organisation where confidential information is both received and stored in a secure manner.
- The Safe Haven concept should be used to ensure good practice for all person identifiable, confidential and/or sensitive information received and sent from the CCG and contractors should seek assurances from system suppliers concerning the security of digital communications channels.
- The procedure applies to all personal confidential data and/or sensitive information including corporate sensitive information that may be transferred via the following formats:
    - Post/courier
    - Telephone
    - Fax machines (Prohibited from April 2020)
    - Email
    - SMS Messaging Instant Messaging (IM)
    - Web Interfaces
    - Portable Data Storage Devices
- All routine transfers/flows of personal, confidential and sensitive information should be subject to a risk assessment and procedures should be in place to ensure receipt at a secure and protected point.
- The principles and procedure in this document should be adhered to for all person identifiable, confidential and/or sensitive information processed by the CCG.
- The Accountable Officer is responsible for ensuring the safe use and transfer of personal confidential data and corporate sensitive data in the CCG.
- The Senior Information Risk Owner (SIRO) is responsible for understanding how the strategic business goals of the organisation may be impacted by any information risks

- Information Asset Owners (IAO) are responsible for ensuring that information is protected appropriately, and where the information is shared that the proper confidentiality, integrity and availability safeguards apply. IAOs are accountable should an information security incident occur.
- Information Asset Administrators (IAA) are responsible for supporting the IAO to fulfil their responsibilities. IAAs will 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.
- The Caldicott Guardian is responsible for protecting the confidentiality of patient information and ensuring that appropriate procedures are in place.
- All Staff are responsible for ensuring personal confidential and corporate sensitive data is kept secure and confidential at all times. Staff must only process information on a 'need to know basis'
- Personal confidential data and sensitive documents and records will be stored in locked drawers or cabinets, in a locked office area with a swipe card door entry security system, or coded key pad, limited to authorised staff working for the CCG.
- Identification and/or approval will be required from a relevant Information Asset Owner (IAO) before a member of the CCG staff will be given access to information stored in a Safe Haven.
- Unauthorised people will not be allowed access to areas where confidential information is kept unless supervised. ID badges will be checked before access is permitted.
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office or any visitors
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- A nominated person will be responsible for the security of locked cabinets where personal confidential data and sensitive records are stored within individual business teams. They will be responsible for the safe-keeping of the information stored in the cabinets.
- Desks should be kept clear and all personal confidential data locked away at the end of the day.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screensaver function and be switched off when not in use.

- Business teams that have a Safe Haven storage facility within their own work areas should ensure an appropriate tracking system is in place for all information stored in the facility.

- All business areas that have personal, confidential data and/or sensitive information must have an appropriate Safe Haven and ensure that it meets appropriate standards (ie that it complies with the Data Protection Act2018, in particular with reference to Principle 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and Caldicott Principle 4 Access to patient identifiable information should be on a strict need-to-know basis).

- The person removing the information is then responsible for maintaining its confidentiality and returning it as quickly as possible to its storage place.

- Fax machines are not to be used within the CCG. Their use will become unlawful from April 2020.

- External requesting parties should comply with the CCG Safe Haven Procedure and meet appropriate legislation and related guidance. It is the responsibility of CCG staff to ensure the receiving party is compliant before transferring the information e.g. this may be done by sending/emailing a copy of our Safe Haven Procedure to the requesting party and asking them to ensure compliance.

Communicating by mail

- When sending person identifiable confidential and/or sensitive information mark the envelope 'Private & Confidential – To be opened by Addressee Only'.

- Confirm the name, department and address of the recipient, do not use acronyms as these can be easily confused. Ask the recipient to acknowledge receipt of the information.

- Seal the information in a robust envelope using strong wrapping tape.

- Where appropriate place the document/record in double bags and send the information by Special Delivery or by courier. Ensure a signed confirmation of receipt is obtained.

- Deliver confidential incoming post immediately or as soon as possible to the recipient but do not leave on the desk or pass to anyone else if the recipient is not available. Lock in a drawer or cabinet until the recipient is available.

- Open incoming mail away from public areas. Mail must be opened by the addressee only if marked as such.

- Pass items not marked with a name or department, that are not labelled 'Private and Confidential' to the Governance Team to establish to whom it belongs.

- Avoid sending large amounts of information about one person or information about many persons by mail.

- Recipients of frequent or significant numbers of confidential mail are advised to keep a log to record receipt or transfer within the organisation.
- All sensitive documents must be stored face down in public areas and not left unsupervised at any time.

Transfers of bulk confidential hard copy information

- Lockable crates must be used to move bulk confidential hard copy information from one place to another. Hardcopy information must be stored in a locked cupboard or cabinet.
- Obtain a receipt for hand delivered confidential information.
- Personal confidential information should only be taken off site when absolutely necessary, or in accordance with local policy.
- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave person identifiable information unattended.
- Ensure the information is returned as soon as possible.
- Record that the information has been returned.

Communicating by Telephone

- Personal confidential data and/or sensitive information should not be divulged over the telephone because of the risks involved (e.g. being overheard, inadvertent disclosure of confidential information, disclosing confidential information in an appropriate manner etc.)
- If the use of a telephone is essential to convey the information then the following security protocols must be adhered to:
    - Confirm the name, job title, department and organisation of the person requesting the information, ensuring that you are speaking to the correct person
    - Take a contact telephone number e.g. main switchboard number (never a direct line or mobile telephone number if possible)
    - Ring back to confirm that person's identity
    - Confirm the reason for the request
    - Provide the information only to the person who has requested it (do not leave messages)

- Ensure that the enquirer has a legitimate right to have access to the information before information is given out and provide information only to the person who has requested it
- Ensure that you record your name, the date and time of disclosure, the reason for it and who authorised sharing. Also record the recipient's named, job title, organisation and telephone number.
- Where staff are working in an open plan office an available private room should be used for telephone conversations that are highly confidential.

Communicating by Email

- NHS mail is currently the only NHS approved method for exchanging person identifiable or sensitive data, but only if both the sender and recipient use an NHS mail account or if sending to another government secure domain.
- Always consider first if email is the best way to send the information. NHS.net email is automatically encrypted in transit, therefore any email sent from one NHS.net email account to another (e.g xxx@nhs.net to yyy@nhs.net) is secure.
- The user sending the email must first confirm the recipient's correct email address, for example verbally over the telephone or through the NHS.net mail directory.
- NHS.net email is hosted on the N3 network and as such forms part of the wider public sector (Public Services Network (PSN). This means that email is encrypted when delivered to any of the following email domains:
  - NHSmail addresses
- Government secure email domains
  - Police National Network/Criminal Justice Services secure email domains
  - Ministry of Defence secure email domains
  - Local Government/Social Services secure email domains
- All emails sent between these domains are encrypted in transit and the entire environment/infrastructure is accredited with strict end point access controls.
- Emails sent to or received from any other domain is untrusted (open to forging, interception or alteration) unless the NHSmail Encryption feature is used. Please see the CCG Email policy or NHSmail. (Tools / Guidance / Emailing personal confidential data or sensitive information) for full details on how to use the encryption feature.
- Emails containing confidential information should be clearly marked 'Confidential' in the subject header box.

- Always check that the email address(es) of the recipient(s) appear correctly in the To and Cc boxes. Automatic recognition of names can result in the information being sent to the incorrect recipient and cause an Information Governance breach.
- If sending to multiple recipients use a distribution list ensuring security permissions and access controls have been checked. The members of the distribution list can be checked through the Properties button when you select it.
- Always ensure that the distribution lists contain only those individuals who are authorised to receive the information.
- Do not send or forward person identifiable, confidential and/or sensitive information by email to any person or organisation that is not specifically authorised to receive and view that information.
- Do not send emails containing personal confidential data and/or sensitive information to your home computer or personal email accounts.
- Emails containing personal confidential data and/or sensitive information must be stored appropriately upon receipt e.g. incorporated within HR personal records and deleted from the email system when no longer required.
    - SMS Text Messages should not be used to convey person confidential data and/or sensitive information.

Instant Messaging

- Personal confidential data and sensitive information can be transferred via instant messaging by the NHS approved platform Skype for Business. Other platforms such as WhatsApp are insecure and should not be used.
- Users should exercise the same care as they would when using email communications to ensure that the correct recipients are contacted, only authorised users receive the information, information is managed appropriately.

Portable Storage Devices

- Data storage devices e.g. Hard Drives, Memory Sticks, CD's, DVD's, PDA's or mobile telephones containing personal confidential information or business sensitive information must be encrypted to NHS standards using encryption provided by the CCG in conjunction with IT services.
- Laptops are classed as moveable media. When travelling, laptops must not be carried in open view and must be removed from sight and not left in the car once the journey is complete. If laptops are taken home by staff they must be kept safely and securely. This means that other members of their family and/or their friends/colleagues must not be able to access or use the laptop.

Safe Haven Printers

- There are no designated safe haven printers, however, CCG sites with printers that have a 'secure print' function should use this to print confidential documents e.g. Multi-Functional Devices. Where this is not possible, staff must ensure confidential printing is collected immediately.

- Confidential printing that is left lying around should be reported to the IG team.

Information Flow Mapping

- To support Safe Haven principles and implementation the CCG must ensure that all information transfers are identified by determining where, why, how and with whom it exchanges information.

- This is known as Information Flow Mapping Mapping. This mapping of Information Flow Mappings, particularly Personal Confidential Data (PCD) will identify the high risk areas of information transfers that require effective management.

Appendix 5 – Best Practice Principles in Naming Files and Folders

Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of data. Through consistency and the application of logical standards we benefit from secure storage, and the ability to locate and access information. The CCG have chosen not to dictate to teams how files must be referenced, but to provide good practice guidance.

Good practice dictates that all information (files, datasets, documents, or records) should be identifiable and traceable. This can be achieved by following good practices by applying referencing to all documents/files.

Document/file references will include:

- File name, or full file path including file name
- Name/role of file author(s) or originator(s)
- Date of creation, edit or event which is the subject of the document/file
- Version number if applicable & approving committee

Suggested file and folder naming conventions:

1. Keep file and folder names short, but meaningful.
2. Avoid unnecessary repetition and redundant words in file names and file paths.
3. Use capital letters to delimit words, not spaces.
4. When including a number in a file name always give it as a two-digit number rather than one, i.e. 01, 02 … 99, unless it is a year or another number with more than two digits.
5. If using a date in the file name always state the date ‘back to front’, and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY.
6. When including a personal name in a file name give the family name first followed by the initials.
7. Avoid using common words such as ‘draft’ or ‘letter’ at the start of file names, unless doing so will make it easier to retrieve the record.
8. Order the elements in a file name in the most appropriate way to retrieve the record.
9. The file names of records relating to recurring events should include the date and a description of the event, except where the inclusion of any of either of these elements would be incompatible with rule 2.

10. The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence, except where the inclusion of any of these elements would be incompatible with rule 2.

11. The file name of an email attachment should include the name of the correspondent, an indication of the subject, the date of the correspondence, and an indication of the number of attachments sent with the covering email, except where the inclusion of any of these elements would be incompatible with rule 2.

12. The version number of a record should be indicated in its file name by the inclusion of ‘d’ followed by the version number and, where applicable, ‘d’ indicating ‘draft version’.

13. Avoid using non-alphanumeric characters in file names