Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page
Title: Business & Corporate Records Management Protocol **Version: 3** **Reference Number: CO97**
Keywords Records, management, record keeping, audit, transportation, health records, records lifecycle
Supersedes: V2 **Description of Amendment(s):** • **Merged with CO63 Creation, filing & retention of electronic records protocol** • **Incorporating changes made following the publication by the Information Governance Alliance of the Records Management Code of Practice for Health and Social Care 2016 which includes information on specific types of records such as Email, social media, bring your own device, website and cloud based records** • **Includes the archiving procedure for HR leavers records as an appendix** ***Important Notice*** ***From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.***
Originator **Originated By: Carole McCarthy** **Designation: Records Manager**
Equality Analysis Assessment (EAA) Process **Equality Relevance Assessment Undertaken by: Records Manager** **ERA undertaken on: 21/01/2016** **ERA approved by EIA Work group on:** **Where policy deemed relevant to equality- NO** **EIA undertaken by Carole McCarthy** **EIA undertaken on** **EIA approved by EIA work group on**

Approval and Ratification

Referred for approval by: Records Manager

Date of Referral: 01/03/2017

Approved by: Information Governance Assurance Group

Approval Date: 01/03/2017

Date Ratified by Executive Directors : 20th March 2017

Executive Director Lead: Medical Director

Circulation

Issue Date: 22nd March 2017

Circulated by: Performance and Information

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? Yes

Review: 2 years

Review Date: 1st March 2019

Responsibility of: Carole McCarthy

Designation: Records Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 22nd March 2017

CONTENTS

1. INTRODUCTION

1.1 Everyone in Pennine Care NHS Foundation Trust has a duty of care to ensure that all records, and especially confidential records, are stored in a safe and secure environment, which recognises their sensitivity.

1.2 This guidance is intended primarily for those working in corporate services and those who have an administrative / clerical role within the divisional business units (DBU's).

1.3 Pennine Care NHS Foundation Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. In principle electronic and paper records should be managed consistently and to the same high standards.

1.4 Robust procedures can help to:

- Support innovation and better ways of working;
- Avoid duplication and wasted work by standardisation;
- Prevent the loss of records;
- Make a broader range of information accessible to a wider range of people;
- Provide a more flexible response to organisational changes;
- Assist the organisation in meeting its responsibilities.

1.5 Although this protocol relates in the main to corporate records there is supporting guidance regarding electronic clinical documentation – please see section 11 below.

1.6 This procedure document should be read in conjunction with the Trust's Records Management Policy, which is available on the Pennine Care NHS Foundation Trust Intranet (CO20).

2. SCOPE

2.1 This guidance relates to all corporate operational records held in paper or electronic format by the Trust. Operational records are defined as information created or received in the course of Trust business and captured in readable form in any medium, providing evidence of the functions, activities and transactions. They include:

- Text-based word-processed documents;
- Spreadsheets;
- Presentations;
- Microform (i.e. fiche/film);
- Digital Audio and video, cassettes;
- Computerised records;
- Scanned images;
- Photographs, slides and other images;
- Email messages;
- Website (hypertext) documents;
- Multimedia documents;
- Faxed messages;

This list is not exhaustive.

2.2 All records created in the course of the business of Pennine Care NHS Foundation Trust are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This includes email messages and other electronic records. (For advice on the management and storage of email see the Email Policy (CO6) located on the Trust's intranet).

2.3 While paper is still the most common storage method for records, usually within paper-based filing systems, electronic media are increasingly used to create documents. Well-managed electronic records are a vital part of our organisation's information resources. As much as paper records, they enable an organisation to retain a corporate memory of its various activities, provide an auditable trail of transactions, demonstrate accountability for actions, and fulfil its obligations under the Public Records Acts.

2.4 Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record.

3. MANAGEMENT OF CORPORATE RECORDS

3.1 It is the aim of this protocol to provide best practice in the management of corporate records which has three main functions: business purposes, accountability and cultural purposes and which will allow staff to:

- Create and maintain records in accordance with the purposes of the directorate / service they serve;
- Classify the records in accordance with the purpose for which they are created and maintain an index of all records created;
- Ensure the records are kept up to date and that all filing is carried out expeditiously to ensure the records are contemporaneous;
- Link all paper records to the electronic record created in the department to ensure that access to both types of records is seamless;
- Monitor all records in use and identify when they become inactive and are ready for secondary storage;
- Ensure all inactive or closed files are annotated with a destruction date in accordance with the NHS Records Management Code of Practice for Health & Social Care 2016;
- Remove inactive or closed files to secondary storage;
- Ensure that all records which have an accountability function e.g. Board Minutes are preserved according to the Retention Schedule (CO98).

4. CREATING A CORPORATE RECORD

4.1 Corporate records are created to ensure that information is available within the Trust: -

- To support day to day business which underpins delivery of care;
- To support sound administrative and managerial decision making;
- To meet legal requirements, including requests from patients under access to health records legislation;
- To assist internal and external audits;
- Whenever and wherever there is a justified need for information, and in whatever media it is required.

4.2 Each department/service should have in place a process for documenting it's activities in respect of records management. Records of operational activities should be complete and accurate in order to allow employees and their successors to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of the Trust by anyone so authorised, to protect the legal and other rights of the Trust, patients, staff and any other people affected by its actions, and provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

4.3 Records created by the Trust should be arranged in a record-keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information.

4.4 Network users should always store electronic documents on the shared network drive or the personal network drive as they are secure and backed up by the ICT Department on a nightly basis. The personal network drive is a private storage area on the network file server and can be used to store information that is not needed to be shared with colleagues and the shared network drive should be used for storage of work files that need to be shared for business continuity between multiple users such as functions, departments or services. Staff are not permitted to save documents on their hard drive.

5. COMMON TYPES OF RECORDS

5.1 The Trust generates many records of the same type, even though they may be stored in a variety of locations. Time spent on producing records can be minimised if staff use the corporate templates for core record types (available on the intranet, see trust stationary & templates).

5.2 In addition, templates for common record types help guarantee the right information is documented and that it is presented in accordance with expected corporate identity, regardless of who is creating the record. They ensure accurate and consistent information is captured and presented in meaningful ways.

5.3 Examples of common sets of records that are ideal for templates are:

- Minutes, agendas, policies, reports, guidelines, correspondence, cover sheets, memorandums, invoices, etc.

5.4 Corporate identity is important to validate business and evidence so when using Trust logo's, icons, it is important to ensure it is appropriate use and contemporary; if ever unsure check with the Trust Communications Team.

6. CORPORATE FILING / INDEXING SYSTEMS

6.1 FILING STRUCTURE

There needs to be some corporate filing structure both in paper and electronic filing systems in place to prevent the loss of records and to facilitate access. This filing system through the use of naming conventions, provide the means by which individual documents are held in meaningful record collections and indicate the sequence of events amongst the documents, establishing a narrative of events.

6.2. RECORDS AND METADATA

Record keeping systems must have a means of physically arranging or organising records. This is often referred to as a file plan or by the technical name of a business classification scheme. The scheme can be designed along several lines for example:

- Function (recommended) e.g. Finance
- Hierarchy/organisation e.g. Financial Accounts
- Hybrid function/hierarchy e.g. Community Services
- Subject/thematic e.g. Accounts Payable

The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems. When the recommended functional classification has been selected, the scheme can be further refined to produce a classification tree based on function, activity and transaction.

Personal names **should not** be used. Correct naming conventions enable business continuity especially when considering electronic records.

6.3 NAMING CONVENTIONS

Naming conventions provide a set of rules, which assist the individual end user in allocating a framework for the naming of folders that hold a group of documents.

Naming conventions for record titles should aim to:

- Give a unique title to each record

- Give a meaningful title which closely reflects the records contents
- Express elements of the title in a structured and predictable order
- Locate the most specific information at the beginning of the title and the most general at the end
- Give a similarly structured and worded title to records which are linked (e.g. an earlier and a later version)

7. DECLARING A RECORD

7.1 Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This process is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.

7.2 Some activity will be predefined as a record that needs to be kept, such as clinical records. Other records will need to fulfil criteria as being worth keeping, such as unique instances of a business document or email. Key legislation, such as the Data Protection Act (DPA) or Freedom of Information Act (FOIA), applies to all recorded information of the types covered by these Acts, whether declared as a formal record or not.

7.3 Declaration makes it easier to manage information in accordance with the legislation and business need. Accumulations of informal recorded information should be minimised as they will rarely meet these requirements.

7.4 It is harder to manage records over their lifecycle if they clutter up the folders or the workspace used on a daily basis or they are held in personal systems where only one person can access them. Just as a paper file was once closed when full or it ran over into the following year's business cycle, electronic information should also be closed off and filed in a place that does not clutter up the current business such as an archive folder.

8. MANAGING VERSIONS

8.1 To remain an authentic representation of events, once declared a record, a document should not be capable of being changed.

8.2 After a document is stabilised as a record, the ability to edit and make changes to the document should be prevented, as far as is possible within the available technology e.g. approved policies are held in portable document format (pdf) format on the Trust's intranet.

8.3 New and related versions of the record can be created by making and editing a copy, and saving this as a new record; e.g. it may be appropriate to retain various versions of a document as it passes through draft to finalisation. The record-keeping system should be capable of linking together versions of the same record, either automatically by the system or through the use of strict naming conventions, to ensure that the latest

version is retrieved by a user search. The user should be aware that earlier versions of the record exist in the system.

8.4 Filing of the primary corporate record should be on the shared network drive.

8.5 An audit trail should be kept recording significant actions which have been taken on a record, including the date of the action and identification of the individual responsible. Actions taken should include:

- Any changes which affect the status of the record as a reliable record
- Any change to the description of the record
- Copies of the record to create a new version

9. ELECTRONIC PENNINE CARE CLINICAL DOCUMENTATION

The shared drive (G Drive) should not be used as a complete electronic patient record.

Although points 3 – 8 listed above relate to documents that have become records and are therefore have corporate ownership, below is guidance relating to clinical documents which can be typed electronically but which should not become 'records' i.e. should not be kept on the pc for longer than is necessary.

These electronic documents may be used as long as the following guidelines are adhered to:

- Save electronically person identifiable data for example: clinic letters onto the shared network drive.
- Do not save any person identifiable data to the hard drive (desktop) as this is not secure.
- Do not save any patient information onto the personal network drive even if the individual is on the person's caseload. This is so that other team members can carry on with patient care if the staff member is absent from work.
- Do not copy and paste clinical information from one review / care plan etc to another as this can leads to incidents where another clients name is copied and pasted into the wrong document.
- The naming convention of the files should be Surname / Forename / Identifier (NHS Number).
- If a paper record is being maintained then a copy will need to be printed and retained in the client's records.

10. SECURITY & STORAGE

10.1 The Trust must safeguard it's records in whichever format to ensure that individuals do not alter, erase or in any way change the content of the record for fraudulent purposes and that transactions can be audited.

10.2 Corporate Services should keep their paper records safe and secure and dependent on the sensitivity of the records in a locked filing cabinet in a locked room.

10.3 Departments must also guard against storage media deterioration and rapid technology changes that can leave electronic records inaccessible over a period of time because of hardware or software obsolescence.

10.4 To eliminate the possibility of creating a situation where information can no longer be retrieved, each department must ensure IT makes provision for future accessibility by migrating all electronic records, when there are major changes to the next generation of hardware or software.

10.5 Different backup media (floppy diskettes, CDs, DVDs, reels, cassettes, optical disks, and microfiche) retain information for different periods of time before deterioration of the information may begin. The longer the backup media is retained without replacement of information, the more stable the backup media needs to be. This media technology creep endangers the accessibility, usability, and readability of the Trust's information;

10.6 Whenever new databases and automated systems are designed or purchased, appropriate care should be taken to determine whether and what records should be created by the system.

10.7 For existing electronic systems and databases it is important to ensure that information is kept and readable for as long as required. This may entail the migration of data when new systems are introduced.

11. APPRAISAL

11.1 The process of deciding what to do with records when their business use has ceased is called appraisal. This is defined in the Retention Schedule and any decisions must be auditable and linked to a mandate to act, derived from the Board. No record or series can be automatically destroyed or deleted. There will be one of three outcomes from appraisal:

- Destroy / delete
- To keep for a longer period
- To transfer to a place of deposit (PoD) appointed under the Public Records Act 1958.

11.2 There are also a number of other records which may be of interest to a local PoD. Appraisal may also result in a record being retained for longer.

11.3 If as a result of appraisal, a decision is made to destroy a record there must be evidence of the decision.

11.4 Records selected as a result of an appraisal may also have security classifications applied which may continue to exempt them from FOI requests or disclosure after transfer to a place of deposit. Records transferred to a place of deposit, such as unpublished board papers, may continue to be subject to FOIA exemptions on public access following transfer.

11.5 Electronic records can be appraised if they are arranged in an organised filing system which can differentiate the year the records were created and the subject of the record. If electronic records have been organised in an effective file plan or an electronic record keeping system, this process will be made much easier. Decisions can then be applied to an entire class of records rather than reviewing each record in turn.

12. RETENTION

12.1 The length of the retention period depends upon the type of record and its importance to the business of the Trust. The destruction of records is an irreversible act, whilst the cost of keeping them can be high and continuing.

12.2 The Guidance for the Retention of all Clinical and Corporate Records (CO98) lists the retention periods approved by the Information Governance Assurance Group (IGAG). If a particular record is not listed within the appendix, advice must be sought from the Records Manager who will establish the retention period in consultation with the Information Asset Manager and the department concerned.

12.3 Where the record in question is a Trust-wide document, the retention period will need to be approved by IGAG. All new retention periods agreed will be added to the policy when it is reviewed.

12.4. The Trust holds the majority of the Corporate records in the Corporate Records store at Birch Hill, Rochdale. The procedure for sending records to this facility can be found in Appendix 1. If this facility is full or if the Records Manager decides some corporate records may be sent to our offsite storage provider, however a full inventory will be kept as to the location of these records.

13. DESTRUCTION

13.1 **Paper:** paper records can be destroyed to an international standard. They can put in the red confidential waste bins, incinerated or shredded (using a cross cut shredder) under confidential conditions. Do not use the domestic waste or put them on a rubbish tip, because they remain accessible to anyone who finds them. The relevant standard for destruction in all formats is BSIA EN15713:2009 - Secure Destruction of Confidential Material[1]

[1] BSIA EN15713:2009 - http://www.bsia.co.uk/Portals/4/Publications/form_204_id_en15713.pdf

13.2 **Electronic**: destruction of digital information is more challenging. Records management is concerned with accounting for information so any destruction of hard assets, like computers and hard drives and backup tapes, must be auditable in respect of the information they hold. An electronic records management system will retain a metadata stub which will show what has been destroyed. At present there are two ways of permanently destroying digital information and these are either: overwriting the media a sufficient number of times or the physical destruction of the media.

13.3 If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process completed.

14. SPECIFIC TYPES OF RECORDS

14.1 HR RECORDS

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the paperwork collected through the recruitment process and this will include the job advert, application form, right to work, identity checks and any correspondence relating to acceptance of the contract. The central file must be the repository for this information.

It is common practice for the line manager to hold staff records which can contain large portions of an employee's employment history (for example training records). This practice runs the risk of much of the employment record being lost if there is an internal move of the employee or upon termination of contact. It is important that there is a single record of the employment of an employee and therefore records should follow the employee.

Upon termination of contract, records must be held up to and beyond their statutory retirement age. To reduce the burden of storage and for reasons of confidentiality it is recommended that a summary be prepared and held until the employee's 75th birthday or 6 years after leaving whichever is the longer and then reviewed. Where a summary is made it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- Professional training history and professional qualifications related to the delivery of care
- List of buildings where the member of staff worked and the dates worked in each location.

Disciplinary warnings can be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record.

Employee relations case files will be stored until the employee's 75th birthday; however once a disciplinary warning has expired the case file can no longer be referred to.

All personnel files must be kept in a lockable cabinet, which is kept locked at all times when not in immediate use.

Access is to be restricted to managers only, who should hold the keys to the cabinet. Access might also be permitted to other named individuals, such as deputies or secretaries when there is a reason for this access.

Information from an individual's personnel file should not be disclosed to a third party, except where the third party is in a direct line management relationship with the individual, without the permission of the individual, including references.

Any members of staff wishing to access their own personnel file must do so in accordance with the Data Protection Policy (CO59).

There is no definitive list of what should be held in a personnel file, however, examples of appropriate contents include:

a) Application Form or Curriculum Vitae (CV)
b) References
c) Pre-employment checks / registration confirmation
d) Letters of Appointment
e) Contract of Employment
f) Employee / assignment number
g) Paybands
h) Local Induction Forms
i) Registration Authority Forms
j) Study Leave applications
k) Training Records
l) Job Description
m) IPDR / Quarterly review forms
n) Return to work Interviews
o) Copies of relevant correspondence sent to the individual e.g. letters of praise etc
p) Timesheets, duty rosters etc
q) Flexible working applications
r) Applications for special leave
s) Building or sites worked at
t) Reasons for leaving

Personnel files must be accurately maintained and updated. This is the responsibility of the holding manager or the HR Department depending

where the files are held. It is essential that all files are well maintained and records kept of matters relating to each individual. The manager will review personnel files at least once a year.

The movement and location of personnel files within the HR systems will be controlled by tracer card (see Appendix 6) or book to ensure that:

- A p file can be easily retrieved at any time
- There is an auditable trail of the movement of the p file

If the personnel file cannot be located the Missing Record Procedure (CO28) must be completed.

Leaver's Files

It is the responsibility of the Manager to:

- Send or deliver securely all leavers' files to the HR Department, Birch Hill ***within one month*** of the employee leaving – please see Appendix 2

- Send or deliver securely an individual's file to the new line manager when an individual transfers within the Trust ***within one month*** of the date of transfer using tamper proof envelopes

The archiving procedure for HR records can be found in Appendix 2. The box label can be found in Appendix 7.

14.1.1. Safe Transportation of HR Records

- If HR records are being delivered to another location they should be enclosed in tamper proof envelopes or satchels and sealed for transfer.
- The procedure and associated forms for sending HR records externally by Royal Mail Special Delivery or by secure courier can be found in Appendices 3 - 5.
- For larger quantities, HR records should be boxed in suitable boxes or containers for their protection. All archive boxes should be labelled with a list of contents and destruction year.
- Each tamper proof envelope should be addressed clearly and marked confidential with the senders name and address on the reverse of the envelope.
- If HR records are to be transported via secure couriers; only contracted couriers should be used, who have agreed to the information governance arrangements around Data Protection. A signature should be obtained on collection & delivery of HR records (please see Appendix 5)
- ***Taxi's should not be used to transport HR records.***
- Common sense in relation to the security of HR records should be used when taking them off-site. Consideration should be given to storing the HR records safely within your vehicle so that they cannot be seen. Try to plan your journey so that HR records are not left unattended however, if this is

unavoidable they must be secured within the vehicle e.g. locked in the boot.

- **HR records/ person identifiable information must not be left in the vehicle overnight.**
- When travelling on public transport paper HR records must be stored out of sight, in a suitable secure bag and must be closely monitored.
- HR records should be carried in an appropriate case and not carried 'loosely', as this increases the risk of dropping the record and losing some of the contents.
- HR records / reports / letters should be kept in a sealed envelope or tamper proof bag and marked 'private and confidential'.

14.2 ELECTRONIC MAIL AND RECORD KEEPING IMPLICATIONS

Electronic Mail (Email) should also be viewed as a record as it has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. Please refer to the Electronic Mail Policy (CO6).

A common problem with Email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates.

Where Email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record. Where email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral - for example an email approving a business case must be saved with the business case file.

Automatic deletion of Email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation. Legal holds can take many forms and records cannot be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This may include national or local inquiries, criminal investigation, and expected cases of litigation or records that may be requested under FOI or subject access.

This means that no records can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a place of deposit.

The NHS mail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation another NHS organisation, they must

ensure that no sensitive personal data relating to the former organisation is transferred.

It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of security classified information. This is facilitated by staff storing only those emails that need to be retained on an ongoing basis. Emails that are the sole record of an event or issue, for example an exchange between a clinician and a patient, should be copied in to the relevant clinical record rather than being simply deleted.

14.3 RECORDS CREATED VIA SOCIAL MEDIA

Where social media is used as a means of communicating information for business purposes or it is a means of interacting with clients, it may be a record that needs to be kept. Where this is the case, information must be retained within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription or periodic storage.

14.4 RECORDS CREATED THROUGH BRING YOUR OWN DEVICE (BYOD)

Any record that is created in the context of health and social care business is the intellectual property of the employing organisation and this extends to information created on personally owned computers and equipment. This in turn extends to emails and text messages sent in the course of business on personally owned devices from personal accounts. They must be captured in the record keeping system if they are considered to fall within the definition of a record.
When an individual staff member no longer works for the employing organisation, any information that staff take away could be a risk to the organisation. If this includes sensitive personal data, this is reportable to the Information Commissioner's Office (ICO) and may be a breach of confidentiality. For this reason it is not permitted to store patient confidential insecure device or system that does not meet national requirements.

14.5 WEBSITE AS A BUSINESS RECORD

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively.

A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate, or some other method to recreate what the website or intranet visitor viewed.

14.6 CLOUD BASED RECORDS

Use of cloud based solutions for health and social care are increasingly being considered as an alternative to managing large networks and infrastructure. Before any cloud based solution is implemented there are a number of records considerations that must be addressed. The ICO has guidance on cloud storage they also advise to conduct a privacy impact assessment for any potential cloud solutions.

The NHS has a prohibition on storing patient identifiable data outside of England where there is any link to national systems or applications (e.g. N3 or NHSmail), so any solution must have servers that can be traced to England if it is going to be used to store patient data.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records, including all the formats, onto another solution and this may be technically challenging.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever increasing storage instead of good records management will not meet the records management recommendations of this Code.

Where personal data is stored there is also the risk of breaching the requirements of the DPA not to store personal information longer than necessary.

15. RECORDS MANAGEMENT AUDIT AND MONITORING

15.1 An annual audit will be carried out in line with the Information Governance Toolkit in conjunction with the Asset Register. This will involve knowing what series of records are held by business areas and their named asset owners, managers and administrators. This audit also examines the process for retaining and disposing of records in line with the retention periods.

15.2 The Information Governance Assurance Group (IGAG) is also responsible for the review of results for this audit and the subsequent development and monitoring of action plans. The divisional business units are responsible for implementing the action plans.

16. REVIEW

16.1 This protocol will be reviewed by the Records Manager(s) every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).

16.2 Any revisions of this protocol will need to be approved by IGAG and will be ratified by the Executive Directors.

17. ASSOCIATED POLICIES

Associated Policies, Protocols and Procedures

CO4 - Confidentiality Policy

CO6 – Electronic Mail Policy

CO10 - Incident Reporting, Management & Investigation Policy

CO11 - Information Security Policy

CO13 - Information Sharing Policy

CO27 - Freedom of Information Act Policy

CO28 - Missing Records Procedure

CO44- Information Governance Policy

CO51- Electronic transfer of Person Identifiable Data Policy

CO59-Data Protection Policy

CO62- Records Management Moving Protocol

CO80- Placing a risk of violence marker on electronic and paper records

CO98 Guidance for the retention of clinical and corporate records

HR43 - Induction Policy

Appendix 1

PROCEDURE FOR SENDING CORPORATE RECORDS TO THE ONSITE ARCHIVING FACILITY, @ BIRCH HILL, ROCHDALE

All staff are reminded that:

- All records have a value and are required to be retained in accordance with the Records Management Code of Practice for Health and Social Care 2016: http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf
- The Records Manager has identified priority areas for the Trust and no records should be sent without prior agreement.
- All archived records must be clearly labelled for example, “Box Number, Finance Records, Budget Statements 2016”
- All archived records must have a clear destruction date in accordance with the Retention & Disposal Schedules outlined in CO98 Records Retention Policy.
- All archived records must have a full inventory made with a copy enclosed in the Archive Box and a copy retained by the owner and a copy given to the Task Force Officer to allow them to request retrieval of the records.
- For health & safety reasons all archived boxes should be of a size and weight which can be moved and carried by a member of staff.
- Once the boxes have been packed and labelled the department must contact the Task Force Officer (details below) to arrange safe transportation

For advice: Please contact Gillian Saldanha De Magalhaes, Task Force Officer on 0161 716 3268 or Gillian.SaldanhaDeMagalhaes@nhs.net or the Archiving Records Team on 0161 716 3264 / 3265 or art.helpdesk@nhs.net

Retrieval Process

If a file or a box needs to be retrieved from the Corporate Records Store the Task Force Officer should be contacted by email or telephone 0161 716 3268 or email (as above). The Records Department holds a central index of records by department and box contents and can identify in which room the box and its contents can be located. If available the Task Force Officer will travel to Birch Hill to retrieve either the box or a file or will accompany a member of staff. The Corporate Records store is accessible via a lift which is secured by a key. The Task Force Officer holds the key to the lift. If the records are located in one of the rooms the key pad code is also held by the Task Force Officer.

For retrieval of HR Records, please see the HR Archiving Procedure.

If a box is removed from the store then the Task Force Officer needs to be informed in order to update the central index.

Emergency Process

If the Task Force Officer or Records Manager is not available the key to the lift is available from the Porters Office in Rochdale. The Porters should be contacted in advance on 07825 735344. The key pad codes are available from the Archiving Records Team by email: art.helpdesk@nhs.net and they can be contacted on 0161 716 3264/ 3265. HR can be contacted regarding HR records by email: tracy.mellor1@nhs.net .

Retention

The records remain the responsibility of the department and these should be annually appraised and culled in accordance with the Retention & Disposal Schedule outlined in CO98 Records Retention Policy on an annual basis. Any records that exceed the retention period and are no longer required should be confidentially disposed of using the confidential waste bags and sealed. The porters should be informed if there are any confidential waste bags that would need collecting for incineration. The Task Force Officer should be informed if any boxes are disposed of so that the central index can be maintained.

Appendix 2

HR Department Archiving Process

Staff leaver's personnel files or casework files are covered in the following archiving process. Within one month of leaving the leaver's file should be sent securely to the HR Department. They will then be sent to the Corporate Records store at Birch Hill Hospital, Rochdale initially for sorting into year of retention before being archived at our off-site storage provider.

How to archive HR files

- Ensure everything is securely fastened into the file.
- Ensure the employees name is visible on the outside of the file.
- Ensure that the employee's date of birth is written clearly on the front of the file (dd/mm/yy) on the top right hand corner of the file. Personnel records are retained in line with the NHS Records Management Code of Practice and currently the retention period is the 75th birthday of the individual. This means that the records at Birch Hill will be catalogued in date of birth order for archiving.
- For case files if the employees DOB is not found, after all avenues have been exhausted, write the start date of the case in the top right hand of the corner and the destruction date will be gained from that date.
- Pack the files into a secure box or tamper proof envelope (suitable for personal data being transported).
- List the box contents onto the 'archive BHIL' spreadsheet kept in the Archiving folder in G drive or download it from the Records Management Intranet homepage.
- Select a delivery date for drop off to the archives from the available dates (one day per month). Notification of delivery to the archives on that date is not necessary (but preferable). The archiving spreadsheet must be submitted electronically and a copy be placed in the boxes as an audit trail of what has been moved to archives in case the file is required at a later date.

- Save the spreadsheet in the Archiving folder corresponding to the date of delivery to Birch Hill. Files can be traced back to when they were moved from the Divisional Business Unit (DBU) and put into Birch Hill archives using this process.

- Any files that are listed on the completed spreadsheets will be assumed in the archives, if there is no record of the date they were accepted into archives it will be assumed that the file is still with the manager in the DBU.

- To retrieve a file from the Archives department initially email: tracy.mellor1@nhs.net with the completed 'Retrieval request corporate' spreadsheet which can be found on the Records Management Homepage If the file is located at Birch Hill it will be retrieved and sent back to you.

  If the file has already been archived off site you will be notified and your retrieval will then need to be initiated through the archiving records team using the 'Retrieval request corporate' spreadsheet and emailing it to art.helpdesk@nhs.net.

Appendix 3

FOR INTERNAL USE ONLY

CONFIDENTIAL/SENSITIVE DATA MAIL FOR HAND DELIVERY VIA THE INTERNAL POSTAL ROUTE i.e., Borough to Borough.

Please complete this form for any mail to be hand delivered within the internal postal route by the Trust HQ Postman *(the form should be stapled to the envelope/parcel)*

REQUESTED BY: ……..(Please print name)

Tamper proof envelope code no(s).	
Contents: e.g. health record / HR record, identifier and volume (DO NOT USE PATIENT INDENTIFIABLE INFORMATION)	
Delivery location:	

Signature on collection:		
Print name:		***Date***

Signature on delivery:		
Print name:		***Date***

Appendix 4

HEALTH RECORDS TO BE DELIVERED VIA ROYAL MAIL SPECIAL DELIVERY

Contact Name: …….. Tel No. ……

Job Title: ……Location: ……..

……

Signature:…… Date: ……

FOR DELIVERY TO:

Name:
……

Full Address

……

……Postcode: ……

To arrive by 9am ☐

1pm ☐

Nb. If not ticked delivery by 1pm will be assumed

Tamper Proof Envelope code number	

Cost of postage: …… **SD1**

Appendix 5

ECORDS FOR HAND DELIVERY VIA COURIER SERVICE

Date:

Pickup and delivery: Urgent (immediately) ☐
Same day (between 5.30am and 9.00pm) ☐
Within 24 hours (from receipt of form) ☐

PICK UP ADDRESS (***please give FULL address,*** *including postcode****)***

……

……. Closing time of pick up point ……

Contact Name: …… Tel No. ……At pick up point

Contact Name: …….. Date: ……Of person booking

Signature: …… Date: …….

Booking area : Healthy Young Minds ☐ Drug & Alcohol Team ☐ Forensic and High Support ☐ Trust HQ ☐ Bury ☐ Oldham ☐ Rochdale ☐ Stockport ☐ Tameside ☐

Signature of Courier: …… Job no. ……..

(provided by Courier)

Date and time of pickup: ……

FOR DELIVERY TO:

Name: ……Tel No. ……

Full Address
……

……Postcode: ……

Closing time of delivery address: ……

No of parcels/boxes	
Cost (given by courier)	
Tamper Proof Envelope code number	

SAMEDAY PLC COURIERS 0800 338888 CS1

Appendix 6

Tracer card

(can be used for health or personnel records)

Surname:	**Forename:**	**Date of birth:**	**NHS or Employee Number:**
Volume Number:			

Taken / requested by (name and contact no.)	**Destination**	**Purpose**	**Method of transportation i.e. self, courier, royal mail**	**Date Out**	**Date returned**

Appendix 7

ARCHIVED STORAGE	
Department Name:	**Date of Destruction:**

Contents:

Ref no.	**Description**
……	……
……	……
……	……
……	……