Acacium Group

Health Records Management Policy

Policy Reference | CLIN 14

Version | V3.1

Policy Name	Health Records Management Policy
Purpose of Document	To inform. all Acacium Group workers of their responsibilities and the standards required in regard to managing records to ensure compliance with national, and Acacium Group policy.
Target Audience	All Acacium Group workers.
Version	V3.1
Author	Karen Matthews-Shard
Date of Approval	November 2011
Published Date	December 2011
Lead Director	Karen Matthews-Shard
Review Frequency	3 Yearly
Last Reviewed	March 2024
Next Review Date	March 2027
Risk and Resource Implications	Resource: Training
Associated Strategies and SOPs	CLIN 06 Consent Policy CLIN 08 Safeguarding Children Policy CLIN 09 Safeguarding Vulnerable Adults Policy CORP03 Whistleblowing for Internal Employees Policy CORP04 Whistleblowing for Associate Workers and External Parties Policy CORP10 Policy on Policies Policy CORP14 Complaint Report Policy ORG 04 Incident Reporting Policy
Equality Impact Assessment (EIA) Form	Acacium Group is committed to Equality, Diversity and Inclusion and in line with our values, we strive to ensure that everyone that is part of the Acacium community is not disadvantaged or discriminated against given their individual need or characteristics. To support this, an Equality Impact Assessment has been undertaken on this policy/procedure. This information is held centrally and can be requested from the Clinical Governance Team.
About Acacium Group	Details of all Acacium Group trading companies that this policy applies to are detailed within Appendix A
Legislation	Legislation and Guidance pertinent to this policy can be found within Appendix B

Document History			
Version	Date	Changes made/comments	By whom
Draft v 1	Sept 2011	First draft.	K. Matthews- Shard
Draft v 2	Nov 2011	Included the management of staff records.	K. Matthews- Shard
V1	Mar 2013	Annual review.	KNF/KMS
V1	May 2014	Annual review.	KNF/KMS
V1	Apr 2016	Annual review V1.	KNF/TJ
V1.1	Jan 2017	Implementation of new policy template.	KNF/SJ
V1.1	Jun 2017	Annual review.	KNF/VM
V2	Nov 2017	Updated to include new TCS bio brand description page.	LB/MS
V2	Mar 2018	Updated front sheet to include new review frequency date.	KMS/MS
V2.1	Apr 2019	Implementation of new Policy template	CCR/KG
V2.2	Dec 2019	Frequency amendment and update to brand information	KG
V2.3	Oct 2020	Update re Rebrand	CCR/CC
V2.4	Jan 2021	Update re Rebrand 2	CC
V2.5	Feb 2021	Clinical Advisory Group Review	CAG
V2.6	Apr 2021	Added CHS brand	CC
V3.0	Jan 2024	Rebrand	Clinical Advisory Group
V3.1	Mar 2024	Reviewed and updated	Clinical Advisory Group

Table of Contents

1. Introduction 5
2. Definitions 5
3. Roles & Responsibilities 6
4. Records Management Best Practice 7
5. Best Practice: Disclosure 9
6. Best Practice: Closure and Transfer of Records 10
7. Best Practice: Storage of Records 11
8. Best Practice: Archiving Records 12
9. Best Practice: Disposal of Records 14
10. Access to Records of the Deceased 14
11. Record Keeping 15
12. Confidentiality 17
13. Training 17
14. Implementation Plan 17
15. Associated Policies / SOPs 18
16. References 18
Appendix A: About Acacium Group 20
Appendix B: Legislation 21
Appendix C: Minimum Time to Retain Health Records 25
Appendix D: Filing ad Retrieving Records 28
Appendix E: Disclosure Model 30
Appendix F: Request for Information 33
Appendix G: Record of Disclosures 34
Appendix H: Principles of Good Record Keeping 35
Appendix I: Information Governance Toolkit 36
Appendix J: Records Inventory 37
Appendix K: Record Log Out Form 38

1. Introduction

1.1 Acacium Group has a systematic and planned approach to the management of all records. This system ensures that:

- from the time a record is created, until its ultimate disposal, the control of both the quality and quantity of information is contained
- the maintenance of information is effective and serves the needs of the organisation, its service user (inclusive of service user /patient) and its workers. This information must also be compliant with appropriate legislation.

1.2 Health records created by Acacium Group are an essential part of its corporate memory. These records provide evidence of actions and decisions, support daily functions, operations, policy formation and managerial decision making. In so doing, it protects the interests of Acacium Group and the needs of the service users, and workers.

1.3 Acacium Group believes that every service user has the right to have all of the information held about them to be kept securely. All of the information held must be accurate and only used by those who have a genuine need to access it. service user's records must be disposed of in accordance with national policies, procedures and monitoring requirements.

2. Definitions

Term	Definition
Records management	Is an administrative system of controlling records that meets legal requirements and includes: • the creation of a record • version control • distribution of records • filing records • archiving records • storage and disposal of records • preserving an appropriate historical record. The key components of record management are: • record creation • record keeping • record maintenance (including tracking of record movements) • access and disclosure (information sharing) • closure and transfer • appraisal (review to decide next action with records) • archiving • disposal.
Records	Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business.
Health Records	Consists of data concerning health has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.
Electronic health records	All records appertaining to a service user and their health, or care, needs that are held on a computer, laptop, netbook, PDA, memory device, or any other electronic device.
Paper health records	All records appertaining to a service user and their health, or care, needs that are documented on any piece of paper.

Service user identifiable information (personal information)	Information such as: • the service user's name • address and full post code • date of birth • pictures • photographs • videos, audio-tapes or other images of service user s • NHS number • local service user identifiable codes • anything else that may be used to identify a service user directly or indirectly. For example, rare diseases, drug treatments or statistical analysis.
Anonymised information	Information which does not identify an individual directly, and which cannot reasonably be used to determine their identity.
Anonymisation	Is the removal of name, address, full post code and any other detail, or combination of details, that might support identification.
Pseudonymised information	Similar to anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key, or index.
Pseudonymisation	Allows information about the same individual to be linked in a way that true anonymisation does not.
Information sharing protocols	Documented rules and procedures for the disclosure and use of service user information, which specifically relate to security, confidentiality and data destruction, between two or more organisations, or agencies.
Disclosure	Divulging or provision of access to data.
Public interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader social interest.

3. Roles & Responsibilities

3.1 The overall organisational roles and responsibilities are set out in the policy document, CORP 10 Policy on Policies for Drafting, Approval and Review of Policies and SOPs.

3.2 Acacium Group acknowledges that the management of records is the responsibility of all its workers. The following table outlines the responsibilities of the key people involved in the effective reporting and management of complaints.

Job Title	Responsibilities
Clinical Director / Caldicott Guardian	The Clinical Director is the responsible director for records management and, therefore, acts as the Caldicott Guardian. The Clinical Director ensures that policy, standard operating procedures (SOPs), protocols, training, and competencies, are in place to support the vital aspect that effective health records management contributes to the organisation. The role of the Caldicott Guardian is to reflect the interests of service user s' regarding the use of their personally identifiable information, ensuring that it is shared in an appropriate and secure manner.

Clinical Governance Manager	Supports the Clinical Director / Caldicott Guardian in the effective management of health records. Is responsible for: • logging of records removed • archiving and disposal of records • maintaining a register of all records held by the organisation • the person who receives Freedom of Information Act (FOIA) requests.
Line Managers / appropriate others	Ensure that health records management is identified in appraisal and Personal Development Plans.
Individual workers	• promote the confidentiality of service user information whilst supporting the need for information sharing where appropriate • comply with any records management policies set by their professional regulatory body • seek agreement from the Caldicott Guardian on the use of service user personally identifiable information including how to share information and if the information is to be used for data analysis • maintain accurate, comprehensive and legible records • store records securely in line with local guidance. • Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC) or Social Work England will be required to adhere to record keeping standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies.
Clinical Advisory Group (CAG)	Review polices associated documents and training content for the Group. To support high clinical standards and quality improvement agendas in line with the Groups vision, strategic aims

3.3 Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC) or Social Work England will be required to adhere to record keeping standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies.

4. Records Management Best Practice

4.1 Assessment of risk

4.1.1 Assessment of risk and planning are integral to safe, and effective, use of health records and Acacium Group workers will be expected to contribute to these processes. The Clinical Director must be informed in the event of risks to the organisation involving records management, so that they are monitored via the risk management process.

4.2 Aims of records management

4.2.1 The aims of good health record management are:

- they are available when needed
- they can be readily accessed
- they can be interpreted accurately
- health records can be trusted
- they can be maintained through time
- they are secure from authorised or unauthorised alteration, erasure, or access, while disclosure is properly controlled
- they are retained and disposed of appropriately
- workers are trained and made aware of their responsibilities.

4.3 Records maintenance

4.3.1 The fact that health records are kept will be registered on a central register held by the Quality Compliance Manager. Individual records will not need to be registered. When health records are transferred from Acacium Group to other care providers, the worker transferring the information will inform the Quality Compliance Manager so that a central record of the transfer may be made.

4.4 Access and disclosure (information sharing)

4.4.1 When any information is disclosed, receipts for the information given must be requested and obtained. Before disclosing any information, the information request must be validated. It is important to find out who is asking for the information, their designation, what they want and why. This may be provided by email, fax, or letter, but information should not be released until this has been completed and Acacium Group is satisfied that the information request is genuine and does not contravene national or Acacium Group policy.

4.4.2 Do not access the records of any service user, or their family, to find out personal information that is not relevant to their care.

4.5 Service user understanding of how their information is used

4.5.1 It is extremely important that service users are made aware of the following:

- information disclosures that must take place in order to provide them with high quality care i.e. their involvement in clinical audit
- the need to share information between members of care teams and between different organisations involved in healthcare provision, including if care is transferred to another care organisation
- upon completion of care, records will be returned to the rightful owner, such as, the organisation who commissioned the care. Alternatively, they may be retained by Acacium Group for several years, if required nationally, as detailed in Appendix D: The minimum time that Acacium Group is required to retain health records and the method of disposal
- their information may be used to benefit the healthcare of others, such as, when studies are undertaken by the NHS, local government organisations or public health departments
- that if information needs to be shared because of public interest the service user will not be asked to give consent
- their information may be used for statistical analysis and this may be anonymised or pseudonymised.

4.6 Informing service users about their rights when sharing information

4.6.1 The most effective way of informing service users about their rights is at the start of a contract, at which time all service users are given a copy of the 'Service users Guide'. This sets out how their information will be used.

4.7 Difficulties accessing records

4.7.1 If there is a problem relating to access or record keeping, such as, missing records or problems accessing records, then report the matter to the Line Manager / appropriate other. Keep a record of this action.

5. Best Practice: Disclosure

5.1 Service user's right to decline disclosure

5.1.1 Service users have the right to object to the use and disclosure of confidential information that identifies them. Sometimes, if service users choose to prohibit information being disclosed to other health workers involved in providing care, it may mean that the care given will be limited. service users must be informed that their decisions about disclosure will have implications for the provision of care or treatment.

5.1.2 Special attention should be paid to the issues around child consent. For further information, see the Acacium Group Consent Policy.

5.1.3 Where the purpose of sharing information is not directly concerned with the healthcare of the service user, consent must not be assumed. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

5.2 Obtaining consent for disclosure of information

5.2.1 There are situations where consent cannot be obtained for the use or disclosure of service user identifiable information, yet the public good of this use outweighs issues of privacy. 'Section 60' of the Health and Social Care Act 2001 currently provides an interim power to ensure that service user identifiable information, needed to support a range of important work such as clinical audit, record validation, and research, can be used without the consent of the service user but he / she must be informed. Documentation of the consent, including the information given to enable the service user to reach their decision, must be documented in the service user's record.

5.3 When disclosure is required by law

5.3.1 Disclosure of healthcare records is required by law when a court of law requests them and when there is a coroner's case. The service user does not need to consent in these cases, but it is best practice to inform the service user or their next of kin before the release of the records. Care must be taken to only disclose what is in the terms of the court order and if Acacium Group feels that there are ethical concerns about what is requested, these should be raised with the court.

5.4 Disclosure to service users

5.4.1 Under the DPA 2018, principle 7, service users are able to gain access to their health records. At the point of care, health records are maintained in a service user's own home. Therefore, they are easily accessible to the service user. However, in the rare circumstances where this is not the case, Acacium Group is legally obliged to provide this information. It is best practice to provide copies rather than originals.

5.5 Disclosure of information to carers without parental consent

5.5.1 Carers often provide valuable healthcare and, subject to complying with the best practice outlined, every effort should be made to support and facilitate their work. Only information essential to a service user's care should be disclosed and the service user should be made aware that this is the case. However, the explicit consent of a competent service user is needed before disclosing information to a carer. The best interests of a service user who is not competent to consent may warrant disclosure. See also the Acacium Group Consent Policy.

5.6 Disclosure of information when handling complaints

5.6.1 Explicit consent is required from the service user to share their health records and personal information. See also the Acacium Group Reporting and Managing Complaints Policy.

5.7 Disclosure to the police

5.7.1 Whilst the police have no general right of access to health records there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure a legitimate function in the circumstances they cover. In the absence of a requirement to disclose there must be either explicit service user consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the courts.

5.7.2 Where disclosure is justified it should be limited to the minimum necessary to meet the need and the service user should be informed of the disclosure, unless it would defeat the purpose of the investigation or allow a potential criminal to escape or put Acacium Group workers or others at risk.

5.8 Disclosure to the media

5.8.1 Any request for disclosure of service user information to the media must be referred to the Clinical Director. There are generally no reasons why personal or health information should be shared with the media. However, there may be rare circumstances where this may be permissible. For instance, where a service user or their relatives are complaining to the media about the level of care given and the sharing of information facilitates understanding of the actual situation. Where practicable, explicit consent should be obtained from the service user.

5.9 Disclosure to solicitors

5.9.1 Solicitors may require health records for such things as compensation claims. Ideally, disclosure should be based only on the actual query. However, if disclosure of the whole record is required, this should be complied with as long as it is clear to the service user that the full record is required, and they have consented. In all cases, the service user must be informed of the disclosure.

5.10 Sharing without service user consent

5.10.1 There are circumstances when Acacium Group may share personal information about a service user without their consent. This is when circumstances dictate the need to protect the service user concerned, protect Acacium Group workers or assist the police with their investigations. Acacium Group will comply with any validated request to share information as long as the request complies with information governance and sharing policies, and agreement has been provided by the Acacium Group information management lead. Information will only be shared on a need to know basis. See also Appendix J: Information Governance Toolkit Commercial 3rd Party, version 8.

6. Best Practice: Closure and Transfer of Records

6.1 When the following occurs, the health records will either be closed or transferred:

- death of the service user, closure of record, storage or transfer to the commissioning organisation
- transfer to another care provider, transfer of record.

6.2 Closure

6.2.1 When records are closed i.e. made inactive and transferred to secondary storage, they should be moved as soon as they have ceased to be in active use other than for reference purposes. The Quality Compliance Manager will be requested to store the

information, either electronically or in hard copy. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the record of disposal. See Appendix E regarding storage.

6.3 Transfer of information

6.3.1 When health records are transferred from Acacium Group to other care providers, the Acacium Group worker transferring the information will inform the Quality Compliance Manager so that a central record of the transfer may be made. Health records are more often transferred with the service user or may be scanned, and transferred, via email or CD-ROM. Acacium Group must be sure of the arrangements for electronic security before transferring information by email. Where it is not possible to transfer information with the service user or secure email, transfer will be undertaken by courier or registered post. The records must be secure for the whole of the journey. The Quality Compliance Manager must be informed about all records transferred out, so that a record is maintained.

6.4 Transferring records

6.4.1 Put records in an unmarked envelope:

- secure them with a return name and address on the back
- mark the envelope, 'Private and Confidential'.

6.4.2 Transfer to the appropriate person or their representative and obtain a receipt. If sending by email, mark the email, 'High priority' and 'Confidential'. Ensure you password protect the attached documents. Request a delivered and read receipt and still ask for a written email confirming receipt of all records.

6.5 Transfer in (receipt of information)

6.5.1 In order to ensure quality of care, Acacium Group may require information to be sent to them from care providers who have provided care. The same principles of management must be provided and requested. Acacium Group will ensure that information is received into a safe area where access to service user information is restricted to those who need to know.

7. Best Practice: Storage of Records

7.1 Day to day management of healthcare records

7.1.1 Management of records in service user's home.

7.1.2 The service user's clinical records are almost always kept in the service user's home. It is the responsibility of the service user to ensure that records in the home are kept safe and secure, and free from loss or inappropriate use. Acacium Group workers may advise service users on how they think this could best be done and then comply with the requirements.

7.1.3 When Acacium Group workers are using the records they are responsible for the correct use of records according to policy at all times. Under no circumstances should records be removed from the service user's home, unless for reasons of transfer of healthcare, archiving of records or going on a trip with the service user. If records are to accompany the service user on a trip, they must be protected by being put in an unmarked envelope and kept with the service user at all times.

7.1.4 For all types of records i.e. Acacium Group workers in offices, where records may be seen. All workers must:

- shut / lock doors and cabinets as required
- wear Acacium Group ID
- query the status of strangers

- know who to tell if anything suspicious or worrying is noted
- not tell unauthorised personnel how the security systems operate
- not breach security themselves.

7.1.5 Manual records must be:

- formally booked out from their normal filing system
- tracked if transferred, with a note made or sent to the filing location of the transfer
- returned to the filing location as soon as possible after use
- stored securely
- stored closed when not in use so that contents are not seen accidentally.

7.1.6 With electronic records, Acacium Group workers must:

- always log-out of any computer system or application when work on it is finished
- not leave a terminal unattended and logged-in
- not share logins with other people. If other workers need to access records, then:
  - appropriate access should be organised for them, this must not be by using another worker's access identity
  - not reveal passwords to others
- change passwords at regular intervals to prevent anyone else using them, according to Acacium Group IT management systems
- avoid using short passwords, names or words that are known to be associated with them i.e. children's names, pet's names or birthdays
- always clear the screen of a previous service user's information before seeing another
- use a password-protected screen-saver to prevent casual viewing of service user information by others.

7.1.7 For the purpose of saving space, Acacium Group may scan health records into electronic formats. Acacium Group will use a consistent filing system with clear file management. The holder of these records will ensure that all information is retained in its original format as initially documented with no loss of information. Acacium Group will also ensure there is one key holder with a deputy for backup. Access to scanned files will be restricted to those who have a need to know basis.

8. Best Practice: Archiving Records

8.1 Archiving

8.1.1 It is a fundamental requirement that all of Acacium Group' health records are retained for a minimum period of time for legal, operational and safety reasons. The list in Appendix D sets out the minimum times that Acacium Group are required to retain health records and dictates the method of disposal. This list is not exhaustive and further guidance should be sought from the Records Management NHS Code of Practice part 2, Archiving and Disposal schedule.

8.1.2 Where Acacium Group has transferred care of a service user to another organisation, all healthcare records must be transferred, and it is the responsibility of the receiving organisation to store and / or transfer the information according to national requirements.

8.1.3 Where a service user is in the care of Acacium Group on a private paying basis, Acacium Group retain full responsibility for the management of those records.

8.1.4 The minimum archiving periods should be calculated from the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2001 and the last in September 2004, and for which the archiving period is 7 years, should be kept in its entirety, at least until the beginning of 2012. If Acacium Group considers that records are to be retained permanently, advice will be sought from National Archives and they will be deposited in a 'Place of Deposit'. At the end of the minimum archiving period, Acacium Group will review its record and either dispose of, as per policy, or transfer to a 'Place of Deposit', or National Archives, or destroy the record. For Northern Ireland, records must be retained for 8 years from the date of the last entry made in the records.

8.1.5 When records are retained, they must be held in secure storage with clear labelling. Protective 'wrappers' must indicate sensitivity – though they do not need to indicate the reason for sensitivity. Records also need to identify who is permitted to have access to them and identify a secure means of destruction i.e. shredding.

8.2 Storage, retention (archive) and disposal of personnel records

8.2.1 The Data Protection Act (DPA) is the key Act that applies to this area of management. The Data Protection Directive covers all files that are manual or computerised that are identifiable by a personal factor, i.e., worker number or name. The Directive applies to data held in a 'relevant' filing system, which should be structured. This covers all computerised and manual systems including local text and data processing applications.

8.2.2 Good practice includes:

- keeping personnel files on a computer without network or internet access. This will prevent anyone from viewing or tampering with files from a distance. The person responsible for the data has first-hand control over who can access files
- locking any hard copies in a secure cabinet. Only senior management should have a key to unlock the personnel files and those keys should be handed back as soon as that person moves to a new job. The keys to the cabinet should also be 'do not duplicate' keys to prevent extra copies from being in use
- password protecting any programs that are used to access personnel files. Change the password every month to make sure that the only people with access to files are those with proper authorisation
- keeping medical records separate from other personnel files. Different laws apply regarding the confidentiality of medical records and they can only legally be shared with medical professionals in an emergency situation or with insurance companies who are covering the worker under certain conditions
- establishing strict policies about who can access personnel records and who can't. There should be a human resources person who is in charge of the record keeping and who accesses files. In any case, there should be a specific hierarchy established and only those with 'need-to-know' job responsibilities should be given the ability to look through employee records
- auditing the personnel files annually to separate the files of anyone who is no longer working for the company and check for any missing or altered information.

8.2.3 If there are any queries about this aspect of records management, please refer to the Human Resources department and human resources policies and procedures.

8.3 Sites used for archive (minimum storage period)

8.3.1 Records that are not stored in a service user's own home and have no more use, other than audit or archiving for a minimum length of time, must be kept in safe storage. These must be removed from the service user's home as soon as care is completed and stored in Acacium Group off-site storage facilities, details of the off-site storage site and / or provider must be passed to the Clinical Governance

Manager. If this is with a provider there must be a contract which specifies key performance indicators and requirements. These should include who has access to the records, emergency access arrangements and how records are kept secure. If not with a provider but a site controlled by Acacium Group, an annual risk assessment must be undertaken to ensure continued safety and management of any risks.

8.3.2 Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution i.e. a 'Place of Deposit' that has adequate storage and access. It must be a site approved by the National Archives. This must be done via the Quality Compliance Manager.

8.4 Filing and documentation

8.4.1 In order to facilitate audit, which is a vital part of record keeping, there must be good, clear documentation. As well as facilitating audit it will enable those with responsibility for overseeing the records to retrieve them easily and, where necessary, put them through the next stage of their management within the organisation. Please refer to Appendix E: Filing and Retrieving Records.

9. Best Practice: Disposal of Records

9.1 Freedom of information

9.1.1 It is particularly important under the freedom of information legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies and procedures. The organisation should have formally adopted these policies and procedures which must be enforced by trained, and authorised, workers.

9.2 Recording disposal of records

9.2.1 When records are disposed of there must be a record kept and their method of disposal recorded. Therefore, when health records are transferred or archived there must be a system of documentation. When records are shredded, this must be documented and recorded. Records, including copies, not selected for archival preservation, and which have reached the end of their administrative life, should be destroyed in a secure manner appropriate to the level of confidentiality, or the protective markings. This can be undertaken on site or via an approved contractor.

9.3 When the need for destruction must be delayed

9.3.1 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.

9.4 Storage for longer than 30 years

9.4.1 Ordinarily, archived information is not to be stored for longer than 30 years unless it has statistical research significance, such as, the service user had CJD. In these types of situations, records may be stored indefinitely but with the approval of the National Archives.

10. Access to Records of the Deceased

10.1 Under the Access to Health Records Act 1990 (AHRA), if the record has not been updated during the 40 days preceding the access request, access must be given within 21 days of the request.

10.2 Where the record concerns information all of which was recorded more than 40 days before the application, access must be given within 40 days. However, as with the Data Protection Act 2018 (DPA), organisations should endeavour to supply the information within 21 days. A fee of up to £10 may be charged for providing access to information where all of the records were made more than 40 days before the date of the application.

10.3 No fee may be charged for providing access to information if the records have been amended or added to in the last 40 days. Where a copy is supplied, a fee not exceeding the cost of making the copy may be charged. The copy charges should be reasonable, as the organisation may have to justify them. If applicable, the cost of posting the records may also be charged.

11. Record Keeping

11.1 All records must be kept in accordance with national requirements such as the DPA 2018 and with Acacium Group' information governance and records management policies.

11.1.1 All records remain the property of the commissioner of the care package, and the commissioner is responsible for the storage and archiving of the records in line with the Care Quality Commission (CQC) Nurses and Midwives Code, the Regulation and Quality Improvement Authority (RQIA) and Social Care and Social Work Improvement Scotland (SCSWIS).

11.1.2 All health records must have:

- a unique identifier that separates service users from anyone with a similar name. Wherever possible, Acacium Group will use the service user's NHS number or Acacium Group service user code. Where this is not known, the local hospital number will be used
- the Acacium Group unique identifier documented
- all demographic information such as date of birth, gender, age, home address, GP and next of kin.

11.2 Principles of record keeping

11.2.1 Good record keeping helps to safeguard the welfare of the service user and the workers through the promotion of:

- high standards of clinical care
- continuity of care
- improved communication and sharing of information
- an accurate account of treatment and care planning
- improved detection of problems or changes in a patient's condition
- workers should be particularly diligent in the recording and maintenance of their own 'handover notes'. Every worker is accountable and responsible for the notes they take and how they retain them. They are legal documents and confidentiality must be maintained.

11.2.2 All records must be CLEAR, INTELLIGIBLE and ACCURATE, See Appendix I: Principles of good record keeping.

11.2.3 Good record keeping, whether at an individual, team or organisational level, has many important functions. These include a range of clinical, administrative and educational uses, such as:

- helping to improve accountability
- showing how decisions related to a service user were made
- supporting the delivery of services
- supporting effective clinical judgments and decisions
- supporting the service user and communications

- facilitating continuity of carer
- providing documentary evidence of services delivered
- promoting better communication and sharing of information between members of the multi-professional healthcare team
- helping to identify risks, and enabling early detection of complications
- supporting clinical audit, research, allocation of resources and performance planning.

11.2.4 The DPA (2018) defines a health record as 'consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual'.

11.2.5 The principles of good record keeping apply to all types of records, regardless of how they are held. These can include:

- handwritten clinical notes
- emails
- letters to and from other health professionals
- laboratory reports
- X-rays
- printouts from monitoring equipment
- incident reports and statements
- photographs
- videos
- tape-recordings of telephone conversations
- text messages.

11.3 Statements

11.3.1 Statements must be written as close as possible to an event. They must state the date and time of recording, and the date and time of events. Where people were involved, this should be made clear including name, designation and role at the time. The Clinical Director will advise on how and where statements are to be stored but there must be an expectation that copies, or originals will need to be stored at head office where the coordination of incidents takes place.

11.4 Bring your own device (BYOD) created records

11.4.1 Any record that is created in the context of health and 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 Acacium Group, any information that staff take away could be a risk to the organisation. If this includes personal data or confidential patient information, it is reportable to the ICO and may be a breach of confidentiality. For this reason, personal/confidential patient information should not be stored on the device unless absolutely necessary and appropriate security is in place.

11.4.2 Refer to Acacium Group Bring Your Own Device (BYOD) Policy V1.2.

11.5 Cloud-based records

11.5.1 The use of cloud-based solutions for health and care is increasingly being considered and used as an alternative to manage large networks and infrastructure. UK Healthcare has been given approval to use cloud-based solution, provided they follow published local guidance and that from NHS Digital and information on

11.5.2 GOV.UK. Acacium Group hosts a variety of cloud storage systems and has internal processes in place for management and security of these.

12. Confidentiality

12.1 All workers must be fully aware of the rules governing confidentiality in respect of the supply and use of data for secondary purposes. Always follow local policy and guidelines when using records for research purposes.

- Do not discuss the service users in places where you might be overheard.
- Nor should you leave records, either on paper or on computer screens, where they might be seen by workers or members of the public.
- Do not take or keep photographs of any person, or their family, which are not clinically relevant.

12.2 Information systems

12.2.1 Workers should be aware of, and know how to use, the information systems and tools that are available.

12.2.2 Smartcards or passwords to access information systems must not be shared. When finished working on a system do not leave the system open to access.

12.2.3 Check that your organisation's systems for recording and storing information, whether by computer, email, fax or any other electronic means, are secure.

12.2.4 Use the system appropriately, particularly in relation to confidentiality.

13. Training

13.1 Acacium Group will enable their workers to participate in training in effective records management. This will be backed up in local induction programmes. This is a mandatory requirement upon commencement of employment with Acacium Group. Acacium Group workers are also expected to attend regular updates. The training will be proportionate, and relevant, to the roles and responsibilities of each worker.

13.2 The delivery of training is the responsibility of the Line Managers / appropriate others. It is the responsibility of the central training team to organise and publicise educational sessions, and to keep records of attendance.

14. Implementation Plan

14.1 For **consultation, ratification and dissemination** of this Policy see the Policy for Drafting, Approval and Review of Policies and SOPs. Policy CORP10.

14.2 This Policy will be implemented through:

- communication of the Policy to all relevant workers
- communication of the Policy to all stakeholders
- raising awareness and understanding of the Policy and related processes throughout the organisation through committee meetings, Acacium Group workers' meetings, Acacium Group Pages, the website and general communication through Acacium Group induction programmes and related training.

14.3 This Policy was implemented as part of the review of governance mechanisms and policies in Acacium Group during 2011. The Clinical Director will ensure the dissemination of this Policy across the organisation.

14.4 Audit and monitoring

14.4.1 The Clinical Director will monitor compliance with this Policy. See also the Policy Author's responsibilities in Table 2 for the Acacium Group Policy Drafting, Approval and Review of Policies and SOPs. Policy CORP10

14.4.2 Processes for monitoring the effectiveness of this Policy include:

- audits of the standard of service user records
- audit of evidence of effective management of records
- appraisal and Personal Development Plans (PDP).

14.4.3 The audit will:

- identify areas of operation that are covered by this Policy
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
- highlight where non-conformance to the procedures has occurred and suggest a tightening of controls, and adjustment to related procedures
- report the results to the Governance Committee via the Clinical Director.

15. Associated Policies / SOPs

Policies
CLIN 06 Consent Policy
CLIN 08 Safeguarding Children Policy
CLIN 09 Safeguarding Vulnerable Adults Policy
CORP03 Whistleblowing for Internal Employees Policy
CORP04 Whistleblowing for Associate Workers and External Parties Policy
CORP10 Policy on Policies Policy
CORP14 Complaint Report Policy
ORG 04 Incident Reporting Policy
Acacium Group Bring Your Own Device (BYOD) Policy V1.2

16. References

- Connecting for Health, 2006. *Records Management Roadmap: Suggested Records Management Policy.*
- Department of Health, 2003. *Confidentiality: NHS Code of practice.*
- Department of Health, 2006. *Records Management: NHS Code of Practice part 1, 2, 3 and 4.*
- Connecting for Health, 2011. *Information governance toolkit requirements list* - commercial 3rd party version 8 (2010 -11),
- NHS Scotland, 2008. *Records Management: Best practice in relation to the creation, use, storage, management and disposal of records.*
- Health and Personal Social Services Organisation. Northern Ireland, 2004. *Good management, good records: Guidance for managing records.* HPSSO.
- Public Record Office of Northern Ireland, 2002.*Northern Ireland Record Management Standards.* PRONI.
- Public Record Office of Northern Ireland, 2002. *Guidelines on informal audits and disposal schedules for Northern Ireland (currently under review).*
- The Access to Health Records (Northern Ireland) Order 1993. Department of Health.
- Department of Health, 2007. *NHS Information Governance: Guidance on legal and professional obligations.*
- Data Protection Act ,2018. *A guide for record managers and archivists*.
- Nursing & Midwifery Council, 2009. *Nurses and midwives code: advice sheet in confidentiality.* NMC.
- Nursing & Midwifery Council, 2010. *Record keeping guidance for nurses and midwives.* NMC.
- Professional Records Standards Body https://theprsb.org/

- ISO 15489-1:2016 Information and documentation Records management
- Records Management Code of Practice 2023– NHS England https://transform.england.nhs.uk/media/documents/NHSE_Records_Management_CoP_2023_V5.pdf

Appendix A: About Acacium Group

Acacium Group consists of a number of trading companies, each providing services within core niche areas of the health and social care industries. Therefore, as this document is a Group Policy, the Policy herein applies to all trading companies detailed below:

GP World Part of Acacium Group	pulse Part of Acacium Group	Proclinical Part of Acacium Group
Bank partners	espirita	INGAGE multistaffing | one solution
Liquid Healthcare Part of Acacium Group	Thornbury Nursing Services Part of Acacium Group	Scottish Nursing Guild Part of Acacium Group
Thornbury Community Services Part of Acacium Group	Hobson Prior Part of Acacium Group	maxxima Part of Acacium Group
xyla Part of Acacium Group	Ellea Nursing Part of Acacium Group	CHS Healthcare Part of Acacium Group
DUNN REGULATORY ASSOCIATES Part of Acacium Group		

Appendix B: Legislation

1. This Policy is supported by the following legislation and national guidance as set out below

Act, policy, guidance	Explanation
Data Protection Act 2018 (DPA)	The DPA applies to personal information generally not just health records, but includes finance, human resources etc. All workers who record, handle, store or otherwise come across information have a personal, common law duty of confidentiality to service user s, and to their employer. Other specific provisions in the DPA state that data must be: • fairly and lawfully processed • processed for limited purposes • adequate, relevant and not excessive • accurate and up to date • not kept longer than necessary • processed in accordance to the individual's rights • kept safe and secure • transferred with adequate protection. Since March 2000, the key legislation governing the protection and use of identifiable person-based information has been the Data Protection Act. The DPA does not apply to information relating to the deceased. The Access to Health Records Act 1990 (AHRA) and the common law duty of confidentiality apply. The DPA gives seven rights to individuals in respect of their own personal data held by others, they are the: • right of subject access • right to prevent processing likely to cause damage or distress • right to prevent processing for the purpose of direct marketing • rights in relation to automated decision taking • right to take action for compensation if the individual suffers damage • right to take action to rectify, block, erase or destroy inaccurate data • right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened. The DPA applies to 'personal data', that is, data about identifiable living individuals. Those who decide how and why personal data is processed must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the DPA. Data Protection Act revision in 12/2013 clarified the interpretation of "Personal Data".
Access to Health Records Act, 1990 (AHRA)	The DPA 2018 supersedes the AHRA 1990, apart from the sections dealing with access to information about the deceased. The AHRA provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.
The Caldicott Review 1996.	The Caldicott Committee's report, published in December 1997, included 16 recommendations, which related to ensuring best practice in the use of information flows.

Guidance on 'The protection and use of patient information'	
Human Rights Act 1998 (HRA)	Article 8 of the HRA98 establishes a right to, 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserves the confidentiality of their health records. Current understanding is that compliance with the DPA 2018 and the common law of confidentiality should satisfy human rights requirements. There is also a more general requirement that actions that interfere with the right to respect for private and family life i.e. disclosing confidential information, must also be justified as being necessary to support legitimate aims and be proportionate to the need.
Public Records Act 1958 (PRA)	All 'NHS records' are public records under the terms of the PRA 1958 sections 3 (1) – (2). The Secretary of State for Health, and all NHS organisations, have a duty under the PRA to make arrangements for the safe keeping and eventual disposal of all types of NHS records. The PRA states that public records selected for permanent preservation shall be transferred not later than 30 years after their creation either to the Public Record Office, or to such other place of deposit appointed by the Lord Chancellor.
Civil Evidence Act 1995 (CEA)	The CEA 1995 provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic service user records. Statements contained within documents may be admissible even where the original document has been lost and only a copy is available.
Freedom of Information Act England 2000 (FOIA)	The FOIA lays down requirements for public bodies to keep and make information available on request. The new rights of access in the FOIA signal a new recognition of, and commitment to, the public interest in openness about government. They are additional to other access rights, such as access to personal information under the Data Protection Act 2018. The main features of the FOIA are: • a general right of access to recorded information held by public authorities, regardless of the age of the record / document • a duty on every public authority to adopt and maintain a scheme, which relates to the publication of information by the authority and is approved by the Information Commissioner.
Public Interest Disclosure Act 1998 (PIDA)	The PIDA allows a worker to breach his duty as regards confidentiality towards his / her employer for the purpose of 'whistleblowing'. A disclosure qualifying for protection under the PIDA is known as a 'qualifying disclosure'. Such a disclosure is allowed in the following circumstances where: • criminal activity or breach of civil law has occurred, is occurring, or is likely to occur • a miscarriage of justice has occurred, is occurring, or is likely to occur • health and safety has been, is, or is likely to be compromised • the environment has been, is being, or is likely to be damaged • information indicating evidence of one of the above circumstances is being, or is likely to be deliberately concealed.

Freedom of Information Act Scotland 2002 (FOISA)	As above.
The Freedom of Information Act (FOIA) 2000.Northern Ireland	As above.
The Computer Misuse Act 1990 (CMA) England. Also, Computer Misuse Act for Scotland (1990) and Northern Ireland (1990).	A law that makes illegal certain activities i.e. misusing software, helping a person gain access to protected files.
NHS Code of Practice: Records Management. 2002, 2009 (withdrawn 2016)	Records management best practice in relation to the creation, use, storage, management and disposal of NHS records.
NHS Code of Practice: Records Management (Scotland) Version 2.1 Updated, June 2020	Records management best practice in relation to the creation, use, storage, management and disposal of NHS records.
Department of Health, Social Services and Public Safety. Northern Ireland 2009	Code of practice on protecting the confidentiality of service user information.
CQC. Essential standards of quality and safety. March 2010	Regulator standards.
Regulation and Quality Improvement Authority 2005, 2009 (RQIA)	' The Regulation and Quality Improvement Authority (RQIA) is the independent body responsible for monitoring and inspecting the availability and quality of health and social care services in Northern Ireland and encouraging improvements in the quality of those services'. The reviews undertaken by the RQIA are based on the 2006 'Quality standards for health and social care'. In 2009, the duties of the Mental Health Commission were also transferred to the RQIA.
Health and Social Care Act 2008 - updated 2014 (HSCA)	The relevant part of the HSCA to this Policy is the introduction of the Care Quality Commission (CQC) which is an integrated regulator for health and adult social care, bringing together existing health and social care regulators under one regulatory body. The CQC has new powers to ensure safe and high-quality services.
Social Care and Social Work Improvement Scotland September 2011 (SCSWIS) (known as the Care Inspectorate).	The independent regulator of social care and social work services across Scotland. They regulate, inspect, and support, improvement of care, social work and child protection services for the benefit of the people who use them.
Health & Safety at Work Act 1974	The Health & Safety at Work Act 1974 requires that all organisations with more than three staff have in place processes to promote the health and safety of their staff.
Control of Substances Hazardous to Health	Latex is classed as a hazardous substance which is covered by the Health and Safety Executive's Control of Substances Hazardous to Health (COSHH) Regulations 2002. Under the regulations,

(COSHH) Regulations 2002	organisations have a duty to assess the risk, eliminate, substitute, and limit and control exposure to latex, unless there is a need to use it.
RIDDOR (The Reporting of Injuries, Diseases and Dangerous Occurrences) Regulations 1995	There is a requirement to report diagnosed cases of Occupational dermatitis (schedule 3) to.

2. Equality and diversity

Under the Race Relation (Amendment) Act 2000 Acacium Group has a statutory duty to 'set out arrangements to assess and consult on how their policies and functions impact on race equality', in effect to undertake Equality Impact Assessments (EIA) on all policies and SOPs. The Equality Act October 2010 demands a similar process of Equality Impact Assessment in relation to disability. An EAI must be completed by the author of this policy using the checklist provided in Appendix A. See also Acacium Group Equality and Diversity policy.

Appendix C: Minimum Time to Retain Health Records

The minimum time that Acacium Group is required to retain health records and the method of disposal.

Type of record	Archiving period	Method of disposal
Healthcare records: compiled by workers, including information on an individual's educational status, care needs, etc.	Retain for the period of time appropriate to the service user / specialty, i.e. children's records should be retained as per the archiving period for the records of children and young people; mentally disordered persons (within the meaning of the Mental Health Act 1983) twenty years after the last entry in the record or eight years after the service user's death, if the service user died while in the care of Acacium Group. For paediatrics, it is for the same period of time, but the time does not start until their eighteenth birthday i.e. if a child is ten then the records must be retained until the eighteenth birthday and then a further twenty years. For records of adults, retain for ten years after the last entry was made.	Destroy under confidential conditions.
Clinical audit.	Five years.	Destroy under confidential conditions.
Controlled drugs records: Register destruction records.	Two years from last entry. Five years.	Destroy under confidential conditions.
Diaries of health professionals.	Two years after end of year to which diary relates. Service user specific information should be transferred to the service user record. Any notes made in the diary as an 'aide memoire' must also be transferred to the service user record as soon as possible.	Destroy under confidential conditions.
Dietetic and nutrition.	Retain for the period of time appropriate to the service user / specialty, i.e. children's records should be retained as per the archiving period for the records of children and young people.	Destroy under confidential conditions.
Health care acquired infection records.	Six years.	Destroy under confidential conditions.
Hospital records.	Eight years after conclusion of treatment / care or death.	Destroy under confidential conditions.
Occupational therapy, physiotherapy or speech and language therapy record.	Retain for the period of time appropriate to the service user / specialty, i.e. children's records should be retained as per the archiving period for the records of children and young people.	Destroy under confidential conditions.

Type of record	Archiving period	Method of disposal
Service user / parent held records.	At the end of an episode of care Acacium Group must make appropriate arrangements to retrieve the service user or parent-held records. If records are in relation to a child or young person the records should then be retained until the service user's twenty-fifth birthday, or twenty-sixth birthday if the young person was seventeen at the conclusion of treatment, or eight years after death.	Destroy under confidential conditions.
Equipment / instruments maintenance logs, records of service inspection.	For the life of the product.	No specific requirements.
External quality control records.	Two years	No specific requirements.
Internal quality control records, relating to products such as blood glucose monitoring machines.	Ten years	No specific requirements.
Private service user records.	Although technically exempt from the Public Records Acts, it would be appropriate for authorities to treat such records as if they were not exempt and retain for the period of time appropriate to the service user / specialty i.e. children's records should be retained as per the archiving period for the records of children and young people.	Destroy under confidential conditions.
Records / documents related to any litigation.	As advised by Acacium Group' solicitors. All records to be reviewed. Normal review ten years after the file is closed.	Move to a 'Place of Deposit'.
Records of destruction of individual health records. Case notes and other health-related records contained in this archiving schedule, in manual or electronic format.	Permanent according to BS ISO 15489, section 9.10.	Move to a 'Place of Deposit'.

Type of record	Archiving period	Method of disposal
Referral letters for service users referred to health or care services but not accepted.	Where there is a letter or correspondence detailing the reasons for not accepting the referral from Acacium Group, so the information is also held elsewhere - retain for two years after the decision is made. Where Acacium Group has referred the service user and there is no letter or correspondence detailing the reasons for non-acceptance, retain for the period of time appropriate to the service user / specialty. For example, children's records should be retained as per the archiving period for the records of children, young people, or mentally disordered persons, within the meaning of the Mental Health Act, 1983, twenty years after the last entry in the record or eight years after the service user's death, if the service user died while in the care of the organisation.	Destroy under confidential conditions.
Risk assessment record.	Retain the latest risk assessment until a new one replaces it.	No specific requirements.
Scanned records relating to service user care.	Retain for the period of time appropriate to the service user / specialty. For example, children's records should be retained as per the archiving period for the records of children, young people, or mentally disordered persons, within the meaning of the Mental Health Act 1983, twenty years after the last entry in the record or eight years after the service user's death, if the service user died while in the care of the organisation. NB. Providing the scanning process and procedures are compliant with BSI'sBIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. Once the health records have been scanned the paper records can be destroyed.	Destroy under confidential conditions.

Appendix D: Filing ad Retrieving Records

All Acacium Group workers are required to follow this procedure:

1. Equipment

- Documents for storage or retention
- Documentation to document filing of records (not relevant for records that are in use)
- Stationery to make records secure e.g. envelopes, plastic covers, (where relevant).

2. Filing and retrieving records procedure.

	Action	Rationale
1.	Whilst a service user is receiving care, keep records secure at the service user's home.	To comply with legislation.
2.	If transferring records – follow the 'Disclosure' section in the Records Management Policy.	To ensure due process if followed when transferring records.
3.	Paper records	
3.1	If healthcare for a service user is completed and records are not being transferred, put records into retention following the below process.	To ensure consistency of process.
3.2	Decide on the type of record it is and the length of time for which it needs to be retained. Check whether this is for a minimum time period or permanent.	
3.3	Ensure that all notes are contained within the relevant files. If necessary, secure with elastic bands, ties or in a see-through plastic envelope.	To ensure that all notes are completed and filed securely.
3.4	On the front cover or front of the envelope, put the following information: • service user's name • PRIVATE AND CONFIDENTIAL • date retention started • date retention is due to end • follow on action after retention is completed, i.e. archive or destroy confidentially.	To ensure there is a clear record of the status of all records retained.
3.5	Put the same information as in 3.4 on a 'Records Inventory', see Appendix K: Records Inventory, ensuring the Records Inventory is put back in the same place.	To allow for systematic use of the Records Inventory and ease of finding.
3.6.	Place the file in the relevant filing system in alphabetical order by the service user's surname.	For ease of finding the record for any future use or destruction.
3.7.	Store the records using locking storage and secure filing systems.	To ensure confidentiality is maintained.

4	Electronic records	
4.1	Complete the Records Inventory as in 3.3.	To maintain a record of all records retained or archived.
4.2	File records in the relevant part of the computer storage system i.e. health records, ensuring that access is given only to those who have a need to know or are permitted to manage all electronic records.	To prevent inappropriate access.
4.3.	Each electronic record relating to a service user must be filed with the following file saving format: • surname (in capitals) • initials of person doing the filing.	To ensure a systematic form of filing that easily identifies individuals.
4.4.	Ensure back up of all electronic records, as per Acacium Group IT policies.	Back up must be performed to prevent loss of records.
5	For paper and electronic records	
5.1	On a quarterly basis, the Records Inventory must be checked to undertake any follow-on actions such as archive and destruction.	To ensure compliance with legislative acts and maintain enough storage space.
5.2	Each storage area should have a designated lead for the records and follow on actions. The Clinical Governance Manager should have a list of these designated leads.	Ensures consistency of process and procedure.
6.	Train a second person to act as deputy so that there is continuity during periods of sickness or leave.	Business continuity ensures a system continues when the normal processes cannot take place for some reason.
7.	Records with service user identifiable information must not be stored on CD or memory stick.	The loss of memory sticks and CDs is high risk with a workforce that works between service user s. Therefore, this practice must be avoided.
8	Removal of stored records	
8.1	If records are removed for any reason, they must be logged out. They must be returned as soon as they are no longer required and logged back in. See Appendix L: Record log out form.	All records must be accounted for and be available for audit at any time. If they are removed, it must be clear who is in possession of them, why and where.
9	Destruction of records	
9.1	All records with any identifiable information, such as: • names • addresses • ID numbers • names and addresses of next of kin or GP • clinical diagnosis. Must be shredded then disposed of according to the Acacium Group Waste Management Policy. This includes diaries and post-it notes where this type of information is held.	Service user's identifiable information must not be in a recognisable format once shredding has taken place. Ensure shredders meet a high specification.

Appendix E: Disclosure Model

Disclosure model where it is proposed to share in order to improve service user healthcare

This may be used in the following circumstances:

- Disclosures to NHS staff involved in the provision of healthcare
- Disclosures to social workers or other staff of non-NHS agencies involved in the provision of healthcare
- Disclosures to clinical auditors
- Disclosures to parents and guardians
- Disclosures to carers without parental responsibility.

1. Is there a statutory requirement for, or a court order demanding disclosure?
   - Yes – disclose the information appropriately but, unless special circumstances exist, the service user should be informed of the disclosure ASAP.
   - No – go to the next question.

2. Is the use or sharing intended to support or audit the provision of healthcare to the service user concerned?
   - Yes and No – go to next question.

3. Is the service user competent to understand and give consent to proposed information sharing, or is someone with parental responsibility able to consent?
   - Yes – go to next question.
   - No – act in the best interests of the service user concerned, informing as much as possible and using / sharing information to provide care, and treatment.

4. Has the service user concerned been made aware of who may see what information, for what purposes, and of his / her right to object?
   - Yes – go to next question.
   - No – inform the service user about who may need to see what information, for what purposes, and of his / her right to object.

5. Has the service user raised any concerns or objections?
   - Yes - are you able to agree a compromise where use / sharing of information is acceptable to the service user and the quality of care isn't compromised? If yes, disclose information, on a need to know basis to provide and audit care. If no, do not disclose.
   - If no objections are raised – disclose information, on a need to know basis to provide and audit care.

Disclosures for other medical purposes

This may be used in the following circumstances:

- Disclosures to researchers
- Disclosures to Occupational Health Practitioners
- Disclosures to bodies with statutory investigative powers – GMC, NMC, the Health Service Ombudsman
- Disclosures to NHS Complaints Committees
- Disclosures to cancer registries.

1. Is the disclosure of service user identifiable information essential and appropriate?
   - Yes – go to next question.
   - No – only disclose information in an effectively anonymised form.

2. Is the proposed disclosure of information in connection with a "medical purpose" other than care and treatment i.e. medical research or healthcare management?
   - Yes and no – go to next question.

3. Has the service user or consenting parent been made aware of who may see what information, for what purposes, and of his / her right to object?
   - Yes – go to next question.
   - No – is there a public interest in disclosure? Disclose appropriate information if this is the case.

4. Has the service user given explicit consent?
   - Yes – disclose appropriate information.
   - No – go to next question.

5. Has disclosure been approved under 'section 60' of the Health & Social Care Act?
   - Yes – go to the next question.
   - No – don't disclose unless the public interest justifies disclosure.

6. Has the service user objected to disclosure?
   - Yes – don't disclose unless the public interest justifies disclosure.
   - No – disclose appropriate information.

Disclosures for non-medical purposes

This may be used in the following circumstances:

- Disclosures to non-statutory investigations
- Disclosures to government departments
- Disclosures to the police
- Disclosures required by a court, including a coroner's court, tribunals and inquiries
- Disclosures to Sure Start Teams
- Disclosures to the media
- Disclosures to solicitors.

1. Is there a statutory gateway permitting disclosure such as GMC, NMC?
   - Yes – go to next question.
   - No – is there a public interest in disclosure? If yes, only disclose effectively anonymised information. If yes, disclose and document appropriately.

2. Has the service user or consenting parent been made aware of who may see what information, for what purposes, and of his / her right to object?

- Yes – go to next question.
- No – only disclose in an anonymised format.

3. Has the service user given explicit consent?
    - Yes – disclose and document.
    - No – only disclose in an anonymised format.

Appendix F: Request for Information

Request for information sharing.

Name of person requesting information: _____

Organisation name: _____ Date: _____

Address: _____

Email: _____

Telephone number: _____

Information required:

_____

_____

Why the information is required: _____

_____

Please circle the Act that you think the disclosure is required to comply with:

Data Protection FOI Public InterestAccess to Medical Records

Is consent required? Please circle relevant answer

Yes No

Is consent given if required? Please circle relevant answer

Yes No

Permission for disclosure given by:

Name: _____ Date: _____

Signature: _____ Job title: _____

Date information disclosed: _____

Information disclosed by (sign and print name): _____

Appendix G: Record of Disclosures

The record of disclosures needs to include the following information:

- Date of request
- Applicant name
- Applicant contact details
- Organisation
- Information requested
- Reason information requested
- Act the disclosure refers to
- Reason for non-disclosure (if relevant).

Date:

Appendix H: Principles of Good Record Keeping

The principles of good record keeping include:

- Handwriting must be legible
- Write in black permanent ink only
- all entries to records should be signed. Record date and time on each entry in the left-hand column. In the case of written records, the person's name and job title should be printed alongside the first entry date and time on all records. This should be in real time and chronological order and be as close to the actual time as possible. At the end of a document, put a diagonal line through any unused lines, date and sign
- Records should be accurate and recorded in such a way that the meaning is clear. Records should be factual and not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation. Do not add personal feelings i.e. this pleasant lady. You should not use coded expressions of sarcasm or humorous abbreviations to describe the service users
- If you are recording a conversation, then put the comment in adverted commas
- Number each new page
- Use professional judgment to decide what is relevant and what should be recorded
- Record details of any assessments and reviews undertaken and provide clear evidence of the arrangements that have been made for future and ongoing care. This should also include details of information given about care and treatment
- Identify any risks or problems that have arisen and show the action taken to deal with them
- Communicate fully and effectively with other workers, ensuring that they have all the information they need about the care of the service user. Do not alter or destroy any records without being authorised to do so. Do not falsify records Do not use correction fluid such as tippex or erasers, and do not cross out or scribble through the whole word, or sentence, so that it cannot be read. In the unlikely event that you need to alter your own or another worker's records, you must give your name and job title, and sign and date the original documentation. Make sure that the alterations made and the original record, are clear and auditable i.e. put a single line through the word or sentence so that the original comment is still visible. Discuss with the Line Manager / appropriate other
- Where appropriate, the service user, or their carer, should be involved in the record keeping process
- The language that you use should be easily understood by the people in your care
- Records should be legible when photocopied or scanned
- Keep records safe and secure at all times.

This guidance is supported by further notes and frequently asked questions which are available at ww.nmc-uk.org.

Appendix I: Information Governance Toolkit

Information Governance Toolkit Commercial Third-Party Version 8 (2010-2011)

Requirements List:

- Responsibility for information governance has been assigned to an appropriate member, or members, of staff
- There is an Information Governance Policy that addresses the overall requirements of information governance
- All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities
- All staff members are provided with appropriate training on information governance requirements
- Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected
- There are appropriate confidentiality audit procedures to monitor access to confidential personal information
- All new processes, services, information systems, and other relevant information assets, are developed, and implemented, in a secure and structured manner They must comply with IG security accreditation, information quality, confidentiality and data protection requirements
- All transfers of personal and sensitive information are conducted in a secure, and confidential manner
- Operating and application information systems (under the organisation's control) support appropriate access control functionality. Documented and managed access rights are in place for all users of these systems
- Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
- Policy and procedures ensure that mobile computing and tele-working are secure
- There is an information asset register that includes all key information, software, hardware and services
- Unauthorised access to the premises, equipment, records and other assets is prevented
- There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions
- There are documented incident management and reporting procedures
- All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.

Appendix J: Records Inventory

Service user name (surname first)	Date of birth	Date record placed into archive	Date removed from archive	Follow on action after archive

Appendix K: Record Log Out Form

Service user name (Surname first)	Date of birth	Type of record removed	Date record removed	Reason record removed	Date record returned