DOCUMENT AND RECORDS MANAGEMENT POLICY

V5.0 20 FEB 2020

This is a Controlled Document. This policy is issued by the Company. Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Human Resources Department and/or appropriate delegate should ensure the policy is communicated to all staff and contractors where applicable. The master copy of this document is kept on the Company Policies and SOPs Smartsheet and NAS drive. A copy may be made available on the Company website for public transparency. Staff may print this document for training and reference purposes but are responsible for regularly checking for more recent versions of the document.

AUTHORS

Name: Francis K. Appiagyei

Position: Clinical Manager / IG Lead

AUTHORISATION

Name: Chris Price

Position: Commercial and Legal Director / SIRO

Signature: 

Date: 20 February 2020

CONTENT

ABBREVIATIONS

OPC or OPC UK	Optimum Patient Care Limited
POL	Policy
SOP	Standard Operating Procedure
HR	Human Resources
GP	General Practice
NHS	National Health Service
IG	Information Governance
IT	Information Technology
DSP	Data security and protection
DSPT	NHS Data Security and Protection Toolkit
GDPR	EU General Data Protection Regulation 2016
DPA	Data Protection Act 2018
DPO	Data Protection Officer
SIRO	Senior Information Risk Owner
ICO	Information Commissioner's Office
IAO	Information Asset Owner
CRM	Corporate Records Manager

BACKGROUND

Optimum Patient Care Ltd (OPC) or referred to as 'Company', supports GP practices, commissioners, health researchers and the wider NHS to improve healthcare provision to patients and better patient outcomes. Service users and the public would rightly expect that the Company maintains records on its activities and decisions that affect service provision in an exemplary way. This policy is important because it will help to ensure the Company keeps the records they need for business, regulatory, legal and accountability purposes.

Records are created to provide information about what happened, what was decided, and how to do things. Staff cannot be expected to remember past policies, discussions, actions and decisions accurately all the time, hence why records are kept e.g. updating registers or databases, writing meeting minutes, audio recordings of meetings, etc. Records also ensure that staff and their successors have information to refer to in the future.
Records management is aimed at controlling records within a framework made up of policies, standard operating procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the Company benefits from effective management of one of its key assets, its records.

A records retention schedule is a control document. It sets out the classes of records which OPC maintains and the length of time these are retained before a final disposition action is taken such as destruction or transfer to a permanent place of deposit. It applies to information regardless of its format or the media in which it is created or might be held. All staff members should be familiar with this records retention schedule and apply retention periods to records.

PURPOSE

This policy describes the standards of practice required of staff and contractors (where applicable) for the management of documents and records based on current legal requirements and best practice.

All employees are bound by a legal duty to protect personal information they may come into contact with during the course of their work. This is not just a requirement of staff employment contractual responsibilities but also a requirement within the data protection legislation i.e. GDPR/DPA.

APPLICABILITY

This policy applies to Company staff, and associated persons such as secondees, third party and freelance contractors. Compliance with this policy is a legal and contractual duty for staff and contractors. Failure to comply with this policy may lead to disciplinary and/or legal action.

RESPONSIBILITY

All Employees:

- All employees must adhere to this policy.
- All employees are responsible for keeping a record of any significant business transaction conducted as part of their duties. The record should be saved appropriately, and access controls applied if necessary.
- Any breach of confidentiality, inappropriate use Company records or business sensitive/confidential information is a disciplinary offence, which could result in disciplinary action, termination of employment or legal action.
- All employees must undertake the recommended annual data security and protection training.

Line Managers:

- Ensure this policy is adhered to in their team and that there is on-going compliance.

- Ensure any confidentiality breaches are reported, investigated and acted upon via the appropriate reporting procedure.

HR Department:

- Ensure contracts for employees and contractors have data protection and confidentiality requirements.
- Ensure confidentiality is included in inductions for all employees and contractors (where appropriate).
- Ensure appropriate action is taken to address non-compliance through staff disciplinary procedures.
- Ensure HR and staff records are retained and delated as per this policy.

Senior Management:

- Accountable for effective and legally compliant management for Company records and documents.
- Ensure that the policy and its supporting standards and guidelines are built into Company processes and that there is on-going compliance.

Data Protection Officer (DPO)

- Informing and advising the Company and all of its employees on data protection principles in relation to documents and records management.
- Monitoring the Company's compliance with data protection laws (GDPR/DPA), including confidentiality.

Senior Information Risk Owner (SIRO):

- Approve this policy and take accountability for risk-based decisions and reviews with regards to Company records.

Corporate Records Manager (CRM) / Information Governance (IG) Lead:

- Overall development and maintenance of this policy and its framework.
- Monitoring compliance with the policy to assess its overall effectiveness.
- Ensure that training is provided for all staff groups to further their understanding of the principles of documents and records management.

IT Manager and IT Department:

- Ensuring that Company documents and records are stored securely and that access to them is controlled.
- Knowing what records the Company holds and where they are, by conducting regular audits of records working closely with the OPC IG Team.

Information Asset Owners (IAOs):

- Ensuring the asset they own is managed in accordance with this policy.
- Maintaining adequate records, both legal and regulatory, of the business area the asset operates.
- Work with the IT department to ensure documents and records are stored securely and access to them is controlled.

POLICY

DEFINITIONS

Documents: Documents consist of information or data that can be structured or unstructured and accessed by people in the Company. Records are documents. Documents will need to be declared as a record before records management procedures and policies are applied to them.

Records: Records provide evidence of the activities of functions and policies. Records have strict compliance requirements about their access, retention and destruction; and usually have to be kept unchanged. All records are documents.

LEGAL REQUIREMENTS

The Company will take action as necessary to comply with the legal and professional obligations for its records. Applicable requirements include:

- Data Protection Act 2018 (DPA)
- EU General Data Protection Regulation 2016 (GDPR)
- Regulation of Investigatory Powers Act 2000

Failure to comply with the GDPR or DPA may result in reputational damage to the Company, carries financial penalties imposed by the Information Commissioner, disciplinary action and/or legal action for staff who knowingly or recklessly disclose, procure or obtain personal data.

POLICY PRINCIPLES

This policy covers the management of both documents and records in the Company. The policy sets in place the strategic governance arrangements for documents and records held by the Company, regardless of format, including, but not limited to paper, electronic and digital, registers and databases. The following principles must be adhered to by all employees and contractors (where applicable):

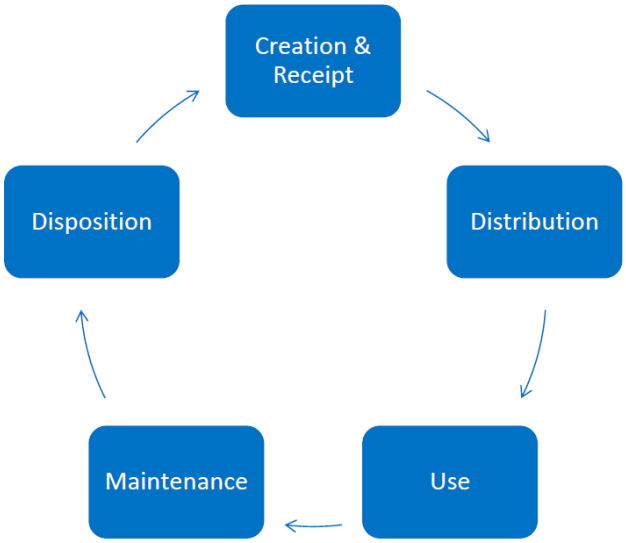
- Staff must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the GDPR/DPA.
- Staff are expected to manage records about individuals in accordance with this policy irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status.
- Where records contain person identifiable data or Company sensitive/confidential information, it is a legal requirement that such data is stored securely. Please contact the IT department for secure storage which must be access controlled.
- The GDPR/DPA allows individuals to find out what personal data is held about them in Company records via Subject Access Request. Staff should ensure records are relevant including their opinions about individuals, as individuals have the right gain access to such records.
- Personal data must not be kept longer than necessary for the purpose of which it was collected, as per the GDPR/DPA.
- Failure of staff to comply with the GDPR or DPA may result in disciplinary action and/or legal action for staff who knowingly or recklessly disclose, procure or obtain personal data or Company confidential data.
- Company documents and records must be held within the recommended or approved storage platform. This ensures that documents and records are easily accessible even in the owner's absence.
- Electronic documents and records should be maintained in accordance with this policy.
- Paper file storage must be secured from unauthorised access and meet fire regulations.
- Where records contain any abbreviations or acronyms, they must be listed or defined.
- Staff must learn about the recommended Record Life Cycle steps and adhere to them where applicable.
- Staff should avoid duplication of records where possible.

- Records must not be created or held unnecessarily. Keeping unnecessary records wastes staff time, uses up valuable space and incurs unnecessary costs.
- Records should only be destroyed in accordance with this policy and the Company's Secure Destruction and Disposal of Data SOP. It can be a personal criminal offence to destroy requested information under the GDPR/DPA upon request if the requested information is within its retention period.
- The recommended retention periods shown in this policy i.e. record retention schedule, apply to the official or master copy of the records.
- Records deleted or destroyed after reaching their retention period, should be logged as part of the asset register in order to prove that the record existed, met its retention and was then disposed of.
- Company records will be reviewed annually as part of Information Assets Review to determine records that should be destroyed and those that should be archived if appropriate.
- Staff must immediately notify HR department or Senior Management if they have been notified of a litigation, investigation or inquiry or have reasonable foresight of a future litigation, investigation or inquiry as this could result in records being held beyond their identified retention period.
- The Company's standard naming convention, including Version Control must be used for the filename of all electronic documents created by staff where appropriate. The re-naming of old documents is optional but new documents must follow the standard naming convention.
- IAOs in conjunction with the IT department should ensure there is a business continuity plan to provide protection for records which are vital to the continued functioning of the Company.
- Electronic records held in databases must have regular back-ups undertaken by the IT department.
- Only approved staff may disclose Company records to third parties. Please refer to guidance in the Company's Data Protection Policy and Confidentiality Policy. Staff with authority to disclose records should make a record of any copies of records they have disclosed, and to whom, in accordance with the Company's guidance on managing personal data requests.
- Staff must not use personal email accounts or private computers to hold or store any Company sensitive/confidential records or information which relates to the business activities of the Company.
- Ideally, personal data should not be stored on any removable device/media. However, if there is no other option, ensure the data is stored on an encrypted device/media. Please contact the IT department for advice.
- Staff must ensure appropriate measures are taken to protect confidentiality when printing paper records, especially sensitive documents – such documents should be collected immediately after printing.
- Staff should ensure appropriate security measures and precautions are in place between the sender and the recipient when transferring records to a third party, particularly records containing person identifiable information or Company confidential information. Wherever possible, records must be anonymised prior to transfer. Please contact the IT department and refer to the Company's Secure Transfer of Data SOP, Data Protection Policy and Confidentiality Policy for further guidance.
- Staff must not leave their computer screen open when unattended, to maintain confidentiality of documents and records. Lock it using the keys Control + Alt + Delete and then click on 'Lock This Computer'.
- Email accounts (both mailbox and personal folder) which do not contain business critical information of staff who have left employment with the Company will be disabled or deleted within 6 months of their exit, unless there are extenuating circumstances e.g. employment tribunal claim or litigation case. This is to ensure best utilisation of IT server space, as well as to ensure that records are not held in excess of their retention period.
- Email accounts (both mailbox and personal folder) which contain business critical information of staff who have left employment with the Company will be declared as records, transferred to a more suitable format and held (archived) for the minimum period below:
  - General staff email account – 1 year or as deemed necessary by Company directors
  - Senior staff email account – 3 years or as deemed necessary by Company directors
  - HR staff – 15 years or as deemed necessary by Company directors
- Missing records should be searched for thoroughly, reported and investigated appropriately, and recorded in line with the guidance in this policy.

RECORDS LIFE CYCLE MANAGEMENT

Information and records management plays a key role in how the Company handles and shares information with service users, suppliers and researchers.
Records are used on a daily basis for internal purposes for business operations, to help make decisions, provide evidence, etc. The law requires certain records to be kept for a defined period – retention period.

The diagram below outlines the key recommended steps in the Records Life Cycle.



Step 1 Creation & Receipt	Making an entry into a paper, electronic document or database. It can be created by employees or received from an external source. It should be complete and accurate.
Step 2 Distribution	Distribution is managing the information once it is created or received, whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when copied, printed, attached to an email, hand delivered or regular mail, etc.
Step 3 Use	After records are distributed, they are used. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other Company operations.
Step 4 Maintenance	Maintenance is when records are not used on a day to day basis and are stored in a records management system e.g. NAS drive, Smartsheet, Google Drive. Even though they are not used on a day to day basis, they will be kept for legal, operational or financial reasons until they have met their retention period. This phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a Records Management system without proper authorisation from Senior Management.
Step 5 Disposition	Disposition is when a record is less frequently accessed, has no more value to the Company or has met its assigned retention period. It is then reviewed and if necessary, destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value to the Company will be held/archived for the future of the Company and may never be destroyed. This is the final phase of a records lifecycle – deletion or archiving.

RECORD RETENTION SCHEDULE

- Keeping unnecessary records wastes staff time, uses up valuable storage space and incurs unnecessary costs. It also imposes a risk liability when it comes to servicing requests for information made under the GDPR/DPA.
- Compliance with the GDPR/DPA means that, records involving personal data must not be kept longer than is necessary for the purposes for which it was collected.
- It may be a criminal offence to destroy requested information under the GDPR/DPA, hence the Company needs to demonstrate that records are destroyed in accordance with proper retention procedures.
- Records should only be destroyed in accordance with the Company's Records Retention Schedule below. The recommended retention periods apply to the official or master copy of the records. Any duplicates/copies made for working purposes should be kept for as short a period of time as possible.

Type of Record	Recommended Retention Period	Legal or Regulatory Requirement
Finance records * IR/HMRC approvals ** Pension schemes	3 – 6 years * Permanent **12 years from the ending of any benefit payable under the policy	Various Acts e.g. Companies Act 1985, Companies Acts 1989 and 2006, Taxes Management Act 1970
HR records *Senior managers	6 years *Permanent for historical purposes	Various Acts e.g. Retirement Benefits Schemes (Information Powers) Regulations 1995, Statutory Maternity Pay (General) Regulations 1986, Taxes Management Act 1970
Application forms and interview notes (for unsuccessful candidates)	1 year	Various discrimination Acts
Supplier or contractor records *Software licences	6 – 10 years (Some records may be held permanently for historical purposes) *Permanent	Company decision
Business operations and administrative data	Permanent unless requested by data controller under GDPR/DPA	GDPR / DPA
Service Databases (including quality improvement database	Permanent unless requested by data controller under GDPR/DPA	Pseudonymised de-identified data – GDPR / DPA
Research Databases	Permanent	Non-identifiable data – Company decision
Research data *OPCRD dataset **Observational research ***Clinical trial/research	Per project data retention period *1 year or as per data sharing agreement **2 – 5 years or as per Sponsor requirement ***10 – 15 years or as per Sponsor requirement	Project or Sponsor data retention requirement Data sharing agreement

RECORDS INVOLVED IN LEGAL HOLDS

- A legal hold, litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation or inquiry.
- The Company has a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated.
- Staff must immediately notify HR department or Senior Management if they have been notified of a litigation, investigation or inquiry or have reasonable foresight of a future litigation, investigation or inquiry as this could result in records being held beyond their identified retention period.
- The legal hold decision will be determined by Senior Management.
- When a legal hold is terminated, records previously covered by the legal hold should be retained in accordance with the applicable retention period under this policy without regard to the legal hold. Documents or records not previously subject to retention may be destroyed.

DOCUMENT AND RECORDS NAMING GOOD PRACTICE

- Document and record naming is an important process in good documents and records management. The Company's standard naming convention below should be used for naming electronic documents wherever possible.

  Company_Document Title_Document Version_Document Date i.e. MMDDDYYYY_Document Status (where applicable e.g. draft or final) e.g.
  OPC UK_Confidentiality Policy_V0.1_11Feb2020_draft
  OPC UK_Confidentiality Policy_V1.0_14Feb2020_final

- Re-naming old documents is optional but new documents must follow the standard naming convention.
- Version Control is the management of multiple revisions to the same document. Version control enables us to tell one version of a document from another.
- Managers may adopt other good practice naming conversions for their teams.
- In delivery of services, it is also acceptable to use the naming conversion requested by the client or Sponsor organisation. Similarly, it is acceptable to recommend the above naming convention to Suppliers working on behalf of the Company or third parties storing documents on company information systems.
- Staff should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual e.g. personnel or HR records.

RECORD MAINTENANCE

- IAOs in conjunction with the IT department should ensure there is a business continuity plan to provide protection for records which are vital to the continued functioning of the Company.
- Electronic documents and records should be maintained in accordance with this policy.
- Electronic records held in databases must have regular back-ups undertaken by the IT department and tested at least annually.
- Paper records, in particular those holding person identifiable or business confidential information must be held in locked storage (secured from unauthorised access) and meet fire regulations.
- The Company at present has no national external storage facility for paper records. This is in accordance with our **environmental aim to become a largely paperless organisation by 2021**.
- All employees are encouraged to save in electronic format wherever possible. Some records may need to remain in paper format for legal reasons e.g. contract records, service agreements, etc.

RECORD ACCESS

- There are legal provisions that give individuals the right of access to personal data created or held by the Company, such as data subject access request right under the GDPR/DPA. This gives individuals the right to find out what personal data is held about them in Company records.
- Please refer to the Company's Data Protection Policy on how to handle data subject access requests.

RECORD DISCLOSURE

- There are legal provisions that limit, prohibit or set conditions on the disclosure of records to third parties. Similarly, there are statutory provisions that require or permit disclosure.
- Only approved staff may disclose Company records to third parties. Staff with authority to disclose records should make a record of any copies of records they have disclosed, and to whom, in accordance with the Company's guidance on managing personal data requests.
- Please refer to the Company's Data Protection Policy and Confidentiality Policy for guidance on disclosure of personal or confidential data.

RECORD APPRAISAL

- Appraisal refers to the process of determining whether Company records should be archived or destroyed. The Company will conduct a review of official annually as part of Information Assets Review to determine records that should be kept for ongoing use, records that should be archived and records that should be destroyed as appropriate.
- The IT department is responsible for secure storage, archiving and deletion of Company records.

RECORD TRANSFERS

- All employees must ensure that appropriate security measures and precautions are in place between the sender and the recipient, when transferring records to a third party. This is very important for records containing personal identifiable data or Company confidential information.
- Wherever possible, records must be anonymised prior to transfer.
- Please contact the IT department for advice on secure transfer of records and refer to the Company's Secure Transfer of Data SOP, Data Protection Policy and Confidentiality Policy for further guidance.

RECORD DISPOSAL

- Disposal is the implementation of appraisal and review decisions and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.
- Records should not be kept longer than is necessary and should be disposed of at the right time.
- Staff should refer to the Record Retention Schedule of this policy.
- Email accounts (both mailbox and personal folder) which do not contain business critical information of staff who have left employment with the Company will be disabled or deleted within 6 months of their exit, unless there are extenuating circumstances e.g. employment tribunal claim or litigation case.
- Email accounts (both mailbox and personal folder) which contain business critical information of staff who have left employment with the Company will be declared as records, transferred to a more suitable format and held (archived) for the minimum period below:
    - General staff email account – 1 year or as deemed necessary by Company directors
    - Senior staff email account – 3 years or as deemed necessary by Company directors
    - HR staff – 15 years or as deemed necessary by Company directors

RECORDS SECURITY

- All person identifiable data or confidential data must be saved with appropriate security measures. Secure storage platforms have been available for storage of records – please contact the IT department.
- All staff must adhere to the Company's Acceptable IT Use Policy and Information Security Policy.
- Staff must not use personal email accounts or private computers to hold or store any Company sensitive/confidential records or information which relates to the business activities of the Company.
- Ideally, person identifiable data should not be stored on any removable device/media. However, if there is no other option, ensure the data is stored on an encrypted device/media. Please contact the IT department for advice.
- Staff must ensure appropriate measures are taken to protect confidentiality when printing paper records. Sensitive documents should be collected immediately after printing.
- Staff must not leave their computer screen open when unattended, to maintain confidentiality of documents and records. Computer screens should be locked using the keys: Control + Alt + Delete and then click on 'Lock This Computer'.

MISSING RECORDS

- Missing records should be searched for thoroughly over 5 working days, after which they should be reported to the OPC IG Team to determine the level of further investigation required and if they should be logged as missing records only or as an information incident.
- The missing record should be marked as missing in the relevant information system.
- If after 6 months, the record is still missing, it is reasonable to assume that the original records has been lost and irrecoverable.
- Data processors acting on behalf of the Company are required to develop and maintain local procedures to handle missing records in line with this policy.

DISSEMINATION & TRAINING

Dissemination: This document will be made available to staff and contractors via Smartsheet and NAS drive or on request from HR Department. This may also be in the form of a global notice sent to staff and contractors notifying them of the release of this document or made available on the Company website.

Training: Training on this document will be provided during induction of staff and contractors or as required by their training needs. Additional and/or regular training will be provided as necessary, based on training requirements to ensure continued awareness and compliance with this document.

MONITORING

Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Compliance with this document will be monitored by Company senior management or appropriate delegate. This may include regular and/or ad hoc compliance checks and audits where appropriate or warranted. This document is to be reviewed annually or sooner where necessary.

RELEVANT DOCUMENTS

Information Governance Policy
Data Protection Policy
Privacy Notice
Confidentiality Policy
Information Security Policy
Acceptable IT Use Policy
Data Quality Policy
Business Continuity Policy
Information Incident Reporting SOP
Audits and Monitoring SOP
Staff Handbook

VERSION HISTORY

VERSION	EFFECTIVE DATE	REASON FOR CHANGE	AUTHORS
V1.0	06 MAR 2016	First final version of new policy	F. Appiagyei
V2.0	07 MAR 2017	Annual review and revisions	F. Appiagyei
V3.0	06 MAR 2018	Annual review and revisions	F. Appiagyei
V4.0	06 MAR 2019	Annual review and revisions	F. Appiagyei
V5.0	20 FEB 2020	New policy and new template	F. Appiagyei