Records Management Policy

Introduction and scope

Good record keeping is an essential part of effective communication and integral to ensuring safe and professional service delivery and business management. Effective records management will ensure that we have the right information at the right time to make the right decisions. It will provide evidence of what we do and why, therefore protecting the interests of Peritus Health Management and its customers and clients.

Records are Peritus Health Management's corporate memory providing evidence of actions, decisions, and events and represent a vital asset to support its daily functions and operations.

Clinical records must be created and maintained in line with the requirements of professional bodies.

Peritus Health Management recognises the following legal and professional obligations and intends to comply through the Information Governance Policy Framework.

- UK GDPR and Data Protection Act 2018
- Health and Social Care Act 2008
- Nursing and Midwifery Council Code of Professional Standards of Practice and Behaviour (Nursing and Midwifery Council, 2015)
- Good Medical Practice (General Medical Council, 2019)
- Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2018)
- NHS Records Management Code of Practice (NHS, 2021)
- The ICO's published guidance and codes of practice

This Policy sets out our commitment to achieving high standards of records management and provides the basis for managing records and information within Peritus Health Management. This includes paper, electronic, health, technical and administrative records. This Policy should be read in association with:

- Information Governance Policy
- Information Security Policy
- Data Protection Policy

By adopting this policy, we aim to ensure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, current and accessible whenever it is needed to:

- help us carry out our business
- help us make informed decisions
- support continuity and consistency in management and administration
- protect the rights of employees, customers and clients
- track policy changes and developments
- provide an audit trail to meet business, legal and professional obligations
- make sure that we work effectively with others
- make sure we are open, transparent and responsive

- promote our achievements

This Policy sits within the Information Government Policy Framework and applies to the management of all documents and records, in all paper and electronic formats or media, created or received by Peritus Health Management in the conduct of its business activities. It applies to all employees, contractors, consultants and third parties who are given access to our documents and records and information processing facilities.

Definitions

Definitions associated with Information Governance within Peritus Health Management are included in Appendix 1.

Roles and Responsibilities

Overall accountability for records management across Peritus Health Management lies with the Managing Director who has overall accountability for records management and managing records management risks.

Senior Management Team are responsible for agreeing the Records Management Policy and considering and approving changes to it, along with reviewing audits and reports on record management issues.

The Operations Manager (Data Protection Officer) is responsible for:

- co-ordinating the implementation and monitoring compliance of this policy to assess and ensure its overall effectiveness
- ensuring that anyone with responsibilities identified in this policy are aware of their responsibilities
- confirming the standards for record keeping
- providing training and advice to all staff and ensuring they understand their obligations
- ensuring access to clinical and organisational records are restricted to those with a legitimate right of access
- enforcing policies and procedures relating to Information Governance and demonstrating compliance with policy through administrative audit, appraisal and competency sign off.

The Clinical Lead is responsible for:

- protection of confidentiality of patient information
- ensuring that patient information is shared appropriately and securely
- enforcing policies and procedures relating to Information Governance and demonstrating compliance with policy through clinical audit, appraisal and competency sign off.

All staff are responsibility for:

- ensuring they comply with Information Governance Policies and professional codes of practice
- creating and maintaining clinical records in accordance with identified standards for record keeping

- reporting incidents involving records to Management, which may include the loss of or missing records.

Records Creation

Records created on behalf of Peritus Health Management should meet the characteristics of a record described in ISO 15489-1 2016 Information and Documentation – Records Management.

Record characteristic	How to evidence
Authentic	It is what it claims to be To have been created or sent by the person claimed to have created or sent it To have been created or sent at the time claimed.
Reliable	Full and accurate record of the transaction, activity of fact Created close to the time of the transaction or activity Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction or activity
Integrity	Complete and unaltered Protected against unauthorised alteration Alterations after creation can be identified as can the person making the changes
Useable	Located, retrieved, presented or interpreted Context can be established through links to other records in the transaction or activity

Clinical Record Keeping Standards

Employees undertaking clinical or clinical administration work on behalf of Peritus Health Management are required to take and maintain full, factual, contemporaneous, dated notes in accordance with the guidance on from the Records Management Code of Practice (NHS, 2021) Ethics Guidance for Occupational Health Practice (Faculty of Occupational Medicine, 2018) and the NMC Code (Nursing and Midwifery Council, 2018). These should be completed at the time of the event, or at the most within 24 hours of the event documented. The author of the records is responsible for the accuracy of the records. All records must be completed accurately and without any falsification, reporting immediately to management if a colleague has not kept to this requirement. Sensitive information collected should be limited to what is required for the particular service required.

The following standards should apply:

1. The client's complete clinical record should be available at all times during their receipt of service delivery by Peritus Health Management.
2. Every page of the clinical record should include the client's name, date of birth, and employer's detail.
3. The documentation in the clinical records should reflect the services delivered and stored in accordance with the naming standards (appendix 2) to ensure chronological order
4. Every entry in the clinical record should be clear, accurate, dated, legible, have minimal abbreviations, and named/signed (electronically as appropriate) by the person making the entry. The designation of the person making the entry and printed name should be against any signature. Deletions and alterations should be countersigned and dated.
5. Personal comments should be avoided.
6. Entries to the clinical record should be made as soon as possible after the event to be documented and before the relevant member of staff goes off duty. If there is a delay, the time of the event and the delay should be recorded.
7. Copies of all correspondence relating to the client should be maintained in the clinical records in the section to which it relates.
8. Consent to release forms should be stored in the area section as the report to which it applies in accordance with the naming standards.
9. Handwritten notes must be written legibly in black ink.
10. Records must be authentic, reliable, useable and stored with integrity.
11. Records whether paper or electronic must be stored to allow retrieval throughout the lifecycle of the record so that the data subject can access the information on request.

Employees creating or receiving documents shall ensure that the Naming Standards (appendix 2) are consistently applied to all documents created, used and stored within Peritus Health Management.

Use

Peritus Health Management uses digital records to ensure easy storage and access and its environmental impact. Different types of records storage arrangements exist within Peritus Health Management, and these are detailed in the Data Protection Policy. The security arrangements for the digital records, including access limitation, are detailed in the Information Security Policy.

All staff must consider the security of records and limit distribution to those with a legitimate right of access. They are responsible for any records they distribute, through printing, photocopying, emailing, uploading and sharing by any other means, and must abide by the security process identified in the series of Information Security Policy.

Personal and Sensitive Records must only be used for the purposes identified on the Privacy Notices.

Transferring data

Peritus Health Management's arrangements for transferring data at the end of a contract period are detailed in the Data Protection Policy.

Retention and Disposal

Retention periods are the minimum periods for which records must be retained for clinical and organisational purposes. Retention periods are defined in appendix 3.

Records will be appraised at the end of the identified retention period to determine whether there is a legitimate reason for maintaining specifically identified individual records or groups of records for longer than the stated minimum.

Paper records that have been scanned into the appropriate electronic storage system are placed in the secured confidential waste bin. The confidential waste bin is kept locked and removed for destruction by a contractor holding a current Waste Carrier's Licence within 24 hours of collection. Receipts for collected confidential waste are stored electronically. Details of the Waste Carrier's Licence are recorded, and a recall date set up to request an up-to-date licence.

Non-clinical electronic records no longer required will be deleted.

Clinical electronic records identified for deletion will be deleted using procedures determined as appropriate by IT Consultant.

All decommissioned IT and mobile equipment will have information erased correctly in accordance with the Information Security Policy.

Monitoring Compliance

Ongoing monitoring of compliance with this policy will be undertaken on a regular basis by the Data Protection Officer with assistance from others as directed.

Terms of Reference

Faculty of Occupational Medicine. (2012). *Ethics Guidance for Occupational Health Practice.* London: Faculty of of Occupational Medicine.

Faculty of Occupational Medicine. (2018). *Ethics Guidance for Occupational Health Practice.* London: Faculty of of Occupational Medicine.

General Medical Council. (2019). *Good Medical Practice.* Retrieved from General Medical Council: https://www.gmc-uk.org/-/media/documents/good-medical-practice---english-20200128_pdf-51527435.pdf?la=en&hash=DA1263358CCA88F298785FE2BD7610EB4EE9A530

ICO. (2018, March 22). *Guide to the General Data Protection Regulation (GDPR) 1.0.51.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

ICO. (Accessed 2021 , 10 21). *Report a Breach.* Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/report-a-breach/

Information Governance Alliance. (2016, July). *Records Management Code of Practice for Health and Social Care 2016*. Retrieved from Digital NHS: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-

governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

National Cyber Security Centre. (2020, August). *https://www.ncsc.gov.uk/cyberessentials/resources.* Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-2.pdf

NHS. (2021, August). *Records Management Code of Practice.* Retrieved from NHS: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Nursing and Midwifery Council. (2015, January 29). *NMC Code.* Retrieved from Nursing and Midwifery Council: https://www.nmc.org.uk/globalassets/sitedocuments/nmc-publications/nmc-code.pdf

Nursing and Midwifery Council. (2018, October 10). *NMC Code.* Retrieved from Nursing and Midwifery Council: https://www.nmc.org.uk/standards/code/read-the-code-online/

Royal College of Nursing. (2015, Dec). *Record Keeping - The facts.* Retrieved from Royal College of Nursing: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjIhOzvlpD0AhV5r1YBHewaCrUQFnoECAMQAQ&url=https%3A%2F%2Fwww.rcn.org.uk%2F-%2Fmedia%2Froyal-college-of-nursing%2Fdocuments%2Freps%2Frecord-keeping-a-pocket-guide-005-34

Revision History

Date	Revision No.	Revision description	Revised by	Authorised
12/11/2021		Created	AD	AD

Appendix 1 – Definitions

Clinical record – any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

Data - means information which:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose
- Is recorded with the intention that it should be processed by means of such equipment
- Is recorded as part of a relevant filing system or with the intention that it should forma part of a relevant filing system
- Does not fall within paragraph (a), (b), or (c) but forms part of an accessible record as defined by section 68 or
- Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

Data Controller– means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

Date Impact Assessment -

Data Processor – in relation to personal data, means any person (other than an employee of a data controller) who processes the data on behalf of the data controller

Data Subject – means an individual who is the subject of personal data

Health record – any record which consists of information relating to the outcome of an occupational health or health surveillance assessment intended to form part of the employer's HR or Health and Safety records.

Legitimate Interest Assessment – an assessment undertaken to ensure that processing under the lawful basis of 'legitimate interest' is lawful. It is a three-part test that considers: the purpose, necessity and balancing test.

Personal Data – data which relate to a living individual who can be identified –

a) From those data, or
b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notice - information made available or provided to data subjects when data is processed about them.

Processing – in relation to information or data means obtaining, recording or holding the information or data of carrying out any operation or set of operations on the information or data, including:

a) Organisation, adaptation or alternation of the information or data
b) Retrieval, consultation or use of the information or data

c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) Alignment, combination, blocking, erasure or destruction of the information of data

Recipient – in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Record – recorded information, in any form, created or received and maintained by Peritus Health Management in the initiation, conduct or completion of a business or individual activity that comprises content, context, and structure sufficient to provide evidence of the activity. This may include but is not limited to information such as:

- clinical records, including notes, reports, test results, photographs etc.
- corporate and administrative records, including policies, procedures, HR, finance, accounting, complaint handling, health and safety, facilities and equipment, meeting minutes, notes and agendas
- computer databases, output, and all other electronic records
- emails and other electronic communications.

Record Management – the process by which all the types of records are managed from creation through their lifecycle to eventual disposal including:

- record keeping
- record maintenance (including tracking of record movements)
- access and disclosure
- closure and transfer
- appraisal
- archiving; and
- disposal

Relevant filing system – any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, with by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Special Category Data – more Special Category personal data which could create more significant risks to a person's fundamental rights and freedoms e.g. information about an individual's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics; health; sex life; or sexual orientation

Third party – in relation to personal data, means any person other than –

a) The data subject
b) The data controller, or
c) Any data processor or other person authorised to process data for the data controller or data processor

Appendix 2 – Naming Standards

Type of record	Example only – correct date and name! Date being date of test
Spirometry results	OGorman F 2021 11 15 Spiro.pdf
Audio results	OGorman F 2013 11 15 audio.pdf
Spiro questionnaire	OGorman F 2013 11 15 resp quest.pdf
Audio questionnaire	OGorman F 2013 11 15 audio quest.pdf
Skin questionnaire	OGorman F 2013 11 15 skin quest.pdf
Health Surveillance Record	TO BE KEPT IN EXCEL FORMAT OGorman F 2013 11 15 Health Surv Rec
Surveillance report forms	OGorman F 2013 11 15 (audio HAVs3) surv rep
Peak Flow readings	OGorman 2013 11 15 peak flows (date refers to last date in series)
Oasys Report	OGorman 2013 11 15 oasys rep.pdf
Chest Physician Referral	OGorman 2013 11 15 Chest Phys Ref
Chest Physician Report	OGorman 2013 11 15 Chest Phys Report
HAVs questionnaire	OGorman F 2013 11 15 HAVS (1,2, 3, 4 or 5).pdf
HAVS review	OGorman F 2013 11 15 HAVS 3 RV
Pre-placement health declaration forms	OGorman F 2013 11 15 Health Dec.pdf
PEHA clearance emails	OGorman F 2013 11 15 clearance email.pdf
PEHA general emails	OGorman F 2013 11 15 email.pdf
PEHA GP reports	OGorman F 2013 11 15 GP rep request.pdf OGorman F 2013 11 15 GP rep AMRA.pdf
PEHA Appointments	OGorman F 2013 11 15 Appt Request OGorman F 2013 11 15 Appt Conf
Management referrals forms	OGorman F 2013 11 15 OH Ref.pdf
Occupational health reports	OGorman F 2013 11 15 OH Report.pdf
Occupational health notes	OGorman F 2013 11 15 OH Notes.pdf
GP report requests	OGorman F 2013 11 15 GP rep req.pdf OGorman F 2013 11 15 GP rep AMRA.pdf

General emails relating to mgt ref	OGorman F 2013 11 15 email.pdf
Access to Medical Reports Act consent form	OGorman F 2013 11 15 AMRA consent.pdf
GP Reports	OGorman F 2013 11 15 GP Report
Access to Medical Reports Act covering letter	OGorman F 16 01 09 AMRA Let.pdf
Specialist report request	OGorman F 2013 11 15 Specialist rep req.pdf
Ill Health Retirement referrals	OGorman F 2021 11 15 IHR Ref
Ill Health Retirement assessment notes	OGorman F 2021 11 15 IHR notes
Ill Health Retirement Pension Fund Form Completed	OGorman F 2021 11 15 IHR Cert
Ill Health Retirement Report	OGorman F 2021 11 15 IHR Report
Counselling referral	OGorman F 2013 11 15 counselling ref.pdf
Specialist report	OGorman F 2013 11 14 Specialist report (or OGorman F 2013 11 14 Dr Hoyle report.pdf)
Counselling report	OGorman F 2013 11 15 counselling rep.pdf
Stress indicator questionnaire	OGorman F 2013 11 15 SIQ summary.pdf
BINDT Vision screening	OGorman F 2013 11 15 BINDT.pdf
Generic notes should be filed against what it refers to	OGorman F 2013 11 14 OH notes.pdf OGorman F 2013 11 14 email.pdf
Consent forms	OGorman F 2013 11 15 consent.pdf
Finance Scanning	
Supplier Invoice/credit	Supplier name-invoice number-invoice date pdf
Supplier delivery note	Supplier name-received date pdf
Customer remittance/statement	Customer name - remittance/statement date pdf

Appendix 3 – Retention Periods

Business Management

- Policies, strategies and operating procedures will be retained for the life of the organisation plus 6 years.
- Management meeting minutes will be stored for 20 years following creation.
- Marketing and patient information leaflets will be retained for 6 years from end of use and then destroyed.
- Website will be stored for 6 years from creation, reviewed and destroyed if no longer required.

Finance

- Financial transactions and accounts records will be retained for 6 years following end of financial year, appraised and if no longer needed destroyed.
- Final annual accounts report will be retained for 20 years from creation and archived.
- Timesheets will be retained for 2 years from creation, appraised and then destroyed.
- Expenses claims will be retained for 6 years following the close of the financial year, appraised and if no longer needed destroyed.
- Petty cash records will be retained for 2 years from end of financial year, appraised and if no longer needed destroyed.
- Salaries paid to staff will be retained for 10 years following the end of the financial year, appraised and if no longer needed destroyed

Clinical

- Occupational Health records (excluding health surveillance records), including ill health retirement applications, will be retained for 6 years after leaving or date of last entry where there is no continued contract with the employer.
- Health surveillance records created after 25 May 2018 will be retained for 6 years from the date of last entry or date of leaving, appraised. Records created before that time will be retained for 40 years unless arrangements have been made with the customer to confirm the correct storage of the pre 2018 records.
- Radiation related health surveillance records will be retained for 6 years from the date of last entry.
- Clinical audit records will be retained for 5 years, appraised, and if no longer needed, destroyed
- Clinical diaries will be stored for 2 years from the end of the year to which they relate
- Clinical supervision meeting minutes will be retained for 5 years, appraised, and if no longer needed, destroyed
- Clinical equipment inspection maintenance and calibration logs will be retained for 6 years, appraised, and if no longer needed, destroyed
- Recorded conversation which may be later needed for clinical negligence purpose will be retained for 3 years following creation, appraised, and if no longer needed, destroyed.
- Recorded conversation which forms part of the health record will be stored as a heath record.

- Emails containing personal data should not be stored in the email system for a period of more than 2 years.

Technical

- Pension records will be retained until the data subjects 75th birthday reviewed and then destroyed.
- Exposure monitoring information will be stored for 6 years from the date of monitoring.
- Employment records will be retained until 6 years from date of leaving, appraised and destroyed if no longer needed.
- Training records will be retained for 6 years from date of leaving, appraised and destroyed if no longer needed.
- Statutory and health protection related training records will be retained for 6 years from date of leaving, appraised, and destroyed.
- Contracts will be retained for 6 years following the end of contract, appraised and destroyed if no longer needed.
- Fraud case files will be retained for 6 years from case closure, reviewed and if no longer destroyed.
- Industrial relations including tribunal case records will be retained for 10 years from close of financial year, appraised and destroyed if no longer needed.
- Litigation records will be retained for 6 years from closure of case, appraised and destroyed if no longer needed.
- Subject access requests and disclosure correspondence will be retained for 3 years following the closure of the SAR, appraised and destroyed if no longer needed.
- Subject access requests where there has been a subsequent appeal, will be retained for 6 years following the closure of the appeal, reviewed and if no longer needed, destroyed.
- Confidential waste transfer notes / receipts to be retained for 3 years, reviewed and destroyed if no longer required.