Information Governance Policy

Contents

What is information governance?

Information governance is a term that is used to describe the way we manage our compliance obligations to the following legislation and professional guidance:

- General Data Protection Regulations 2018 (GDPR)
- Access to Medical Reports Act 1989 (AMRA)
- Access to Health Records Act 1990
- Human Rights Act 1998
- Nursing and Midwifery Council Code of Professional Standards of Practice and Behaviour (Nursing and Midwifery Council, 2015)
- Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012)
- Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016).

The Information Governance Policy sets out the framework for the way Peritus Health Management handles information, in particular, the personal and Special Category data relating to our customers, clients, suppliers, and employees.

The aims of the Information Governance Policy are to:

- Attest to Peritus Health Management's intention to comply with all relevant legislative and professional requirements relating to Data Protection, thereby protecting individuals, the organisation, its customers and its employees from unlawful, inappropriate or insecure processing of data
- Direct all our Information Governance across Peritus Health Management and its interactions with our associate Data Controllers, Data Processors, and Data Subjects.
- Confirm the processes in place to manage the creation, storage, sharing, transfer, and deletion of data in a secure and efficient manner
- Ensure the continued provision of high quality service delivery by defining and promoting the responsible, secure, effective and appropriate use of data
- Confirm the roles and responsibilities of all data controllers and processers within Peritus Health Management and ensure their compliance to their legal and professional obligations.

Definitions

Definitions in relation to this policy are given in appendix 1.

Key requirements and controls

Peritus Health Management recognises and will abide by the 6 key principles of data protection required by Article 5 of the GDPR and the guidance on Information in professional guidance (Faculty of Occupational Medicine, 2012) and section 10 of The Code (Nursing and Midwifery Council, 2015). For us to achieve this, the following arrangements will be implemented for each of the 6 GDPR key principles listed below and specific arrangements for clinical records will be given within the Clinical Records Management section:

Lawful, fair and transparent processing of personal data in relation to individuals.

All business and clinical policies and procedures will reflect legal and professional guidance and be audited against current legislative and professional guidance on a regular basis by a competent person (Data Protection Officer (DPO)). Non-conformances against the policies and procedures will be reported to the Managing Director, corrective action will be identified in Incident & Corrective Action Report Form (PHMF 003.19), and progress will be monitored

by the DPO. The Audit schedule is identified in the Information Audit (PHMF 006.7) and Information Governance Audit Schedule (PHMF 006.8).

All business and clinical practices will reflect documented business and clinical policies and procedures and be audited by a competent person on a regular basis. Non-conformances against the policies and procedures will be reported to the Managing Director, corrective action will be identified in Incident & Corrective Action Report Form (PHMF 003.19), and progress will be monitored by the DPO.

All types of personal data processed within Peritus Health Management are identified in the GDPR Information Audit (PHMF 006.7). The lawful basis, purposes and manner for which the personal data is processed is identified on the Information Audit. Legitimate interest assessments and data impact assessments will be completed where indicated and are also identified in the Information audit.

All data subjects will be informed about the purposes and manner of personal data processing in a Data Protection and Privacy Notice. These will be available on the Peritus Health Management Website (www.peritushealth.com/informationgovernance), in notices within the Peritus Health Management waiting room and mobile screening units, and provided to all data subjects engaged in services provided from the date of implementation of this policy.

Any individual whose personal data has previously been processed by Peritus Health Management, will be provided with a copy of the Privacy Notice in relation to the type of information processed on request.

Due to the complex nature of various categories of data and purposes for processing, Privacy Notices will be specific to the categories of services provided of processing when supplied to individuals so that the information is clear and simple. The Privacy Notices supplied to customers will be specific to the data processed on their behalf and include details of the Data Sharing Agreement which will need to be signed on behalf of Peritus Health Management and the Customer.

Employees of Peritus Health Management will be provided information, instruction and training on the requirements of legal and professional obligations, business and clinical policies and procedures and will be required to confirm their understanding of their responsibilities before handing data and their competency in all procedures before commencing unsupervised work. The Privacy Notice relating to employee records is held within this Policy under Employee Records Management.

Potential customers requesting information from Peritus Health Management through the website or by telephone enquiry will be required to opt into the storage of their details on the CRM system and advised of this on enquiry.

The DPO will monitor for changes in legislation and professional guidance in relation to Information Governance, undertake a gap analysis, advise the Managing Director of the changes and work with the Managing Director to create an action plan to amend business or clinical processes as appropriate in light of any changes.

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Peritus Health Management will ensure that data is not processed for any other purpose than that identified in the Information Audit (PHMF 006.7) by:

- identifying all the categories of personal data processed in the information audit, allocating a legitimate purpose for each category of data and reviewing the information audit on a regular basis to ensure currency

- confirming the processes in place to manage the creation, storage, sharing, transfer, and deletion of data in a secure and efficient manner
- confirming the roles and responsibilities of all data controllers and processers within Peritus Health Management and providing training to all staff so that they competently undertake their workplace activities with due regard to the requirements and principals of this policy, legal and professional obligations
- clarifying the roles and responsibilities of joint data controllers with Peritus Health Management and confirming these within a Data Sharing Agreement to ensure compliance with the principals of the Data Sharing Code of Practice, this policy, and legal and professional obligations
- ensuring that all business and clinical policies and procedures comply with the requirements of the legislation and guidance relating to information governance and are audited on a regular basis by the DPO
- ensuring that the Data Protection Officer is consulted in all change management projects so that data protection is integrated into all processing activities;
- implementing audit processes to confirm adherence to legal and professional obligations, policies and procedures. The Audit schedule is identified in the Information Audit (PHMF 006.7) and Information Governance Audit Schedule (PHMF 006.8).

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Peritus Health Management will ensure that the data processed remains limited to what is necessary in relation to the purpose for which they are processed through:

- regular review of business and clinical practices and standardised forms identified in the Document Control Register (PHMF 001.1)
- regular training of staff
- regular audit

accurate, and where necessary, kept up to date

Peritus Health Management will ensure that the information processed is accurate, and where necessary, kept up to date by:

- identifying the categories of data that should be kept up to date in the Information Audit (PHMF 006.7) and reviewing the accuracy of the data on a regular basis
- rectifying inaccurate data within 1 month of request, unless there is a substantial reason for not doing so (if patient / client records accurately reflect the author's opinion at the time, based on information given at the time, they may not be inaccurate)
- checking with data subjects the accuracy of commonly changed data (address, phone number, email address, job titles) during contact
- seeking a regular update of data subject status and data from customers so that data can be archived appropriately
- advising joint data controllers or inaccuracies in data supplied to allow them to amend records

kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed

Peritus Health Management has identified the retention periods for the categories of data processed on the Information Audit (PHMF 006.7) and has administrative processes (PHMH 003.1) in place to ensure that data is archived or erased as appropriate. The latest date for disposal will be used for each data subject's records.

Retention periods are identified in the Storage Periods section below

Where customers are no longer in contact with Peritus Health Management through change of supplier or dissolvement, the date of last entry in the data subjects' records will be used as a reference point for retention periods rather than date of leaving employment.

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures

Peritus Health Management has identified suitable and sufficient technical, physical and organisational measures to ensure the appropriate security of hard (paper) and soft (electronic) data. The security measures are identified in the Information Security and the Transfer of Records section below.

Roles and Responsibilities

Peritus Health Management is a *Data Controller* for the processing of data in relation to services it provides and the management of the business as it exercises control over what and how data is processed.

The *Managing Director* is responsible for:

- ensuring compliance with legislation and professional guidance
- allocating appropriate resources to fulfil the requirements of the legislation, professional guidance and this policy
- reviewing this policy on a regular basis to ensure it remains current
- ensuring performance and independence of DPO and responding appropriately to concerns raised.

The *Data Protection Officer* (DPO) is responsible for:

- informing and advising the Directors of Peritus Health Management and its employees about their obligations to comply with the GDPR and other Information Governance legal and professional obligations and ensuring that this Policy is reviewed on a regular basis to ensure currency
- monitoring for changes in legislation and professional guidance in relation to Information Governance, undertake a gap analysis, advise the Managing Director of the changes; creating an action plan to amend business or clinical processes as appropriate in light of any changes, monitoring progress against the action plan and reporting progress to the Managing Director
- to monitor compliance with the GDPR and other legal and professional obligations, including business and clinical data processing activities, advising on data protection impact assessments, managing change projects, training staff, and conducting internal audits.
- reviewing the planning for changes in services to ensure GDPR compliance is built into the process
- being the first point of contact for supervisory authorities and for individuals whose data is processed (customers, clients, employees etc)

The *Business Manager* is responsible for:

- ensuring that there is a Data Sharing Agreement in place with all joint controllers before the commencement of data sharing
- feeding audit data into the utilisation report in relation to the maintenance, storage and archiving of customer's client records
- ensuring data compliance of the Customer Relationship Management system

Departmental leaders are responsible for:

- ensuring all categories of personal data are identified on the Information Audit
- ensuring that the processes implemented within the department comply with the requirements of this policy and are documented in their departmental handbooks
- co-operating with the DPO and auditing processes
- reporting any concerns about the safety, security and processing of data to the Managing Director and DPO

Employees of Peritus Health Management are responsible for:

- ensuring their compliance with the requirements of this policy and its associated procedures
- providing all new customers with information on Information Governance and ensuring completion of and compliance with data sharing agreements.
- ensuring clients (patients) are provided with Privacy Notices appropriate to the services to be supplied and they understand their continued rights for confidentiality within the guiding principles of the Faculty of Occupational Medicine's Ethical Guidance (Faculty of Occupational Medicine, 2012).
- the data they process is accurate, adequate, relevant and limited to what is necessary
- checking the accuracy of data stored and rectifying inaccurate data as appropriate
- co-operating with the DPO and auditing processes

Customers (employers) are joint controllers with Peritus Health Management as they are responsible for the referral of data subjects to Peritus Health Management and in control of information relating to:

- the data subject
- the data subject's employment status on which Peritus Health Management relies on for the retention and erasure of data
- the hazards to which the data subject is exposed, on which Peritus Health Management relies on for ensuring adequate and relevant data processing and limiting processing of irrelevant data
- the reason for the data subject's referral to or processing by Peritus Health Management

Peritus Health Management and Customers are responsible for ensuring a Data Sharing Agreement is implemented which identifies:

- the subject matter and duration of processing
- the nature and purpose of processing
- the type of personal data and categories of data subject; and
- the obligations and rights of each party

Other health care professionals, such as Consultant Specialists, Occupational Physicians, Physiotherapists, Talking Therapists are also joint controllers, as they are responsible for the processing of data in relation to the referrals received from Peritus Health Management.

Peritus Health Management requires a Data Sharing Agreement to be in place to define the responsibilities for data sharing and the practical elements of compliance with all Joint Data Controllers. This Data Sharing Agreement will be reviewed on a regular basis to ensure currency.

Information risk management

Peritus Health Management recognises that without careful assessment and control of the legal and professional requirements for compliant data control, there is a risk of non-compliance, data breach, loss of reputation, customers and business.

Peritus Health Management intends to use the Information Audit (PHMF 006.7) to identify all categories of data across all departmental areas so that an assessment of the data in relation to the legal and professional obligations can be made.

Legitimate Interest Assessments will be completed for all categories of data processed under this lawful basis. The links to the Legitimate Interest Assessments relating to each category of data will be identified on the Information Audit (PHMF 006.7)

Data Impact Assessments will be completed where Peritus Health Management is using new technologies; the processing is likely to result in a high risk to the rights and freedoms of data subjects and includes systematic and extensive processing or large-scale processing of special category data. The links to the Data Impact Assessments relating to each category of data will be identified on the Information Audit (PHMF 006.7)

Automated decision making is undertaken for new starter medicals through the online portal and is done with the explicit consent of the data subject. The data subject is given information about the processing in a privacy notice on the portal system and they are able to request human intervention or challenge a decision as desired.

Business and Clinical policies and procedures are reviewed in light of the Information Audit (PHMF 006.7), Legitimate Interest Assessments and Data Impact Assessments to reflect the requirements for data control identified within the audits and assessments. The control measures for Information Governance are identified in this policy and the appropriate Business and Clinical policies and procedures relating to the specific data processing activities.

All staff are provided with information, instruction and training so that they competently undertake their workplace activities with due regard to the requirements and principals of this policy, legal and professional obligations. This is refreshed on a regular basis. Training records and confirmation of competency are stored in personnel records.

A Data Protection Officer has been appointed to: inform and advise the organisation and its employees about their obligations to comply with the GDPR and other Information Governance legal and professional guidance; monitor information governance compliance including business and clinical data processing activities; advising on data protection impact assessments; training staff; and conducting internal audits.

Audits of Information Governance are undertaken on a regular basis and identified on the audit schedule within the Information Audit (PHMF 006.7) and Information Governance Audit Schedule (PHMF 006.8).

Information security

Physical data

Clinical paper documents created away from Peritus Health Management's offices will be stored in sealed document transport envelopes and kept securely by the employee responsible for their creation. The information stored in sealed document transport envelope will be brought into the office on a weekly basis, scanned in and stored electronically on the Cloud based Anchor system.

Clinical paper documents created whilst in the office will be stored in locked cabinets when at the end of use and not removed from site. Access to the cabinets will be restricted to those undertaking administrative support duties and clinical personnel only. Keys will be kept secure at all times.

All other paper records containing personal data will be documented in note books provided specifically for the documentation of work-related issues. Note books will be issued out and collected in by the DPO. No notebooks other than those issued by the DPO should be used for

processing personal data. Employees are responsible for ensuring the safe use and disposal of the note books. The note books will be stored in locked bags or sealed document transport envelopes when away from Peritus Health Management's offices.

Paper records containing personal data must not be stored in any other location than those outlined above.

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 of confidential waste are stored electronically. Details of the Waste Carrier's License are recorded and a recall date set up to request an up to date license.

IT records

Personal and Special Category data is processed electronically by a number of different systems within Peritus Health Management and include:

1. email system
2. records storage system
3. recall system
4. customer relationship management system
5. clinical record database
6. clinical portal
7. finance management system
8. clinical equipment databases
9. occupational hygiene equipment software

Peritus Health Management contracts an IT Consultancy to provide a managed IT Services programme to the business to:

- assess the IT requirements of Peritus Health Management ensuring the secure and smooth functioning of IT related activities within the business and advise on the best solutions for the current and future business needs.
- protect the confidentiality, integrity and availability of data on behalf of Peritus Health Management and will organise, implement and maintain robust systems infrastructure and network security arrangements abiding by the principle and codes of practice defined by ISO 27001 as they apply to Peritus Health Management.
- maintain network consistency by installing applications, patches and updates required.
- create and maintain a site database of system hardware and software ensuring authenticity and currency of systems used
- ensure the currency of the IT asset inventory, that all assets are suitable, safe, maintained and fit for purpose
- ensure the safe governance and efficiency of software, applications and operating systems
- logging all systems and storing all audit logs for review as required
- ensure that all IT equipment will be decommissioned appropriately with regards to the erasing of stored information and provide a formal certificate of data erasure for each decommissioned asset.
- provide a review of Peritus Health Management's IT objectives on a quarterly basis to ensure

The IT Consultancy used for the maintenance of software and hardware are required to abide by the codes of confidentiality to ensure no inappropriate access to Special Category personal data.

Peritus Health Management uses a UK based datacentre for storage or processing of health-related data. Access to the data centre is restricted by access controls and alarms (including CCTV) and the information stored is encrypted so that any ghost prints of deleted data remain encrypted. The system is monitored for significant or unauthorised events and managed appropriately. Audit systems are in place and audit logs are maintained for a minimum of 12 months.

Information relating to the Business is stored on Customer Relationship Management software which uses a Belgium based datacentre for the storage or processing of customer (not client) and prospective customer related contact details and marketing information. Access to the data centre is restricted by access controls and alarms (including CCTV) and the information stored is encrypted so that any ghost prints of deleted data remain encrypted.

Peritus Health Management has a password management policy in place. Username and complex password authentication is required for access for all IT hardware. Password authentication is required for mobile devices. Passwords are required to be changed on a regular basis and reminders to users are automatically sent. Passwords and other access will be cancelled immediately a staff member leaves the organisation or is absent for a prolonged period. Where there is a perceived significant risk to the security of data from an employee, a Director will cancel access to the data and investigate appropriately.

Anti-virus and anti-malware products will be kept up to date and used to actively scan the IT devices to prevent or detect threats. Users are aware that removeable media must only be used with permission of a director. A firewall is in place to prevent unauthorised external entry into Peritus Health Management's network. This is reviewed and maintained on a regular basis. All these are monitored by the IT service contracted to the business. Peritus Health Management maintains a list of authorised software and this is monitored by the IT service contractor. Standardised configurations of operating systems and software applications are used. Patch management is deployed on a daily basis from IT support. Vulnerability scans are undertaken on a weekly basis.

Restrictions are in place on all IT equipment to prevent unauthorised up/downloading of software. Employees are classed as users with no administration rights. Directors have Administration rights only. Unauthorised application upload onto company hardware or processing of personal / Special Category data onto unauthorised IT (including mobile devices) hardware is classed as gross-misconduct and will be managed in accordance with disciplinary procedures.

IT hardware (laptops) are not to be connected to 3rd party wireless networks without the permission of a Director and data tethering through company mobile devices should be used for this purpose only.

Administrative privileges to stored records and systems are granted on a role-based need. These are checked on a regular basis in the IT review meeting to ensure that they remain current. Organisational Administrative access to the data is restricted to the directors of Peritus Health Management.

All data is backed up on a continuous basis and the back-up is encrypted and retained for 12 months. Peritus Health Management has a business continuity and disaster recovery plan in place for deployment in case of loss of data. The risk of total loss (erasure) of soft data has been assessed and is considered to be extremely low.

Peritus Health Management uses IDS systems for boundary defence. Continuous monitoring and alerts are set up to ensure all violations, unauthorised access and anomalous activities are logged, monitored, reviewed and addressed in a timely manner by the IT Consultancy.

Transfer of personal or Special Category data files out of Peritus Health Management and between users within Peritus Health Management are undertaken with secure file sharing or file encryption with password protection, unless with prior agreement from the data subject. Passwords are sent separately or a pre-agreed password formula is used. Information transferred using memory sticks will be encrypted, password protected and deleted as soon as the transfer has been completed as per the Transfer of Records procedures below.

Access to data is not granted to 3rd parties other than those identified in the Information Audit and Data Sharing Agreements for lawful purposes.

Mobile devices and IT equipment

Peritus Health Management maintains an inventory of all mobile devices and IT equipment owned by Peritus Health Management and connected to our network. All IT (including mobile devices) hardware is supplied to employees for company use only. Employees receive training on the company IT usage policy.

Peritus Health Management uses full disk encryption on all computers used for processing personal or Special Category data.

Personal or Special Category data relating to Peritus Health Management's work activities will not be stored on any other devices other than those owned and maintained by Peritus Health Management.

The physical security of all IT (including mobile devices) hardware issued to employees are the responsibility of the receiving employees. Employees will ensure that computers are securely stored at all times when they are not in their presence. IT equipment and mobile devices must not be left visible in cars or other locations when securely stored. At the end of their use, employees are responsible for signing back to Peritus Health Management the IT hardware.

All IT equipment will have information erased correctly by the IT contractor. Formal notice of data erasure will be stored electronically.

All mobile devices will be reset to factory settings by Peritus Health Management before disposal. Formal declaration of the reset will be signed by the person undertaking the reset and the declaration stored electronically.

Record Management

Peritus Health Management intends to ensure that all records are stored electronically for the identified period will specific naming standards and folder trees identified for ease of retrieval. This format is identified in the Control of Documentation Policy (PHMP 001).

Clinical Records Management

Employees undertaking clinical work on behalf of Peritus Health Management are required to take and maintain full, factual, contemporaneous, dated notes. They are responsible for the accuracy of the records and the implementation of the storage of records in accordance with this policy. The Clinical Record Keeping Standard applied in Peritus Health Management is documented in Appendix 6 – Clinical Record Keeping Standards and adapted from the Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016).

The individual occupational health record is a confidential medical record to which the principles of medical confidentiality as defined by the Faculty of Occupational Medicine's Guidance on

Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012) and the Nursing and Midwifery Council Code (Nursing and Midwifery Council, 2015) applies. This is in addition to the requirements of the GDPR.

The lawful basis for processing this data and the rights available to individuals (data subjects) are identified in the Privacy Notices for each item of service (appendix 2) and in the Information Audit (PHMF 006.7).

In communicating with managers on the health of employees, unless informed consent to release has been given to release specific health-related details, the outcome of the health assessment (fitness for work) rather than clinical details will be given. Whilst consent to release health-related information is still required, this does not affect the lawful basis on which the data has been processed which is identified in the Information Audit (PHMF 006.7) and Privacy Notice for that item of service. Should a client refuses consent to release the information, a simple statement on fitness to work, referring only to information already in the domain of the recipient for context if required, will be provided.

Employees of Peritus Health Management are responsible for all clinical data, whether held manually or electronically, processed for the duties for which they are employed, and must ensure the security of that data, and the hardware on which it is processed at all times.

Unrestricted access to clinical data is confined to those undertaking clinical duties and those undertaking administrative support duties where it can be demonstrated that they are fully aware of their personal responsibility to keep all clinical information confidential.

The Managing Director of Peritus Health Management is responsible for ensuring all employees are aware of their responsibilities under this policy and that all employees confirm their understanding and agreement to this policy by signing an Information Governance and Confidentiality Statement (Appendix 4 – Information Governance and Confidentiality Statement). This will be reviewed on a regular basis.

Clinical (personal, Special Category health related) data will not be released to others unless:

- the informed consent of the individual is provided in writing or, in exceptional circumstances, verbal consent where the verbal consent is witnessed and signed by 2 people. The reason for verbal consent release should be documented in the clinical records indicating the reason written consent could not be obtained;
- if the disclosure is clearly in the best interest of the individual, but it is not possible to seek consent;
- if there is a real concern that the health or safety of others is endangered;
- if it is required by law;
- if it is in the public interest.

To give informed consent the individual should clearly understand what information will be imparted, to whom, for what purpose and the possible outcomes which may result.

An employee of Peritus Health Management shall only disclose information, without the informed consent of the individual, where a failure to disclose information may expose the individual or others to the risk of death or serious harm, or in order protect the safety of other workers or the general public. This should only do so with consent from the Managing Director of Peritus Health Management (or their deputy), or under guidance from a medical defence organisation or professional body. The Managing Director of Peritus Health Management (or their deputy) will be advised of a disclosure made under guidance as soon as possible. Where there is an immediate risk to the safety of the individual or others, the employee should take formal action to prevent that risk, advising the individual of their intention to do so, where by informing the individual of this intention they do not put their own health and safety at risk. (See appendix 5 – Procedure for Managing Critical Risk Incidents).

Where a client wishes access to their clinical records, the procedure for submitting a request for information should be followed.

Customer and Prospective Customer Records Management

Information relating to the customer or prospective customer is stored on the Customer Relationship Management (CRM) System or file storage system on a UK based datacentre for storage or processing of health-related data.

The categories of data stored on the CRM system, the data subject rights and the lawful basis for processing are identified on the Information Audit (PHMF 006.7).

Consent to process data for prospective customers is requested using opt in boxes on information request submission through the website. Verbal consent to enter information into the CRM system will be sought from prospective customers making enquiries on the telephone. Written consent for storage of data on the CRM system will be requested in the first communication with the prospective customer. The lawful basis for processing this data and the rights available to individuals (data subjects) are identified in the Privacy Notices (appendix 2).

Once the prospective customer becomes a customer, a Data Sharing Agreement will be signed and implemented. No services will be provided to the customer until the Data Sharing Agreement has been signed and returned to Peritus Health Management.

Employee Records Management

The categories of employee data processed, the lawful basis for processing, the sharing and the individual rights are identified on the Information Audit (PHMF 006.7). The Employee Privacy Notice is included in Appendix 2

Special Category data relating to employees will be processed on the Personal Personnel Folders on the file management system held on a UK-based datacentre.

Personal data relating to recall dates will be stored on the CRM system.

Financial (payroll and pension) data will be processed in the Personal Personnel Folder and the Finance system.

Financial Records Management

Special Category data relating to finance will be processed on the Personal Personnel Folders on the file management system held on a UK-based datacentre. Personal data relating to recall dates will be stored on the CRM system.

The categories of financial data processed, the lawful basis for processing and the individual rights are identified on the Information Audit (PHMF 006.7).

Complaints Records management

Special Category data relating to complaints will be processed in the Management Folder on the File Management system held on a UK-based datacentre.

Complaint information must not be recorded in the clinical or personnel record as it may be unfounded, or involve third parties and the inclusion of that information in the clinical or personal record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the persons named in the record.

Retention, Archiving and Disposal of Records

All records no longer in use or pertaining to a data subject who is identified as a leaver, will be transferred into an 'Archive Folder' within the records storage area. The folder in which the record is stored will be identified with the date of disposal as per the Control of Documentation Policy (PHMP 001). The folder will be stored in a folder within Archive named the year of disposal.

Customers are responsible, as joint controllers, are responsible for informing Peritus Health Management of data subjects date of leaving, to allow for the appropriate archiving and destroying of records.

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

Where paper records do not contain Personal or Special Category material, it can be disposed of through normal waste processes.

Computer assets will be disposed of by the IT contractor and evidence of their correct disposal stored electronically.

Electronic records will be disposed of from the main records and the recycle bins to ensure full disposal.

Emails containing personal data which is of ongoing business value as they demonstrate offers and acceptance of contracts for orders from customers; are evidence of communication or trigger formal retention requirements identified below, must created in a PDF format and stored in the appropriate record folder using the naming standards in the Control of Documentation Policy (PHMP 001) or for data requiring shorter periods of retention, moved to a separate mail folder for a period of time following which it has become evident that the information is no longer required.

Retention Periods

Accounts records will be retained for 3 years from the end of the financial year, reviewed and if no longer needed, destroyed.

Final annual accounts report will be retained for 20 years from creation and archived.

Expenses claims will be retained for 6 years following the close of the financial year, reviewed and if no longer needed destroyed.

Petty cash records will be retained for 2 years from end of financial year, reviewed and if no longer needed destroyed.

Financial transactions will be retained for 6 years following end of financial year, reviewed and if no longer needed destroyed.

Salaries paid to staff will be retained for 10 years following the end of the financial year, reviewed and if no longer needed destroyed

Clinical audit records will be retained for 5 years, reviewed, 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 protocols will be retained for 25 years from creation and if no longer needed, destroyed retained for 5 years, reviewed, and if no longer needed, destroyed

Clinical supervision meeting minutes will be retained for 5 years, reviewed, and if no longer needed, destroyed

Clinical equipment inspection maintenance and calibration logs will be retained for 20 years, reviewed, 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, reviewed, 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 for a period of more than 2 years.

Management meeting minutes will be stored for 20 years following creation.

Policies, strategies and operating procedures will be retained for the life of the organisation plus 6 years.

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

Pension records will be retained until the data subjects 75th birthday and then destroyed.

Exposure monitoring information will be stored for 40 years from the monitoring ceases where the record is representative of the personal exposure of customer employees

Occupational Health 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 will be retained for 40 years from the date of last entry

Radiation related health surveillance records will be retained for 50 years from the date of last entry.

Employment records will be retained until 6 years from date of leaving and then destroyed.

Timesheets will be retained for 2 years from creation, reviewed and then destroyed.

Training records will be retained for 6 years from date of leaving and then destroyed.

Statutory and health protection related training records will be retained for 40 years from date of leaving and then reviewed.

Contracts will be retained for 6 years following the end of contract, reviewed and then if no longer needed, destroyed.

Calibration records of exposure monitoring and health surveillance activities, to be retained for 40 years following completion of the test, reviewed and if no longer required, destroyed.

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, reviewed and destroyed if no longer required.

litigation records will be retained for 10 years from closure of case, then reviewed and destroyed if no longer required.

Subject access requests and disclosure correspondence will be retained for 3 years following the closure of the SAR, reviewed and if no longer needed destroyed.

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 2 years, reviewed and destroyed if no longer required.

Submitting a request for information

Peritus Health Management will ensure, wherever appropriate, that a data subject has access to all records stored about them. Data subject should apply in writing to Peritus Health Management to request access to the records or copies of their records.

In order for Peritus Health Management to confirm the identity of the data subject, Peritus Health Management will may request evidence of identity prior to supply. The request for accessing occupational health data (PHMF 010.49) can be used for this purpose.

Peritus Health Management will respond to such a request within 30 working days of receipt of the request. Peritus Health Management will provide an individual with an interpretation of information stored in the records where required.

Where a lawyer employed by a company or the data subject requests access to Occupational Health records, Peritus Health Management will ensure that written informed consent has been gained before disclosure. Where there are records related to other matters unrelated to the injury or issue in question, Peritus Health Management will clarify the consent with the data subject. An Order of Discovery will be required to gain access to records where consent is refused. The Order of Discovery should be checked for a stamp to clarify that this has been a confirmed court document.

Where a data subject consents to the release of only part of the Occupational Health records but refuses the release of other equally relevant parts, Peritus Health Management will advise the solicitors of both parties that all the records relevant to the case have not been made available to both sides. Records will not be released in these circumstances without consent or an Order of Discovery.

Applying for confidential medical information

Where an employee seeks a report from a health care professional responsible for the clinical care of a client, the Access to Medical Reports Act applies and the employee will explain to the client their rights under the Access to Medical Reports Act as part of the process of obtaining the client's informed consent (See appendix 7)

The clinician applying for the confidential medical information is responsible for ensuring that the data subject is aware of the information sought from the health care professional and will send a copy of the request to the data subject at the same time as to the health care professional.

Transfer of records procedures

Peritus Health Management will only transfer Occupational Health records to an appropriate health professional who is able to provide:

- confirmation of a contract between the customer and the occupational health provider (a letter from the customer confirming the new provider's details and contact arrangements)
- sufficient evidence of consultation between the customer and its employees advising of the transfer of services, the opportunity to request for their clinical records to be archived rather than transferred and the future storage of records
- photographic evidence of identity of the professional receiving the records and evidence of current registration of the General Medical Council or Nursing and

Midwifery Council, and who will sign to accept responsibility for the storage and maintenance of the Occupational Health records in accordance with the General Data Protection Regulations and the Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (see appendix 8).

A list of all records transferred will be kept and stored. Electronic records will be transferred on an encrypted memory stick. The stick will be checked by a second person to ensure that the records are encrypted on the stick. The stick will be sent by recorded delivery only and the track and trace record will be stored electronically and details of the track and trace provided to the recipient. The password will be provided to the recipient once they have confirmed receipt of the stick. A copy of the list of all records will be sent to the recipient.

The Occupational Health records are the property of Peritus Health Management and the contents belong to the author.

Where a customer ceases to exist, the records will be retained for the standard periods with Peritus Health Management. Where a client provides a written request, these records may be transferred to the client's GP.

Breach of Data Protection

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A data security breach may happen due to:

- loss of theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking attack

If a personal breach has occurred, the employee identifying the breach will advise the DPO and Managing Director, who will establish the likelihood and severity of the resulting risk to people's rights and freedoms. The range of adverse effects on individuals, including emotional distress, and physical or material damage, will be considered.

If there is a risk to people's rights and freedoms, the Managing Director or DPO in her absence will report the breach to the Information Commissioners Office no later than 72 hours after the becoming aware of the breach. The following steps will also be taken to manage the breach:

- recover the information and limit the damage the breach can cause;
- review security procedures to prevent further loss;
- report criminal activities;
- assess the potential detrimental effect the data subjects arising from the breach. This includes: physical and financial damage as well as emotional distress
- refer to the guidance on security breach management produced by the Information Commissioners Office to see whether the breach should be reported.

The Information Commissioner's Office website will be checked for details of reporting a breach. If all the details of the investigation in to the breach is not available immediately, the ICO must be informed of the delay and when the missing information will be supplied.

If the breach is likely to result in a high risk to the rights and freedoms of the data subject, the data subject(s) will be advised of the breach immediately.

A record of the investigation into the breach will be stored securely in the Management Folder and linked to the appropriate area on the Information Audit. An audit of data protection relating to the breach will be undertaken to prevent further breaches.

Audit and review

The Data Protection Officer is responsible for overseeing audit processes to ensure compliance with the GDPR and other legal and professional guidance, and compliance with this policy.

Outcomes of the audit process will be provided to the Managing Director, and progress on resulting action plans will be monitored by the DPO and Managing Director.

This policy will be reviewed in May 2019 by the DPO.

Revision History

May 2018 – created by Amanda Dowson.

Appendix 1 – Definitions

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

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.

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 – Privacy Notices

Data Protection and Privacy Notice – Employees

Peritus Health Management is committed to meeting our responsibilities under the General Data Protection Regulations and other legal and professional guidance. We would like our employees to be confident that their personal data is being handled responsibly and securely. For full details of our arrangements for Information Governance is available on Anchor in the Policies and Procedures folder.

What information do we collect about you?

The categories of information we process about our employees includes:

- personal information (name, national insurance number, date of birth, right to work in the UK, next of kin; address; telephone number; photographs)
- contract information (such as start date; hours worked; post; roles; salary; references; criminal record; driving license details; fitness for work; payroll; tax; pension details; disciplinary and grievance information)
- work absence information (number of absences and reasons)
- qualifications (and where relevant, experience, professional indemnity, professional registration etc)

For full details of all categories of information we process, please see the PHMF 006.7 GDPR Information Audit.

How will we use that information?

We use employee data to:

- enable formal communication relating to your employment with you in accordance with the legal basis of Article 6(b) necessary for the performance of contract; and Article 9(b) processing necessary for the purpose of carrying out obligations and specific rights in the field of employment law
- contact you or your next of kin in case of emergency
- allow us to process your pay, pension and tax in accordance with the legal basis of Article 6(b) necessary for the performance of contract and 6(c) necessary for compliance with a legal obligation
- ensure that all checks are in place in accordance with the Employment and Subcontracting of Work Policy in accordance with the legal basis of Article 6(b) necessary for the performance of contract; and Article 9(b) processing necessary for the purpose of carrying out obligations and specific rights in the field of employment law; and Article 9(f) processing necessary for the establishment, exercise or defence of legal claims.

Collecting Employee Information

Peritus Health Management collect personal information via employee details forms; additional requests for documentation from employees directly.

Employee data is essential for our operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing Employee Information

Peritus Health Management will hold data securely for the set amount of time shown in our data retention schedule.

Access to personnel information on Anchor is restricted to the Directors.

Photographs of employees will be provided on the 'Meet the Team' page on the website and Customer Handbook.

For more information on our data retention schedule and how we keep your data safe, please review the Information Governance Policy on Anchor in the Policies and Procedures folder.

Sharing Employee Information

Peritus Health Management does not share information about our employees with anyone without consent or unless the law or our policies (staff handbook) allow us to do so.

We may share limited employee data for the following purposes:

- HR Consultant – for processing of contract and other HR purposes
- Accountant, Pension Fund and HMRC – for processing of payroll, pension, national insurance and tax
- External Auditors – for quality accreditation verification of evidence
- DBS Contractor – to gain criminal record check
- Insurance Company – to gain company vehicle insurance
- OH physician – for fitness to work check

Data is transferred using appropriate security measures. For more information on our information security, please review the Information Governance Policy on Anchor in the Policies and Procedures.

For full details about the categories of information we share, please see the PHMF 006.7 GDPR Information Audit.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request to access your personal information, please email dpo@peritushealth.com or amanda@peritushealth.com

You also have a right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing - which we do not do
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Any further questions

If you have any questions relating to this process, please contact the Data Protection Officer on dpo@peritushealth.com and put in the title box, FAO Data Protection Officer. Please

identify how you would like use to contact you in the main body of the text and the nature of your enquiry.

Data Protection and Privacy Notice – Occupational Health

Peritus Health Management is committed to provide safe and effective occupational health and hygiene services to customers. During the course of conducting our business, we process a significant amount of personal and special category data and will ensure that all personal information will be processed in accordance with the requirements of the General Data Protection Regulations and other relevant legal and professional guidance. We want our staff and service users to be confident that personal data is being handled responsibly and securely. For full details of our arrangements for Information Governance is available on our website: www.peritushealth.com/informationgovernance.

What information do we collect about you?

You have been referred to Peritus Health Management by your employer to undertake an assessment of your health in relation to your job and / or your workplace exposures. This is part of their statutory duty of care towards you and may form part of your employer's health and safety management system and equality strategy. You do not have to consent to participating with this referral but if you do not, any decisions that your employer may need to take, will be taken based on the information already available. For health surveillance activities, this may also be a breach of your responsibilities as an employee under the Health and Safety at Work etc Act.

During the course of the assessment, you will be asked questions about your health or medical issues, treatments and impact on your activities of daily living and if appropriate to the reason for your referral, we may undertake some tests e.g. blood pressure, vision, hearing or breathing tests. The Occupational Health professional conducting the assessment is required to take clinical notes of the assessment. These notes will be kept confidential and stored electronically with appropriate access restrictions and security.

You will have the opportunity to discuss any concerns that you have about your health and we will do what we can to help. It is sometimes helpful if you able to bring details of any medications you are taking, healthcare professionals you are seeing, or consultation summary letters in case you wish to refer to this information.

How will we use that information?

The information collected during the assessment is used to make a clinical assessment of your fitness to work, your work capability, early signs of health issues, and/or whether there are any health and safety concerns relating to your health at work.

Following your assessment, the Occupational Health professional will produce a report giving an outcome of the assessments or test(s). This information is intended to be used by management to review your fitness for work; consider any adjustments or restrictions that need to be in place for your safety or wellbeing purposes, or to promote your optimum potential; and/or to determine whether there are any health and safety concerns relating to your exposures at work, the way you work and/or the control measures employed that need to be addressed.

Advice given in the report is usually expressed in terms of fitness to work but may include some medical information where this illustrates the fitness to work decisions. Openness in many cases can result in a greater understanding and support for you, however your consent will be required to release this medical information and the Occupational Health professional will discuss the implications of the report with you before gaining your written consent to release the medical information to your employer using a Consent to Release form or email. We will not release medical information to your employer without your consent to do so*

We may also use the information to arrange any further appointments, to support an application for ill health retirement, to ensure follow-up healthcare with another health care professional, to

contact you further in relation to the nature of the referral or its outcomes, or for clinical supervision and quality audit.

Details of the service provided to you, but not clinical information will be used for internal invoicing purposes, shared with your employer's representative but not shared with your employer's finance department.

The information may also be used for customer surveys; however, you are required to opt into this processing purpose.

We will not use your information for marketing or share it with others without your knowledge or consent*.

*It should be noted that the Occupational Health team does have a professional and ethical responsibility to act on information where there is a risk to others identified during the assessment. This may involve discussions with third parties such as your employer, your health care provider, or governing bodies such as DVLA. You will be advised of this.

Consent to release medical information

The consent to release form or email intends to fulfil our professional duty of confidentiality as required by the Access to Medical Reports Act 1988 and not the General Data Protection Regulations 2018. Your rights under the Act and their implications are given below:

1. You are free to decide to withhold your consent for the release of medical information in your occupational health or health surveillance report. Occupational Health is, however, sometimes unable assist you and your employer with the identification of steps that can be taken to help you at work without this further information and your employer is entitled to make a decision regarding your future employment based on the information that they have.
2. You are entitled to ask us to amend the report should you consider it to be factually inaccurate before sending it to your employer. The report gives the opinion of the Occupational Health Professional in relation to the management questions and should not be edited to give your opinion or that or your relatives/advisors. If you wish for additional information to be provided to your employer, you are able to contact them yourself directly.
3. If you refuse to consent to release the report, Peritus Health Management will advise your employer that consent to release the report has not been provided. A basic report on your fitness to work status, without detail may be provided to you and your employer and your employer is entitled to make a decision based on the information in their domain. The absence of detailed occupational health information could disadvantage any rehabilitation planning or negotiations with your employer.

Sharing Information

If we identify concerns about your health, we may refer our concerns to another health care professional, such as a Consultant Occupational Physician or Clinical Supervisor, for guidance. The information will be managed as confidential medical/sensitive data in accordance with legal and medical professional guidance.

If we identify concerns about your health that needs further investigation through the NHS, we may recommend that the information gained is shared with your GP to support this process. You will be informed that this is happening and the reasons for the concerns.

You will be made aware of the contents of the feedback reports and we will request your consent to release any medical information within the report*.

Access to your information and correction

You have the right to request a copy of the information that we hold about you. We want to make sure that your personal information is accurate and up to date. You may ask us to correct any information you think is inaccurate.

To protect you from physical or mental harm when reading your records, your Occupational Health Professional may withhold information if they consider it could be harmful to you. This is very rare.

You are able to gain copies of your occupational health records by applying in writing directly to the Data Protection Officer at Peritus Health Management at the email or address below, confirming your name, date of birth and current address and providing evidence of your identity and address, such as a utility bill or driving license. This additional information will be retained with details of the access request for up to 6 years in case we need to refer to it for legal purposes. A form is available from Peritus Health Management's Data Protection Officer that allows your employer to confirm your details and identity if you do not wish to provide additional documentation.

Retention Periods

The retention period of occupational health records will depend on the type of assessment undertaken. Health records relating to health surveillance for exposure to noise, vibration or substances hazardous to health must be kept for 40 years from the date of last entry in accordance with legal requirements. These will not contain medical information and will be stored by your employer and not Peritus Health Management. Health records relating to exposure to lead must be stored for 50 years from the date of last entry in accordance with legal requirements. Clinical records relating to fitness to work assessment not containing any health surveillance information will be stored for up to 10 years following date of leaving employment and then erased. You do not have the right to request that these records are deleted before the retention period identified above as we are may rely on this information for the defence of legal claim.

Any further questions

If you have any questions relating to this process, please contact the Data Protection Officer on dpo@peritushealth.com and put in the title box, FAO Data Protection Officer. Please identify how you would like use to contact you in the main body of the text and the nature of your enquiry.

Appendix 3 – Data Sharing Agreement

Company Name: Address: Telephone Number:	
Key Contact name: Email:	

This document confirms the data sharing agreement and arrangements with Peritus Health Management in relation to the provision of occupational health and occupational hygiene services to the above-named company and confirms the acceptance of the agreement.

Confidential occupational health and occupational hygiene reports are sent by encrypted email using winzip or through secure link. For encrypted email, the password is the first 4 letters of your domain name followed by the date the email was sent in a ddmmyy format with no dots or dashes. For example for admin@peritushealth.com, the password prefix is **peri** and if the email was sent on 1 January 2018, the password would be peri010118.

Please check with your IT department that you are able to receive encrypted emails from our email account. Peritus Health Management is not responsible for the loss of security to confidential occupational health or occupational hygiene reports sent unencrypted where (Customer) is unable to receive encrypted emails.

You may wish to set up a group email account for your HR department so that more than one responsible persons are able to receive the reports in case of holidays / absence.

Clinical reports to be forwarded to email:	
Addressee name and title:	

Emergency contacts details for immediate sensitive concerns Addressee name, title, phone and email details:	

(Customer) is responsible for the security of occupational health or occupational hygiene reports forwarded on to others from this email address.

(Customer) is responsible for the secure transfer of personal and special category information to Peritus Health Management and intend to use the following methods:	

(Customer) is responsible for notifying Peritus Health Management of any changes in these arrangements.

Signed on behalf of the company: (sign and print) Position:	
Date:	
Signed on behalf of the Peritus Health Management: (sign and print) Position:	
Date:	

Introduction

Peritus Health Management and (Customer) recognise their legal and professional obligations for safe, effective and responsible data sharing in relation to the services provided by Peritus Health Management to (Customer) and intend to comply with the following legislation and professional guidance:

- General Data Protection Regulations 2018 (GDPR) (ICO, 2018)
- Data Sharing Code of Practice (ICO, 2011)
- Access to Medical Reports Act 1989 (AMRA)
- Access to Health Records Act 1990
- Human Rights Act 1998
- Nursing and Midwifery Council Code of Professional Standards of Practice and Behaviour (Nursing and Midwifery Council, 2015)
- Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012)
- Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016).

Whilst this document uses the language of the General Data Protection in relation to 'data sharing', it is acknowledged that this purpose of agreement is to confirm the responsibilities and arrangements for the distinct types of disclosure of data between Peritus Health Management and (Customer) and Peritus Health Management and other Data Controllers / Processors.

Key Requirements and Controls

Peritus Health Management and (Customer) recognises and will abide by the 6 key principals of data protection required by Article 5 of the GDPR and other legal and professional guidance identified above. In order to achieve this in connection with the provision of occupational hygiene and occupational health services, the following joint arrangements will be implemented for 6 GDPR key principals listed below. Specialist arrangements for clinical records will also be implemented by Peritus Health Management and identified Clinical Records Management section below.

1. Lawful, fair and transparent processing of personal data in relation to individuals.

(Customer) is responsible for the lawful, fair and transparent processing of personal and special category data in their domain, in relation to individuals.

Peritus Health Management is responsible for the lawful, fair and transparent processing of personal and special category data in their domain.

Data sharing between Peritus Health Management and (Customer) will reflect legal and professional guidance and the arrangements for sharing will be reviewed on a regular basis by a representative of Peritus Health Management and (Customer).

Non-conformances against the data sharing agreement will be reported to the Data Protection Officers for Peritus Health Management and (Customer), investigated by both parties and corrective action will be identified in a report to the Contract Co-ordinator and Data Protection Officer of (Customer) and the Managing Director and Data Protection Officer of Peritus Health Management.

All types of personal and special category data shared between Peritus Health Management and (Customer) are identified the Data Sharing section below which identifies the lawful basis for which the data is processed.

All data subjects will be informed about the purposes and manner of personal data processing in a Data Protection and Privacy Notice issued by (Customer) prior to referral. Data subjects may also be required to confirm the accuracy of the information shared with Peritus Health Management by (Customer) prior to referral.

All data subjects will be informed about the content of any report relating to the purpose and outcome of the service received, produced by Peritus Health Management and where it contains medical information or a detailed occupational health opinion, the data subject will be consulted on its contents and accuracy, have the opportunity to request rectification of inaccuracies of information, be required to consent to the release of any medical information, and have the opportunity to decline the release of the report once completed. Data subjects are not able to amend the opinion of the occupational health professional on their fitness for work and advised restrictions.

The DPOs of Peritus Health Management and (Customer) are responsible for monitoring activities highlighted in this Data Sharing Agreement to ensure compliance.

2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Peritus Health Management and (Customer) will ensure that data is not processed for any other purpose than that identified in the Basis for Sharing section below.

Peritus Health Management and (Customer) confirm that processes are in place to manage the creation, storage, sharing, transfer, and deletion of data in a secure and efficient manner and that all staff processing data have been provided with training so that they competently undertake their workplace activities with due regard to the requirements and principals of legal and professional obligations and this Data Sharing Agreement.

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Peritus Health Management and (Customer) will ensure that the data joint controlled will remain limited to what is necessary in relation to the purpose identified in the Data Sharing section above through the regular review of this agreement, business and clinical practices, and standardised forms used by both parties; regular training of staff; and regular audit.

(Customer) is responsible for the creation and maintenance of individual health records for each employee placed under health surveillance. These should include details about the employee and the health surveillance procedures relating to them. Details should include: surname; forename; gender; date of birth; permanent address including post code; national insurance number; date present employment started. Recorded details of each health surveillance check should include: the date they surveillance was carried out and by whom; the outcome of the test/check; the decision made by the occupational health professional in terms of fitness for task and any restrictions required. The fitness for work and restrictions information will relate to an employee's functional ability and fitness for specific work, with any advised restrictions. The record should be linked with other information such as exposure records; occupational hygiene exposure monitoring reports.

4) accurate, and where necessary, kept up to date

Peritus Health Management and (Customer) will ensure that the data processed and controlled will be accurate and kept up to date by:

- rectifying inaccurate data within 1 month of request, unless there is a substantial reason for not doing so (expressions of opinion on which decisions have been made should not be deleted or amended if mistaken, but a comment will be added to the notes)

- checking with data subjects during contact, the accuracy of commonly changed data (address, phone number, email address, job titles)
- seeking a regular update of data subject status and data from customers so that data can be archived appropriately
- advising joint data controllers of inaccuracies in data supplied to allow them to amend records within 1 week of identification.
- (Customer) providing Peritus Health Management with lists of leavers on a regular basis.
- (Customer) arranging for the transfer of records to a new provider as appropriate when Peritus Health Management services are no longer required.

5) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed

(Customer) is responsible for the storage of occupational hygiene reports and individual health records (not clinical records) for all their employees exposed to substances and conditions at work that are hazardous to health and those under health surveillance. These records are important as they allow links between exposure and any health effects. Copies should be kept in a reasonably format for at least 40 years from the date of last entry because often there is long-period between exposure and onset of ill health.

The retention periods for the categories of data processed by Peritus Health Management are given below:

- Exposure monitoring information will be stored for 6 years from the monitoring ceases where the record is representative of the personal exposure of customer employees reviewed, and if no longer needed, destroyed. (Customer) is advised to store the reports for a period of 40 years from date of monitoring.
- Occupational Health clinical records will be retained for 6 years after leaving or date of last entry where there is no continued contract with the employer, reviewed, and if no longer needed, destroyed.
- Health surveillance records will be retained for 10 years from the date of last entry, reviewed, and if no longer needed, destroyed. (Customer) is advised to store the health surveillance report as a health records for a period of 40 years from date of last entry.
- Radiation related health surveillance records will be retained for 10 years from the date of last entry, reviewed, and if no longer needed, destroyed. (Customer) is advised to store the health surveillance report as a health records for a period of 50 years from date of last entry.
- Clinical audit records will be retained for 5 years, reviewed, and if no longer needed, destroyed.
- Clinical equipment inspection maintenance and calibration logs will be retained for 10 years, reviewed, and if no longer needed, destroyed
- Calibration records of exposure monitoring and health surveillance activities, to be retained for 10 years following completion of the test, reviewed and if no longer required, destroyed. (Customer) is advised to store the health surveillance report as a health records for a period of 40 years from date of last entry.
- Recorded conversation which may be later needed for clinical negligence purpose will be retained for 3 years following creation, reviewed, and if no longer needed, destroyed. Recorded conversation which forms part of the health record will be stored as a heath record.
- Subject access requests and disclosure correspondence will be retained for 3 years following the closure of the SAR, reviewed and if no longer needed destroyed.
- 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.

Where Peritus Health Management is notified that an employee has left employment with (Customer), Peritus Health Management will review the employee's data and archive according to retention periods above.

Where (Customer) is no longer in contract with Peritus Health Management through change of supplier where the data subject has declined to transfer the records, or dissolvement, the date of last entry will be used as a reference point for retention periods rather than the date of leaving employment.

6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures

Peritus Health Management has identified suitable and sufficient technical, physical and organisational measures to ensure the appropriate security of hard (paper) and soft (electronic) data. The security measures are identified in the Information Security and the Transfer of Records section below.

All clinical information is stored electronically within UK data centres.

All personal information is stored electronically within EU data centres.

(Customer) will ensure the restricted access of occupational health reports and the appropriate security of hard (paper) and soft (electronic) data.

Data Sharing

Data sharing between Peritus Health Management and (Customer) takes the form of:

1) systematic, routine data sharing where the same data sets are shared between (Customer) and Peritus Health Management for the following established purposes:
   a) referring employees to Peritus Health Management to gain an opinion of fitness for work and adjustments or restrictions recommended and/or to undertake a health risk assessment to assist (Customer) in fulfilling their duty of care towards the employee(s) and legislative responsibility under the Equality Act at the commencement of employment, or identified periods during employment.
   b) referring employees to Peritus Health Management to undertake statutory health surveillance programmes of employees on behalf of (Customer) to aid employees with the early detection and management of disease, to assist (Customer) in undertaking a health risk assessment to fulfil their duty of care towards the employee(s) and to review the suitability and sufficiency of health and safety control measures.
   c) referring employees to Peritus Health Management to undertake biological monitoring of employees on behalf of (Customer) to assist (Customer) in undertaking a health risk assessment to fulfil their duty of care towards the employee(s) and to review the suitability and sufficiency of health and safety control measures.
   d) referring employees or groups of employees to Peritus Health Management to investigate workplace exposure, undertake personal exposure monitoring, advise on health risks and appropriate control measures, on behalf of (Customer), to review the suitability and sufficiency of health and safety risk management.
   e) referring employees or groups of employees to Peritus Health Management to undertake drugs and/or alcohol testing on behalf of (Customer) in order to measure breath alcohol levels and urine drug levels so they are able to make a decision regarding their work capability in relation to (Customer)'s Drugs and Alcohol Policy.

f) referring employees to Peritus Health Management to undertake an assessment of employees' health and work capability in relation to Pension Fund ill health retirement criteria to support an application for early retirement on the grounds of ill health.
g) referring employees to Peritus Health Management to undertake an assessment of the suitability and sufficiency of employees' respiratory protective equipment face fit to ensure the suitability and sufficiency of this health and safety control measure.
h) referring employees to Peritus Health Management to undertake an aural impression of an employee for the supply of personal moulded hearing protection.

2) exceptional, one-off decisions to share data for guidance on health, safety or wellbeing related concerns.

Basis and arrangements for Data Sharing

(Customer) and Peritus Health Management have a mutual legitimate interest for sharing personal contact data for those involved in the administration of the contract between them.

(Customer) is responsible for informing its employees about the contract between Peritus Health Management and (Customer) for the provision of occupational health and occupational hygiene services through general terms e.g. on their intranet, and specific terms, by the provision of a Privacy Notice with every referral to Peritus Health Management.

Peritus Health Management will check to ensure that privacy notices have been issued to (Customer)'s employees during the course of their service delivery.

The basis and arrangements for data sharing between Peritus Health Management and (Customer) are given per item of service below:

Referring employees to Peritus Health Management for (Customer) to gain an opinion of fitness for work

Purpose: referring employees to Peritus Health Management to gain an opinion of fitness for work and adjustments or restrictions recommended and/or to undertake a health risk assessment to assist (Customer) in fulfilling their duty of care towards the employee(s) and legislative responsibility under the Equality Act at the commencement of employment, or identified periods during employment. For Peritus Health Management to provide a report giving an opinion of fitness for work and adjustments or restrictions recommended and/or to undertake a health risk assessment.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) to refer to Peritus Health Management to establish the fitness for work status of (Customer)'s employees as it assists in fulfilling (Customer)'s duty of care towards their employee(s) by considering specific hazards and risks within the workplace and ensuring that the employee(s)' health status does not place them at risk undertaking these work activities.

Example: Employees' working at heights or in confined spaces are considered 'safety critical work' and should not be affected by: sudden loss of consciousness or incapacity; impaired balance, mobility, concentration or awareness. The fitness to work assessment also ensures that the employees' health status, when undertaking specific work activities, does not place others at risk of harm.

Employees' driving vehicles should meet the DVLA fitness to drive standards. Crossing Patrol Officers should meet vision and hearing standards. Teacher should meet the Fitness to Teach standards.

The fitness to work assessment also offers the opportunity to determine whether employees' are more at risk from specific hazards due to pre-existing or new health conditions which may

require adjustments or restrictions putting in place to protect the employee(s) and allow them to achieve their optimum potential, fulfilling legislative responsibility under the Equality Act.

Examples: Employees identified with upper limb disorders may require specific workstation set-up. Employees with mental health problems may require a 'buddy system' and regular management reviews to ensure that they are coping with their workload. Employees with hearing problems may require vibrating or visual fire alarm alerts, adapted telephones, loop systems for training.

Article 9 Lawful Basis for Special Category Data: This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Date of Birth, Address, Job Title and description of duties, Telephone Contact Details, Leaving Date. Information specifically related to the referral may include: Sickness Absence History Outstanding Management Issues; Adjustments / Restrictions to duties implemented; Action Taken by Management; Pertinent details of discussion; Risk assessments.

The information shared with (Customer) by Peritus Health Management may include: medical context (with consent to release of the employee only); functional capacity; opinion of fitness for work; adjustments, recommendations or restrictions suggested; information relating to opinion on health risks and health risk management; opinion on disability status.

3rd party sharing: Peritus Health Management may share information relating to the assessment with a contracted Occupational Health Physician or Clinician, to undertake the assessment or for clinical support. All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Peritus Health Management may also share personal and special category information with specialist providers such as Cognitive Behavioural Therapists or Physiotherapists where the Customer and/or Client (Customer employee) has confirmed they wish to be referred to the 3rd party. This sharing of information will be confirmed by the Customer in the request for referral and by the client by consent form.

Information Used For: identification of employee, records maintenance, invoicing, quality management, assessing health status and work capacity in relation to job requirements and establishing fitness for work, restrictions and adjustments duty are required or recommended in order to protect the employee and allow them to achieve their optimum potential.

Peritus Health Management Retention Period: 6 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: company policy but a recommended 6 years after leaving as a minimum.

Referring employees to Peritus Health Management to undertake statutory health surveillance programmes

Purpose: referring employees to Peritus Health Management to undertake statutory health surveillance programmes of employees on behalf of (Customer) to aid the employee with early detection and management of disease, to assist (Customer) in reviewing health risk assessment to fulfil their duty of care towards the employee(s) and to ensure the suitability and sufficiency of health and safety control measures

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to undertake a health risk assessment and health surveillance review the suitability and sufficiency of health and safety control measures as it assists in fulfilling their duty of care towards the employee(s) and others who may be harmed by a failure to do so.

Examples: Employees exposed to loud noise will require hearing tests to detect the onset of noise-induced hearing loss and changes in hearing status should lead to a review noise control measures. Employees exposed to significant amounts of wood dust will require breathing tests: concerns identified will be investigated further and should lead to a review of exposure control measures and the health risk assessment.

Article 9 Lawful Basis for Special Category Data: This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Job Title, Area of Work, Leaving Date. Information specifically related to the referral may include: workplace practices and exposures, personal protective equipment issued.

The information shared with (Customer) by Peritus Health Management may include: medical context (with consent to release of the employee only); functional capacity; opinion of fitness for work; adjustments, recommendations or restrictions suggested; information relating to opinion on health risks and health risk management; opinion on disability status.

Outcomes of the health surveillance where concerns are identified may be shared internally with the occupational hygiene team to gain specialist insight for the customer relating to health risks and health risk management.

3rd party sharing: Peritus Health Management may share information relating to the assessment with a contracted Occupational Health Physician or Clinician, to undertake the assessment, for clinical supervision or to aid further clinical investigation.

Peritus Health Management may also share information relating to the assessment with a Consultant Specialist (e.g. Consultant Chest Physician or Consultant Dermatologist) for clinical support and to aid further clinical investigations.

All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Information Used For: identification of employee, records maintenance, invoicing, quality management, early detection of disease; assessment of fitness for work; and review of suitability and sufficiency of health and safety control measures.

Peritus Health Management Retention Period: 10 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: 40 years after leaving or date of last entry

Referring employees to Peritus Health Management to undertake biological monitoring

Purpose: referring employees to Peritus Health Management to undertake a biological assessment to establishing whether there are any biological indicators of exposure so that (Customer) can review the suitability and sufficiency of their health and safety control measures.

Examples: Employees working with isocyanate paints or exposed to welding fume should have their urine tested for evidence of exposure and if present, the control measures and health risk assessment should be reviewed.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to review biological measurements to determine the suitability and sufficiency of health and safety control measures as it assists in fulfilling their duty of care towards the employee(s) and others who may be harmed by a failure to do so.

Article 9 Lawful Basis for Special Category Data: This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Job Title, Area of Work, Leaving Date. Information specifically related to the referral may include: workplace practices and exposures, personal protective equipment issued if further investigation is required.

The information shared with (Customer) by Peritus Health Management may include: biological monitoring results; recommendations or restrictions suggested; information relating to opinion on health risks and health risk management.

3rd party sharing: Peritus Health Management will share information relating to the identification of those who have had exposure monitoring with a Scientific Laboratory to aid the chain of custody analysis of the samples taken.

All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Information Used For: identification of employee, records maintenance, invoicing, quality management, early detection of disease; assessment of fitness for work; and review of suitability and sufficiency of health and safety control measures.

Peritus Health Management Retention Period: 10 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: 40 years after leaving or date of last entry.

Referring employees or groups of employees to Peritus Health Management to investigate workplace exposure, undertake personal exposure monitoring, advise on health risks and appropriate control measures

Purpose: referring employees to Peritus Health Management to undertake a personal exposure monitoring to establishing whether there are any indicators of exposure so that (Customer) can review the suitability and sufficiency of their health and safety control measures.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to review personal exposure measurements to determine the suitability and sufficiency of health and safety control measures as it assists in fulfilling their duty of care towards the employee(s) and others who may be harmed by a failure to do so.

Examples: Employees working in a food factory making pies have their personal exposure to flour dust monitored over a representative period and the results used to review whether the

methods of work can be adjusted to reduce the exposure, local exhaust ventilation is suitable and sufficient for controlling risk and whether health surveillance is required.

Employees working in a manufacturing site have their personal exposure to noise and work processes monitored over a representative period and the results used to review whether the methods of work or control measures can be adjusted or improved to reduce exposure, whether the hearing protection supplied is appropriate and whether health surveillance is required.

Article 9 Lawful Basis for Special Category Data: This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Job Title, Area of Work. Information specifically related to the referral may include: workplace practices and exposures, personal protective equipment issued if further investigation is required.

The information shared with (Customer) by Peritus Health Management may include: exposure monitoring results; recommendations or restrictions suggested; information relating to opinion on health risks and health risk management.

3rd party sharing: Peritus Health Management will share information relating to the identification of those who have had exposure monitoring with a Scientific Laboratory to aid the chain of custody analysis of the samples taken.

All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Information Used For: identification of employees, records maintenance, invoicing, quality management, and review of suitability and sufficiency of health and safety control measures

Peritus Health Management Retention Period: 10 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: 40 years after leaving or date of last entry

Referring employees or groups of employees to Peritus Health Management to undertake drugs and/or alcohol testing on behalf of (Customer) in order to measure breath alcohol levels and urine drug levels so they are able to make a decision regarding their work capability in relation to (Customer)'s Drugs and Alcohol Policy.

Purpose: referring employees to Peritus Health Management to establish whether there are measurable indications of drugs and alcohol use in accordance with professional guidelines (European Workplace Drug Testing Society, 2015).

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to establish the drug or alcohol status of their employee(s) to fulfil the employer's contractual requirements to their customer(s), establish the existence of any health or safety risks arising from the use of drugs or alcohol on work capacity as it assists in fulfilling their duty of care towards the employee(s) and others who may be harmed by a failure to do so and act as a deterrent. Peritus Health Management requires the employee to consent to the processing of the drugs and alcohol test and the release of the outcome of the test to the employer.

Examples: An employer may be required by their customer, a Power Station, to ensure that their employees have had a drug and alcohol test on a regular basis to demonstrate they are fit to work in a 'safety critical' environment. Peritus Health Management undertakes the tests with the consent of the employee and provides a report to the employer.

A construction team may be required to demonstrate that they are drug and alcohol free following a significant incident at work. Peritus Health Management undertakes the tests with the consent of the employee and provides a report to the employer.

Article 9 Lawful Basis for Special Category Data: This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Leaving Date

The information shared with (Customer) by Peritus Health Management may include: medical context (with consent to release of the employee only); outcome of tests; whether further chain of custody testing is required.

3rd party sharing: Peritus Health Management will share information relating to the identification of those who have had exposure monitoring with a Scientific Laboratory to aid the chain of custody analysis of the samples taken.

All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Information Used For: identification of employee, records maintenance, invoicing, quality management, and reporting on outcome as per purpose.

Peritus Health Management Retention Period: 10 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: Company policy but a recommended 6 years minimum after leaving or date of last entry.

Referring employees to Peritus Health Management to undertake an assessment of employees' health and work capability in relation to Pension Fund ill health retirement criteria to support an application for early retirement on the grounds of ill health.

Purpose: referring employees to Peritus Health Management to gain an opinion of fitness for work and adjustments or restrictions recommended and establishing whether they meet the Pension Fund's criteria for early retirement on the grounds of ill health.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) to refer to Peritus Health Management to establish the fitness for work status of (Customer)'s employees in relation to Pension Fund's criteria for early retirement on the grounds of ill health.

Peritus Health Management will contract with the employee directly to undertake the assessment, communicate with their health care providers, and provide information to the pension fund provider and employer on the outcome of the assessment.

Example: An employee has been diagnosed with bowel cancer, wishes to apply for ill health retirement and is in two different pension funds: one managed by the current employer and one managed by previous employers. Peritus Health Management will require consent from the employee to approach their health care providers to confirm diagnosis, treatment provided and future options, prognosis and impact on activities of daily living. Peritus Health Management will also require consent from the employee to provide information to both pension fund providers for them to assess against their criteria for ill health retirement. Peritus Health Management will also require consent from the employee to release a detailed report to the current employer to confirm their fitness for work status. If the information from the health care professionals indicates that there is a possibility that the employee will be fit to return to work after their treatment and therefore they do not meet the criteria for ill health retirement, but the individual does not wish this detailed information to be released to the employer, Peritus Health Management will be required by the terms of the contract to advise the employer of the outcome of the assessment and the employees fitness for work status.

Article 9 Lawful Basis for Special Category Data: Article 9(2)(h) – This data is processed under Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; & Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, or pursuant to contract with a health professional.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Date of Birth, Address, Job Title and description of duties, Telephone Contact Details, Leaving Date. Information specifically related to the referral may include: Sickness Absence History Outstanding Management Issues; Adjustments / Restrictions to duties implemented; Action Taken by Management; Pertinent details of discussion; Risk assessments.

The information shared with (Customer) by Peritus Health Management may include: medical context (with consent to release of the employee only); functional capacity; opinion of fitness for work; adjustments, recommendations or restrictions suggested; information relating to opinion on health risks and health risk management; opinion on disability status, opinion on eligibility for early retirement on the grounds of ill health.

3rd party sharing: Peritus Health Management will share information relating to the assessment with a contracted Occupational Health Physician or Clinician, to undertake the assessment.

Peritus Health Management will also share information relating to the assessment with the employee's treating health care professional in order to gain the information required for the assessment.

Peritus Health Management will share information with the Pension Fund Provider(s) as they will require the information to process the ill health retirement application.

All 3rd parties contracted to provide services on behalf of are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above. Peritus Health Management is not responsible for the processing of data by the Pension Fund Provider or the employee's health care provider.

Information Used For: identification of employee, records maintenance, invoicing, quality management, assessing health status and work capacity in relation to job requirements; establishing fitness for work in relation to the Pension Fund's criteria for early retirement on the grounds of ill health; supporting application for early retirement on the grounds of ill health.

Peritus Health Management Retention Period: 6 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: Company policy however a 6 years minimum after leaving or date of last entry is recommended.

Referring employees to Peritus Health Management to undertake an assessment of the employees' respiratory protective equipment face fit

Purpose: referring employees to Peritus Health Management to establish whether there are qualitative indications that the respiratory protective equipment issued to employees is suitable and sufficient and fulfils (Customer)'s duty of care to the employees.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to establish the suitability and sufficiency of this control measure.

Example: The employer refers an employee to Peritus Health Management for a face fit test. Peritus Health Management undertakes the test and provides the employer with a certificate to confirm face fit.

Article 9 Lawful Basis for Special Category Data: Special category data is not processed for the purpose of this service delivery.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name, Leaving Date

The information shared with (Customer) by Peritus Health Management may include: outcome of face fit test of respiratory protective equipment and method used for testing.

3rd party sharing: There is no 3rd party sharing of information in relation to this service provision.

Information Used For: identification of employee, records maintenance, invoicing, quality management, and confirming suitability and sufficient of the respiratory protective equipment.

Peritus Health Management Retention Period: 10 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: 40 years after leaving or date of last entry.

Referring employees to Peritus Health Management to undertake an aural impression of an employee for the supply of personal moulded hearing protection.

Purpose: referring employees to Peritus Health Management to undertake an aural impression of an employee for the supply of personal moulded hearing protection.

Article 6 Lawful Basis for Processing Personal Data: it is the in the legitimate interest of (Customer) for Peritus Health Management to process this data on their behalf so that they can arrange for the supply of personal moulded hearing protection.

Article 9 Lawful Basis for Special Category Data: Special category data is not processed for the purpose of this service delivery.

Information Shared: the information shared with Peritus Health Management by (Customer) includes: Name and Leaving Date

The information shared with (Customer) by Peritus Health Management may include: completion of aural impression.

3rd party sharing: Peritus Health Management may share information relating to the individual's identity with the supplier of the aural impressions to ensure the customised hearing protection is based on the correct aural impression and supplied to the correct individual.

All 3rd parties are vetted by Peritus Health Management and contracted to abide by the GDPR, and other legal and professional guidelines as identified above.

Information Used For: identification of employee, records maintenance, invoicing, quality management, and supply of aural impressions.

Peritus Health Management Retention Period: 6 years after leaving or date of last entry where there is no continued contract with the employer.

(Customer) Retention Period: 6 years after leaving or date of last entry.

Adhoc or 'one-off' sharing of data

Where situations arise that requires the sharing of data not covered by a routine agreement, this should be done in a way which ensures the anonymity of the individual involved e.g. discussing specific details but not individuals. Where this is not possible, the parties involved in the sharing of data, will determine beforehand whether they have the legal power or ability to do so, agree the basis for the sharing.

Records detailing the circumstances, what information was shared and explaining why the disclosure took place should be made.

Clinical Records Management

Employees undertaking clinical work on behalf of Peritus Health Management are required to take and maintain full, factual, contemporaneous, dated notes. They are responsible for the accuracy of the records and the implementation of the storage of records in accordance with this policy. The Clinical Record Keeping Standard applied in Peritus Health Management is documented our Clinical Record Keeping Standards which is adapted from the Records Management Code of Practice for Health and Social Care (Information Governance Alliance, 2016) and available in appendix 6 of the Information Governance Policy on www.peritushealth.com/informationgovernance.

The individual occupational health (clinical) record is a confidential medical record to which the principles of medical confidentiality as defined by the Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians (Faculty of Occupational Medicine, 2012) and the Nursing and Midwifery Council Code (Nursing and Midwifery Council, 2015) applies. This is in addition to the requirements of the GDPR.

The lawful basis for processing this data and the rights available to individuals (data subjects) are identified in the Privacy Notices for each item of service (appendix 1) and in Peritus Health Management's Information Audit.

In communicating with (Customers) on the health of their employees, unless informed consent to release has been given to release specific health-related details, the outcome of the health assessment (fitness for work) rather than clinical details will be given. To gain client's (Customer's employee) consent to release the health-related details, Peritus Health Management's clinician will discuss the contents of this report with the client and the implications of releasing that information, and confirm the client's consent to release the health-related data contained in the report using a Consent to Release Medical Information form, or by seeking a response to an email detailing the individual's rights under the Access to Medical Reports Act.

Whilst consent to release health-related information is still required, this does not affect the lawful basis on which the data has been processed which is identified in the Basis and Arrangements for Data Sharing section above and Privacy Notice for that item of service. Should a client refuses consent to release the information, a simple statement on fitness to work, referring only to information already in the domain of the recipient for context if required, will be provided.

Employees of Peritus Health Management are responsible for all clinical data, whether held manually or electronically, processed for the duties for which they are employed, and they will ensure the security of that data, and the hardware on which it is processed at all times.

Unrestricted access to clinical data is confined to those undertaking clinical duties and those undertaking administrative support duties where it can be demonstrated that they are fully aware of their personal responsibility to keep all clinical information confidential.

The Managing Director of Peritus Health Management is responsible for ensuring all employees of Peritus Health Management are aware of their responsibilities under this policy and that all employees confirm their understanding and agreement to this policy by signing an Information Governance and Confidentiality Statement. This will be reviewed on a regular basis.

(Customer) is responsible for ensuring all its employees are aware of their responsibility under this policy and that they confirm their understanding and agreement in writing.

Clinical (Special Category - health related) data will not be released to others unless:

- the informed consent of the individual is provided in writing or, in exceptional circumstances, verbal consent where the verbal consent is witnessed and signed by 2 people. The reason for verbal consent release should be documented in the clinical records indicating the reason written consent could not be obtained;
- if the disclosure is clearly in the best interest of the individual, but it is not possible to seek consent;
- if there is a real concern that the health or safety of others is endangered;
- if it is required by law;
- if it is in the public interest.

To give informed consent the individual should clearly understand what information will be imparted, to whom, for what purpose and the possible outcomes which may result.

An employee of Peritus Health Management shall only disclose information, without the informed consent of the individual, where a failure to disclose information may expose others to the risk of death or serious harm, or in order protect the safety of other workers or the general public. This will only do so with consent from the Managing Director of Peritus Health Management (or their deputy), or under guidance from a medical defence organisation or professional body. The Managing Director of Peritus Health Management (or their deputy) will be advised of a disclosure made under guidance as soon as possible.

Where there is an immediate risk to the safety of the others, Peritus Health Management's employee should take formal action to prevent that risk, advising the client of their intention to do so, where by informing the client of this intention they do not put their own health and safety at risk. This process is identified in Appendix 5 of Peritus Health Management's Information Governance Policy, available on www.peritushealth.com/informationgovernance.

Where a client wishes access to their clinical records, the Peritus Health Management will follow procedure for submitting a request for information detailed below.

Submitting a request for information

Peritus Health Management will ensure, wherever appropriate, that a data subject has access to all records stored about them. Data subject should apply in writing to Peritus Health Management to request access to the records or copies of their records to be sent to them.

In order for Peritus Health Management to confirm the identity of the data subject, Peritus Health Management will may request evidence of identity prior to supply. The request for accessing occupational health data (appendix 2) can be used for this purpose.

Peritus Health Management will respond to such a request within 30 working days of receipt of the request. Peritus Health Management will provide an individual with an interpretation of information stored in the records where required.

Where a lawyer employed by a company or the data subject requests access to Occupational Health records, Peritus Health Management will ensure that written informed consent has been gained before disclosure. Where there are records related to other matters unrelated to the injury or issue in question, Peritus Health Management will clarify the consent with the data subject. An Order of Discovery will be required to gain access to records where consent is refused. The Order of Discovery will be checked for a stamp to clarify that this has been a confirmed court document.

Where a data subject consents to the release of only part of the Occupational Health records but refuses the release of other equally relevant parts, Peritus Health Management will advise the solicitors of both parties that all the records relevant to the case have not been made available to both sides. Records will not be released in these circumstances without consent or an Order of Discovery.

Applying for confidential medical information

Where Peritus Health Management requires a report from a health care professional responsible for the clinical care of a client (Customer's employee), the Access to Medical Reports Act applies. The Clinician managing the case will explain to the client their rights under the Access to Medical Reports Act as part of the process of obtaining informed consent.

The clinician applying for the confidential medical information is responsible for ensuring that the data subject is aware of the information sought from the health care professional and will send a copy of the request to the data subject at the same time as to the health care professional.

Information Security

Peritus Health Management is responsible for the security of data held or transferred by Peritus Health Management.

(Customer) is responsible for the security of data held or transferred by (Customer).

Physical Security

Peritus Health Management's premises have good quality access control systems and CCTV in operation for security purposes.

There are additional locks to Administration areas and visitors are not able to access administration areas without supervision.

Hard (paper) data

Peritus Health Management does not store hard (paper) copy documents for prolonged periods. All hard copy documents are scanned and stored electronically on a Cloud-based system.

Peritus Health Management use secure transportation envelopes to carry of hard (paper) copy documents from site to the main office where they are stored in locked cabinets until scanned electronically. Access to the cabinets will be restricted to those undertaking administrative support duties and clinical personnel only. Keys will be kept secure at all times.

All other paper records containing personal data will be documented in note books provided specifically for the documentation of work-related issues. Note books will be issued out and collected in by the DPO for safe disposal. No notebooks other than those issued by the DPO will be used for processing personal data. The note books will be stored in sealed document transport envelopes when away from Peritus Health Management's offices.

Paper records containing personal data are not be stored in any other location than those outlined above.

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 of confidential waste are stored electronically. Details of the Waste Carrier's License are recorded and a recall date set up to request an up to date license.

(Customer) and their representatives are responsible for the security, use and disposal of any hard (paper) copies of occupational health reports printed out by them for their use.

Soft (electronic) data

Personal and Special Category data is processed electronically by a number of different systems within Peritus Health Management and include:

10. email system
11. records storage system
12. recall system
13. customer relationship management system
14. clinical record database
15. clinical portal
16. finance management system
17. clinical equipment databases
18. occupational hygiene equipment software

Peritus Health Management contracts an IT Consultancy to provide a managed IT Services programme to the business to:

- assess the IT requirements of Peritus Health Management ensuring the secure and smooth functioning of IT related activities within the business and advise on the best solutions for the current and future business needs.
- protect the confidentiality, integrity and availability of data on behalf of Peritus Health Management and will organise, implement and maintain robust systems infrastructure and network security arrangements abiding by the principle and codes of practice defined by ISO 27001 as they apply to Peritus Health Management.
- maintain network consistency by installing applications, patches and updates required.
- create and maintain a site database of system hardware and software ensuring authenticity and currency of systems used
- ensure the currency of the IT asset inventory, that all assets are suitable, safe, maintained and fit for purpose

- ensure the safe governance and efficiency of software, applications and operating systems
- logging all systems and storing all audit logs for review as required
- ensure that all IT equipment will be decommissioned appropriately with regards to the erasing of stored information and provide a formal certificate of data erasure for each decommissioned asset.
- provide a review of Peritus Health Management's IT objectives on a quarterly basis to ensure

The IT Consultancy used for the maintenance of software and hardware are required to abide by the codes of confidentiality to ensure no inappropriate access to Special Category personal data.

Peritus Health Management uses a UK based datacentre for storage or processing of health-related data. Access to the data centre is restricted by access controls and alarms (including CCTV) and the information stored is encrypted so that any ghost prints of deleted data remain encrypted. The system is monitored for significant or unauthorised events and managed appropriately. Audit systems are in place and audit logs are maintained for a minimum of 12 months.

Information relating to the Business is stored on Customer Relationship Management software which uses a Belgium based datacentre for the storage or processing of customer (not client) and prospective customer related contact details and marketing information. Access to the data centre is restricted by access controls and alarms (including CCTV) and the information stored is encrypted so that any ghost prints of deleted data remain encrypted.

Peritus Health Management has a password management policy in place. Username and complex password authentication is required for access for all IT hardware. Password authentication is required for mobile devices. Passwords are required to be changed on a regular basis and reminders to users are automatically sent. Passwords and other access will be cancelled immediately a Peritus Health Management employee leaves the organisation or is absent for a prolonged period. Where there is a perceived significant risk to the security of data from Peritus Health Management employee, a Director will cancel access to the data and investigate appropriately.

Anti-virus and anti-malware products will be kept up to date and used to actively scan the IT devices to prevent or detect threats. Peritus Health Management employees are aware that removeable media must only be used with permission of a director. A firewall is in place to prevent unauthorised external entry into Peritus Health Management's network. This is reviewed and maintained on a regular basis. All these are monitored by the IT service contracted to the business. Peritus Health Management maintains a list of authorised software and this is monitored by the IT service contractor. Standardised configurations of operating systems and software applications are used. Patch management is deployed on a daily basis from IT support. Vulnerability scans are undertaken on a weekly basis.

Restrictions are in place on all IT equipment to prevent unauthorised up/downloading of software. Peritus Health Management employees are classed as users with no administration rights. Peritus Health Management Directors have Administration rights only. Unauthorised application upload onto company hardware or processing of personal / Special Category data onto unauthorised IT (including mobile devices) hardware is classed as gross-misconduct and will be managed in accordance with disciplinary procedures.

Peritus Health Management employees are not permitted to connect IT hardware (laptops) to 3rd party wireless networks without the permission of a Director and data tethering through company mobile devices is used for this purpose only.

Administrative privileges to stored records and systems are granted on a role-based need. These are checked on a regular basis in the IT review meeting to ensure that they remain current. Organisational Administrative access to the data is restricted to the directors of Peritus Health Management.

All data is backed up on a continuous basis and the back-up is encrypted and retained for 12 months. Peritus Health Management has a business continuity and disaster recovery plan in place for deployment in case of loss of data. The risk of total loss (erasure) of soft data has been assessed and is considered to be extremely low.

Peritus Health Management uses IDS systems for boundary defence. Continuous monitoring and alerts are set up to ensure all violations, unauthorised access and anomalous activities are logged, monitored, reviewed and addressed in a timely manner by the IT Consultancy.

Transfer of personal or Special Category data files out of Peritus Health Management and between users within Peritus Health Management are undertaken with secure file sharing or file encryption with password protection, unless with prior agreement from the data subject. Passwords are sent separately or a pre-agreed password formula is used.

(Customer) is responsible for arranging secure electronic transfer of personal or Special Category data files through encryption or secure file sharing from (Customer) to Peritus Health Management and between users within (Customer). Passwords should be sent separately or a pre-agreed password formula is used.

Bulk information transferred on completion of contract using memory sticks will be encrypted, password protected and deleted as soon as the transfer has been completed as per the Transfer of Records procedures below.

Access to data is not granted to 3rd parties by Peritus Health Management other than those identified in the Information Audit and Data Sharing Agreements for lawful purposes.

Mobile devices and IT equipment

Peritus Health Management maintains an inventory of all mobile devices and IT equipment owned by Peritus Health Management and connected to our network. All IT (including mobile devices) hardware is supplied to Peritus Health Management employees for company use only. Peritus Health Management employees receive training on the company IT usage policy.

Peritus Health Management uses full disk encryption on all computers used for processing personal or Special Category data.

Personal or Special Category data relating to Peritus Health Management's work activities will not be stored on any other devices other than those owned and maintained by Peritus Health Management.

The physical security of all IT (including mobile devices) hardware issued to Peritus Health Management employees are the responsibility of the receiving employees. Peritus Health Management employees will ensure that computers are securely stored at all times when they are not in their presence.

All IT equipment will have information erased correctly by the IT contractor. Formal notice of data erasure will be stored electronically.

All mobile devices will be reset to factory settings by Peritus Health Management before disposal. Formal declaration of the reset will be signed by the person undertaking the reset and the declaration stored electronically.

Transfer of records procedures

Peritus Health Management will only transfer Occupational Health records to an appropriate health professional who is able to provide:

- confirmation of a contract between the customer and the occupational health provider (a letter from the customer confirming the new provider's details and contact arrangements)
- sufficient evidence of consultation between the customer and its employees advising of the transfer of services, the opportunity to request for their clinical records to be archived rather than transferred and the future storage of records
- photographic evidence of identity of the professional receiving the records and evidence of current registration of the General Medical Council or Nursing and Midwifery Council, and who will sign to accept responsibility for the storage and maintenance of the Occupational Health records in accordance with the General Data Protection Regulations and the Faculty of Occupational Medicine's Guidance on Ethics for Occupational Physicians.

A list of all records transferred will be kept and stored. Electronic records will be transferred on an encrypted memory stick or secure link. Secure memory sticks will be checked by a second person to ensure that the records are encrypted on the stick. The stick will be sent by recorded delivery only and the track and trace record will be stored electronically and details of the track and trace provided to the recipient. The password will be provided to the recipient once they have confirmed receipt of the stick. A copy of the list of all records will be sent to the recipient.

Where a customer ceases to exist, the records will be retained for the standard periods with Peritus Health Management. Where a client provides a written request, these records may be transferred to the client's GP.

Breach of Data Protection

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. A data security breach may happen due to:

- loss of theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use
- equipment failure
- human error
- unforeseen circumstances such as fire or flood
- hacking attack

If a personal breach has occurred, the employee identifying the breach will advise the DPO of their organisation and / or other person depending on their policy, who will establish the likelihood and severity of the resulting risk to people's rights and freedoms. The range of adverse effects on individuals, including emotional distress, and physical or material damage, will be considered.

If there is a risk to people's rights and freedoms, the Managing Director or DPO in her absence will report the breach to the Information Commissioners Office and (Customer) no later than 72 hours after the becoming aware of the breach, following current guidance on the ICO website https://ico.org.uk/for-organisations/report-a-breach . The following steps will also be taken to manage the breach:

- recover the information and limit the damage the breach can cause;
- review security procedures to prevent further loss;
- report criminal activities;

- assess the potential detrimental effect the data subjects arising from the breach. This includes: physical and financial damage as well as emotional distress
- refer to the guidance on security breach management produced by the Information Commissioners Office to see whether the breach should be reported.

If the breach is likely to result in a high risk to the rights and freedoms of the data subject, the data subject(s) will be advised of the breach immediately.

Audit and review

Compliance with this Data Sharing Agreement will be audited by respective parties Data Protection Officers.

Feedback to (Customer) on the audit process will be included in the Utilisation Report.

This Data Sharing Agreement will be reviewed on a regular basis and with any identified changes in legal or professional guidance.

References

European Workplace Drug Testing Society. (2015, Nov 01). *European Guidelines for Workplace Drug Testing in Urine Version 2.0.* Retrieved from European Workplace Drug Testing Society: http://www.ewdts.org/data/uploads/documents/ewdts-urine-guideline-2015-11-01-v2.0.pdf

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

ICO. (2011, May). *Data Sharing Code of Practice.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

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

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

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

Appendix 4 – Information Governance and Confidentiality Statement

Background

Peritus Health Management recognises its responsibilities under the General Data Protection Regulations (GDPR) 2018, the Access to Medical Reports Act (AMRA) 1988, the Access to Health Records Act 1990 and professional guidance. The framework for the way Peritus Health Management handles information is set out in the Information Governance Policy.

Summary of Policy

The aims of the Information Governance Policy are to:

- Attest to Peritus Health Management's intention to comply with all relevant legislative and professional requirements, thereby protecting individuals, the organisation and its employees
- Direct all our Information Governance across Peritus Health Management and its interactions with our associate Data Controllers, Data Processors, and Data Subjects.
- Confirm the processes in place to manage the creation, storage, sharing, transfer, and deletion of data in a secure and efficient manner
- Ensure the continued provision of high quality service delivery by defining and promoting the effective and appropriate use of data
- Confirm that roles and responsibilities of all data controllers and processes within Peritus Health Management and associated with their data control and ensure their compliance to legal and professional obligations.

The Information Governance Policy applies to all employees and non-employees - clinical and administrative, whether temporary, permanent or contracted. Non-compliance of the policy may be considered as gross misconduct and could result in summary dismissal and/or reporting to the Information Commissioner. In addition, clinical staff that breach confidentiality will be reported to their professional body. All data which relates to a living individual who can be identified must be treated as personal data in accordance with the GDPR and is confidential.

Clinical staff should read, understood and adhere to the guidelines on information governance, Ethics Guidance issued by the Faculty of Occupational Medicine and standards of practice relating to confidentiality and record keeping issued by their professional bodies (General Nursing Council, Nursing and Midwifery Council etc).

Non-clinical staff should understand their responsibilities under this policy and the requirements of the clinical guidelines on confidentiality and medical ethics as it applies to their duties.

All staff must receive training on their responsibilities under the Information Governance Policy and confirm their understanding in writing.

General Principles of the Information Governance Policy

1. All personal data shall be processed lawfully, fairly, and in a transparent manner in relation to individuals. Employees and clients will be provided with Privacy Notices explaining their rights relating to the processed data. Clinicians must record in the notes that the client has received a copy of the Privacy Notice.
2. All personal data shall be collected for specified, explicit and legitimate purposes. Data must not be used for purposes not identified on the Privacy Notice provided to the client.

3. All personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Information irrelevant to the purpose of processing must not be collected. Medical information irrelevant to the referral purpose should not be included in the occupational health report unless there is a substantial and justifiable reason to do so.
4. All personal data shall be accurate, and where necessary, kept up to date. Clinicians must check personal data of clients at the start of every contact and amend records stored where required. Employees should advise Peritus Health Management where there are any changes to the personal data held and check personal data with data subjects when in consultation with them.
5. All personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Data will be stored in accordance with naming standards and folder trees. Hand written notes will be made in issued notebooks which will be kept secure, exchanged for new notebooks when full and disposed of by the DPO in the confidential waste bin. Archiving, retention and erasure processes must be adhered to.
6. All personal data shall be processed in a manner that ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organization measures. IT and mobile devices will be kept secure and password protected. Hard copy records will be stored securely in blue secure transportation envelopes bags or secured bags.
7. All data subjects have a right to see the data processed about them under the Access to Health Records Act 1990 and GDPR 2018 within 21 days of application and the process in the Information Governance Policy must be followed.
8. Medical information given by an employee must be kept private and not disclosed to a third party unless:
    - the employee consents to the disclosure in writing
    - a court of law requires disclosure
    - disclosure is justified in the public interest (this should be discussed with the employee's clinical supervisor and/or professional body prior to disclosure)
9. Breaches of data protection or potential breaches of data protection must be reported immediately to a Director or the DPO.

Access to employee information is on a 'need to know basis'. When a file is being accessed for an administrative task e.g. sending a letter, only the information relevant to the task should be read.

Personal details of identifiable individuals must not be casually discussed.

Personal data may be verbal, handwritten, computer or email records.

I have read and understand the Information Governance Policy and the summary above and understand how it applies to my role.

Signed: **Date:**

Name:

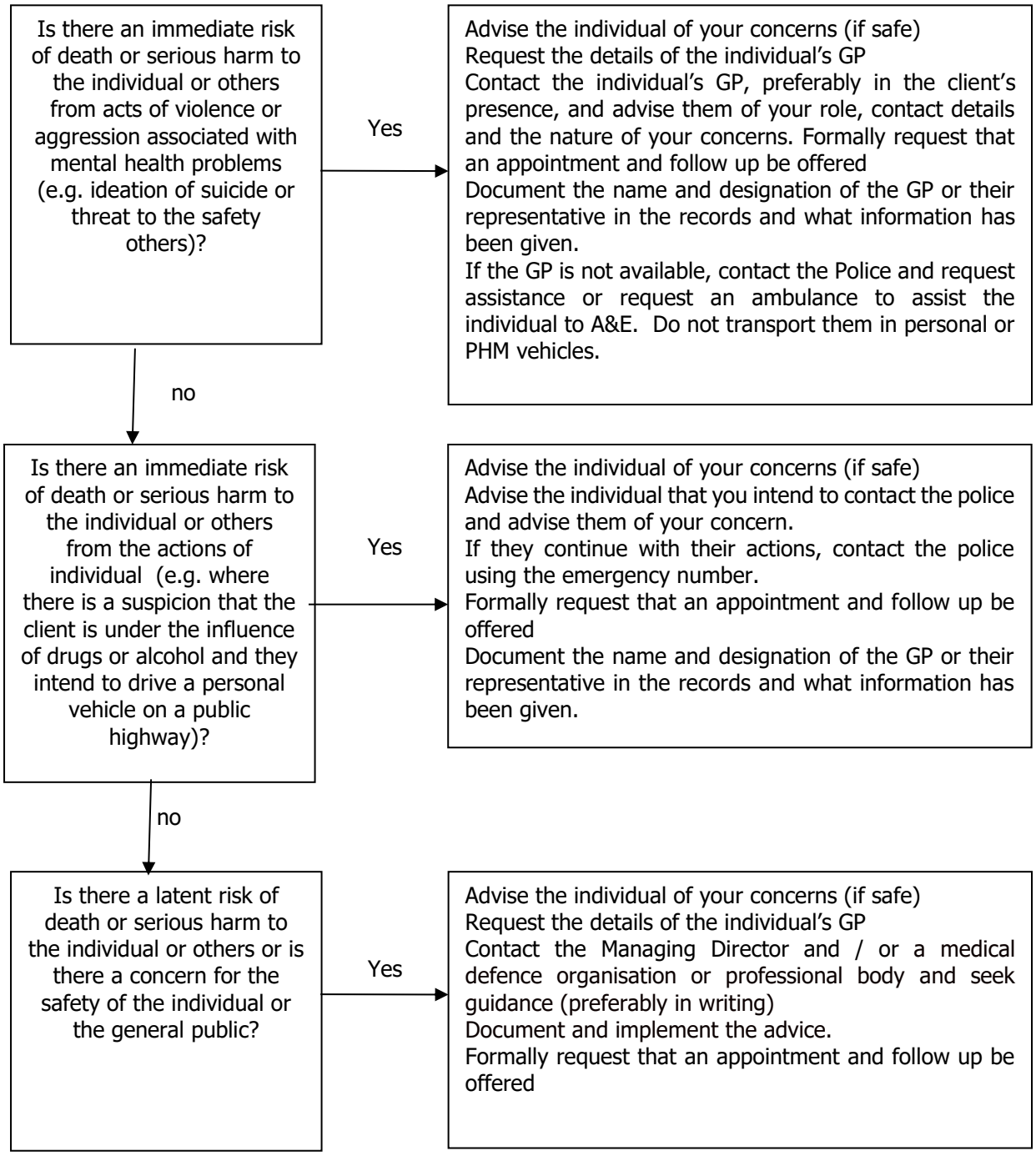
Job Title:

Policy discussed by

Signed: **Date:**

Appendix 5 – Procedure for Managing Critical Risk Incidents

In the event that a client discloses some information to an Occupational Health Advisor in a confidential setting that raises concerns with the Occupational Health Advisor that the individual or others are at risk of death or serious harm the Occupational Health Advisor should take appropriate action as detailed below.



Appendix 6 – Clinical Record Keeping Standards

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 to ensure chronological order
4. every entry in the clinical record should be dated, legible, and signed (electronically as appropriate) by the person making the entry. The designation of the person making the entry and printed name should be against a signature. Deletions and alterations should be countersigned and dated.
5. 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.
6. Copies of all correspondence relating to the client should be maintained in the clinical records in the section to which it relates.
7. Consent to release forms should be stored in the area section as the report to which it applies in accordance with the naming standards.
8. Handwritten notes must be written legibly in black ink.
9. Records must be authentic, reliable, useable and stored with integrity.
10. 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.

Derived from Section 5.2 - ISO15489-1:2016

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

Appendix 7 – Access to Medical Reports Act Consent

Consent Form for Accessing Medical Report from Health Care Professional

Surname:	Forename:
Previous Name:	Date of Birth:
Home Address:	Name and Address of GP / Health Care Professional:

Summary of Principle Rights under the Access to Medical Reports Act 1988 and General Data Protection Regulations 2018

- You have a right to refuse to consent to provide a report from your treating health care professional;
- You have a right to see the report prior to it being forwarded to Peritus Health Management;
- If you wish to see the report, you have 21 days from the date you are informed that the report has been requested, to make your arrangements to see the report. If you have not seen the report within this time, your health care professional may forward the report to Peritus Health Management without you seeing it;
- If you do not understand or agree with any of the points on the report, you have the right to request that your health care professional adjusts the report;
- If the health care professional refuses to change the report, you may write to Peritus Health Management informing us why you disagree with the report and give us the details as you see them;
- You have the right to withdraw your consent for the issue of the report at any time.
- You have a right to access the report once supplied to Peritus Health Management as part of your occupational health records.

Please note that your health care professional may withhold parts of the report if they feel that you may be adversely affected by its contents.

Declaration

- I consent to the provision of a medical report to Peritus Health Management.
- I understand my rights under the Access to Medical Reports Act 1988 and the General Data Protection Regulations 2018 and am aware of the reasons for the report request.
- I understand that this consent form may be photocopied and it will retain the validity of the original copy.
- I do / do not wish to see the report prior to its supply.

Signed:	Date:
Print Name:	

Appendix 8 – Transfer of Records Agreement

Peritus Health Management complies with the Faculty of Occupational Medicine's Ethics Guidance for Occupational Health Practice when transferring records following the change in occupational health provider. In order to maintain good practice and in the interests of the employer and workers, Peritus Health Management will ensure the following checks are in place:

- Evidence of a contract between a new occupational health provider and the employer.
- Evidence that workers have been notified of the transfer of occupational health services to a new provider and have been given the option to 'opt out' of the scheme.
- A list of all employees' whose records have been transferred and those who have 'opted out' has been drawn up and attached to the transfer documentation.
- Confirmation of photographic identification of the occupational health provider, and the GMC / NMC registration details of the specialist practitioner overseeing the contract.

Declaration

I confirm that I will ensure that the occupational health records transferred into my care will be maintained and stored in accordance with legal and professional guidelines and that consent will be sought from the author of the records where requests to release information to a third party is requested.

Name:	
Signature:	
Date:	
Company:	
Name of Responsible Person:	
GMC/NMC:	

Appendix 9 – Legitimate Interest Assessment

Legitimate Interest is one of the 6 lawful bases for processing personal data. It should only be used where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Before commencing a LIA, check to ensure a Data Protection Impact Assessment is not required as a higher level assessment:

☐ Always carry out a DPIA if we plan to:
- ☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- ☐ Process special category data or criminal offence data on a large scale.
- ☐ Systematically monitor a publicly accessible place on a large scale.
- ☐ Use new technologies.
- ☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- ☐ Carry out profiling on a large scale.
- ☐ Process biometric or genetic data.
- ☐ Combine, compare or match data from multiple sources.
- ☐ Process personal data without providing a privacy notice directly to the individual.
- ☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- ☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- ☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

☐ Consider carrying out a DPIA if we plan to carry out any other:
- ☐ Evaluation or scoring.
- ☐ Automated decision-making with significant effects.
- ☐ Systematic monitoring.
- ☐ Processing of sensitive data or data of a highly personal nature.
- ☐ Processing on a large scale.
- ☐ Processing of data concerning vulnerable data subjects.
- ☐ Innovative technological or organisational solutions.
- ☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing

Category of Data:	

Part 1 Purpose Test

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

Part 2 Necessity Test

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3 Balancing Test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

Nature of Personal Data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

Reasonable expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by:	
Date:	

Appendix 10 – Data Impact Assessment Template

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise

Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers

Identify and Assess Risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall Risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced or accepted	Low, medium or high	Yes / No

Sign off and record outcomes

Item	Name / Date	Notes
Measures approved by		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, risk control measures and whether processing can proceed
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 11 – Consent to Release Medical Report

Peritus Health Management is committed to complying with all relevant legislation and professional guidance relating to Data Protection, thereby protecting individuals, the organisation and its customers from unlawful, inappropriate or insecure processing of data. As part of that commitment you should have been supplied with a Privacy Notice by your employer or prospective employer which confirms the arrangements in place for the processing of your data. If you require any additional information relating to the processing of your data, please let your clinician know and we will respond to your request.

A report has been produced for your employer giving an outcome of the health assessment. The information is intended to be used by management to review your fitness for work; consider any adjustments or restrictions that need to be in place for your safety or wellbeing purposes, or to promote your optimum potential; and/or to determine whether there are any health and safety concerns relating to your exposures at work, the way you work and/or the control measures employed that need to be addressed.

Please read the following statements and indicate your confirmation of the statements in the appropriate box.

- ☐ I have been provided with a copy of the Privacy Notice relating to my health assessment.
- ☐ The nature, purpose and outcome of the health assessment has been explained to me by:

- ☐ I have read the contents of the occupational health report, confirm the accuracy of the medical details in the report and consent to its release to my employer.
- ☐ I have read the contents of the occupational health report, and do not wish it to be sent to my employer. I understand that my employer and I will be sent a limited report confirming my fitness to work status only, instead of the detailed report, and that any decisions that my employer may need to take, will be taken based on the information available to them.
- ☐ I wish a copy of the report to be provided to me personally / by email / posted to my home address.
- ☐ I consent to my email address being used to contact me to gain my feedback on the occupational health services provided to me by Peritus Health Management.

Name:			
Date of Birth:			
Company Name:			
Email Address:			
Home Address:			
Phone Number:			
Signed:		Date:	