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:	

Peritus Health Management Ltd
16a Church Lane, Brighouse, HD6 1RY
Tel: 01484 722444 Fax: 01484 599911
admin@peritushealth.com www.peritushealth.com
Company No: 5491540

(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.

Peritus Health Management will from time to time, advise you of any updates in the field of occupational hygiene and health and details of upcoming health promotion events and materials by a newsletter. This will not be excessive. Please confirm whether you wish for these updates to be provided by:

- ☐ Email
- ☐ Letter
- ☐ Telephone
- ☐ No thanks

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

Data Sharing Agreement

Contents

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 Regulation 2016 (GDPR)
- Data Protection Act 2018
- Access to Medical Reports Act 1988 (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)
- General Medical Council Guidance on Confidentiality (2017)
- 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 Regulation in relation to 'data sharing', it is acknowledged that the purpose of this 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 principles 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 principles listed below. Specialist arrangements for clinical records will also be implemented by Peritus Health Management and identified in the 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). Failures to comply with 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 in 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 factual information, be asked 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.

In an exceptional case where Peritus Health Management becomes aware that there is a legal duty to disclose information, for example of a communicable disease, or that the data subject constitutes a serious hazard to other workers and/or the general public information may be given to the employer or the relevant authority without consent in the public interest after first discussing the matter with the data subject.

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 will not use personal data for marketing purposes without consent.

To help improve the quality of our services, Peritus Health Management will seek consent from service users to gain feedback on the services provided by email. Feedback will not be sought without consent.

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 an individual health record for each employee placed under statutory health surveillance, for example in pursuance of the Control of Substances Hazardous to Health Regulations 2002. 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 the 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.

The clinical records of the detailed results of statutory health surveillance will be kept by Peritus Health Management in the confidential records, as advised by the Health and Safety Executive.

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 data which is often subject to change (e.g. 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 and reimbursing Peritus Health Management for any costs of the transfer.

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 who are subject to statutory health surveillance. These records are important as they allow links between exposure and any health effects. Copies should be kept in a reasonably accessible 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 when 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 copies of the reports for a period of 40 years from date of monitoring.
- Occupational Health clinical records will be retained for 6 years after the employee leaving his employment or date of last entry where there is no continued contract with the employer, reviewed, and if no longer needed, destroyed.
- Health surveillance records as a general rule will be retained for 10 years from the date of last entry, reviewed, and if no longer needed, destroyed. (Customer) is advised to store copies of the health records generated by statutory health surveillance for a period of 40 years from date of last entry (further advice is available on the HSE website).
- 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 copies of the health records generated by statutory health surveillance for a period of 30 years from date of last entry (Ionising Radiations Regulations 2017).
- 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 records generated by statutory health surveillance for a period of 40 years from date of last entry.

- Recorded conversations which may be later needed for clinical negligence purposes will be retained for 3 years following creation, reviewed, and if no longer needed, destroyed. Recorded conversations which form part of the clinical records will be stored with the confidential clinical records.
- Subject access requests and disclosure correspondence will be retained for 3 years following the resolution 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 agree to the transfer the records, or the employer's business has closed down, 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.

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 principles of legal and professional obligations and this Data Sharing Agreement.

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 in their domain.

Peritus Health Management is considered to be a Data Processor in relation to the data provided by (Customer) and the documentary data provided by the client (patient) or their healthcare provider, and a Data Controller of the information created by Peritus Health Management for the purposes highlighted below.

(Customer) is considered to be a Data Controller in relation to the information provided to Peritus Health Management, and a Data Processor of the information provided by Peritus Health Management for the purposes highlighted below.

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 within 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. Teachers 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 to be put 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 (only with the employee's consent to release); 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 in order to 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 of 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 a 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 (only with the employee's consent to release); 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) Health Record 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 within 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) Health Record 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 within 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, whether 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 (only with employee's consent to release); 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 comply with 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 employee's 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 (only with employee's consent to release); 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 year 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.

Ad hoc or 'one-off' sharing of data

Where situations arise that require 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, and 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 in our Clinical Record Keeping Standards which are 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), the General Medical Council's Guidance on Confidentiality (2017) and the Nursing and Midwifery Council Code (Nursing and Midwifery Council, 2015) apply. 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 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 obtain the client's consent to release the health-related data contained in the report to the Customer's management using a Consent to Release Medical Information form. Where it is thought necessary to request a report from a doctor who is or has been responsible for clinical care such as the General Practitioner, a response to an email detailing the individual's rights under the Access to Medical Reports Act will be sought. 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 be required to protect 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 and are bound by contract to do so.

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 that 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. Where it is impractical to obtain written consent, for example where the individual is interviewed by telephone, the occupational health professional will make a written contemporaneous note in the records to the effect that oral consent has been given. The reason for oral consent 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 because the individual lacks capacity to make a rational decision;
- if there is a real concern that the health or safety of others is endangered;

- if it is required by law;
- if it is otherwise 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 the procedure for responding to a subject access request detailed below.

Records may need to be accessed by our IT Consultant or data processors for the purpose of processing or maintaining the system on a strictly confidential basis.

Submitting a request for information

Peritus Health Management will ensure, wherever appropriate, that a data subject has access to all records stored about them. The data subject should apply in writing to Peritus Health Management to request access to the records or for 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 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 extent of the consent with the data subject. An Order of Discovery issued by a court or tribunal 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 is a genuine court order.

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

(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:

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 principles and codes of practice defined by ISO 27001 as they apply to Peritus Health Management;
- maintain network consistency by installing applications, patches and updates as 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;
- log all systems and store 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 compliance with data protection principles.

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

Peritus Health Management uses a UK based datacentre for storage and 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 and 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 a 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 is 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 when it is no longer needed. 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 given to them or their GP rather than transferred and details of any future storage of records if they are retained by the customer;
- photographic evidence of the identity of the professional receiving the records and evidence of current registration with 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 goes into liquidation, the records will be retained for the standard periods by 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 or 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 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 as soon as is practicable.

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 after 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.

General Medical Council. (2017, January). *Confidentiality: good practice in handling patient information.* Retrieved from General Medical Council: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality#

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 1

Data Protection and Privacy Notice – Occupational Health

Peritus Health Management is committed to provide safe and effective occupational health services to customers. During the course of our business, we process a significant amount of personal and special category data. We will ensure that all data will be processed in accordance with the requirements of the General Data Protection Regulation and other relevant legal and professional guidance. We want our staff and service users to be confident that the 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 and statutory regulations made thereunder.

Our employees are nurses and doctors and other health professionals with special qualifications and training in the effects of health on work and work on health (occupational health). Sometimes we will ask with your consent for further medical information or guidance from your own GP or specialist or an independent specialist.

During 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*.

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 and assess your entitlement to sick pay; 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 to management and the Occupational Health professional will discuss the implications of the report with you before asking for your written consent to release the medical information to your employer. We will not release medical information to your employer without your consent to do so but will report in the terms of fitness to work*

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 regulatory bodies such as DVLA. Information shared with your employer will be in the terms of fitness to work only. You will be advised of this.

Consent to release medical information

As health professionals, we will fulfil our professional duty of confidentiality as required by the common law and the ethical duties of our professions. Your legal rights 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 if you refuse consent to provide medical information.
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. However, the report gives the opinion of the Occupational Health Professional in relation to the management questions and cannot be edited to give your opinion or that of your relatives/advisors, though it may record your disagreement with the professional's opinion. 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 with your consent 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 need further investigation through the NHS, we may recommend that the information gained is shared with your consent 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*.

Security of Information

Your records will be kept confidential and stored electronically with appropriate access restrictions and security, but they may need to be accessed by our IT Consultant or data processors for the purpose of processing or maintaining the system on a strictly confidential basis.

Access to your information and rectification

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 statement of fact you think is inaccurate, but not an expression of opinion unless based on inaccurate facts.

To protect you from serious 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 a copy of your occupational health records free of charge 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 licence. 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 clinical information and will be stored by your employer and not Peritus Health Management. Health records relating to exposure to lead or asbestos must be stored for 50 years from the date of last entry in accordance with legal requirements. Health records relating to exposure to ionising radiations must be stored for 30 years from the date of the last entry. Clinical records of health surveillance procedures and those relating to fitness to work assessments not containing any health surveillance information will be stored for up to 10 years following date of leaving employment and then erased unless there is a reason for retaining them such as a legal claim, HSE guidance or a research project. You do not have the right to request that these records are deleted before the retention period identified above as we may need to rely on this information for the defence of a 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 us to contact you in the main body of the text and the nature of your enquiry.

Appendix 2 - Request for Accessing Occupational Health Data

Surname:	Forename:
Previous Name:	Date of Birth:
Company Name:	Job Title:
Home Address:	

I would like to apply for a copy of all my occupational health records held by Peritus Health Management and wish for the records to be sent to my home address identified as above.

Signed:	Date:
Print Name:	

Please provide formal evidence of your identification* along with this request and send to:

Peritus Health Management or admin@peritushealth.com
16a Church Lane
Brighouse
West Yorkshire
HD6 1AT

* Formal evidence of identification may include a copy of your bank statement, utility bill, or driving licence confirming your address or you may wish for confirmation of your identify to be provided by your HR Advisor by requesting them to complete the declaration below.

HR Advisor declaration

I declare that the name and address of the above person has been checked against our HR records and the identification of the employee has been confirmed.

Signed:	Date:
Print Name:	