

Standard Terms and Conditions for Occupational Health Services

Integral Occupational Health Ltd (IOH)

(Company number SC 232455; registered office: 76 West Regent Street, Glasgow, G2 2QZ)

Standard Terms and Conditions

1. Definitions

1.1. In these conditions:

“Client”	the person about whom the services have been requested for an examination, health intervention or report
“Commencement”	in the case of Health Surveillance services, the date that the provision of services start from
“Customer”	means the person or entity who has instructed IOH to perform services under the terms of these conditions.
“Data Sharing Agreement”	The IOH Data Sharing Agreement attached as Schedule 2
“GDPR”	The General Data Protection Regulations
“IOH”	Integral Occupational Health
“RIDDOR”	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
“Service Level”	The service levels as per Schedule 1
“Service Quote”	The list of services and fees provided and updated from time to time for the Customer, which forms part of this contract
“Management Fee”	means the fee payable every 12 months from commencement of services, if applied in your Service Quote

2. The Contract

2.1. Integral Occupational Health Ltd will be referred to hereafter as IOH.

- 2.2. These conditions apply between IOH and the Customer commissioning occupational health services from IOH, including ad-hoc utilization of services and/or where an Annual Management Fee has not been applied.
- 2.3. No variation of or addition to these conditions is effective without the written agreement of both IOH and the Customer.
- 2.4. These Standard Terms and Conditions, Schedules 1 and 2 and your Service Quote form the Contract.

3. The Work

- 3.1. IOH shall carry out the work using professional skill and care in the light of information available to IOH at the time.
- 3.2. The Work will be made up of the various services outlined in Clauses 9, 10, 11 and 12 below and as priced in your Service Quote and in accordance with the Service Level in Schedule 1.
- 3.3. IOH will use its best endeavors to carry out the work in accordance with any timetable agreed with the customer. IOH will inform the customer immediately if it becomes apparent that the work will not be carried out in accordance with the timetable and will seek to agree a new timetable with the customer.

4. Liability

- 4.1. The Customer hereby agrees and undertakes to indemnify and keep indemnified IOH during the Contract and thereafter for and against all damages, loss, claims, demands, expenses, costs and liabilities which IOH may at any time incur as a result of any negligent breaches by the Customer, its agents or employees.
- 4.2. While IOH will use all reasonable endeavors to ensure the Services are provided to a level of skill and care commensurate with that of a reasonably skilled professional in the field of the Services, IOH will not be held responsible for any consequence arising out of any inaccuracies or omissions unless such inaccuracies or omissions are the result of any negligent act or willful default on the part of IOH.
- 4.3. Except in respect of death or personal injury caused by IOH's negligence, or as expressly provided in these Conditions, IOH shall not be liable to the Customer by reason of any representation (unless fraudulent), or any implied warranty, condition or other term, or any duty at common law, or under the express terms of the Contract, for any loss of profit or any indirect, special or consequential loss, damages, costs, expenses or other claims (whether caused by the negligence of IOH, its employees or agents or otherwise) which arise out of or in connection with the provision of the Services.
- 4.4. In any event the entire liability of IOH under these terms and conditions will be limited to five million pounds £5,000,000(GBP).

- 4.5. IOH clinical staff are covered by medical malpractice insurance.
- 4.6. IOH shall not be liable to the Customer or be deemed to be in breach of the Contract by reason of any delay in performing, or any failure to perform, any of IOH's obligations in relation to the Services, if the failure or delay was due to any cause beyond IOH's reasonable control.
- 4.7. IOH shall have no liability to the Customer for any loss, damage, costs, expenses or other claims for compensation arising from any fault of the Customer including, without limitation:-
- 4.7.1. any documents or other materials, and any data or other information provided by the Customer or a Client relating to the Services; or
- 4.7.2. any instructions or information supplied by the Customer (or its accountants, solicitors or other professional advisers) relating to the Services; which are incomplete, inaccurate, illegible, or arising from their late arrival or non-arrival.
- 4.8. While IOH shall use all reasonable endeavors to ensure the accuracy of any third party material used by IOH in carrying out the Services, IOH shall have no liability to the Customer for any loss, damage, costs, expenses or other claims for compensation arising from use of such third party material.
- 4.9. While IOH shall use reasonable endeavors to ensure the suitability of information sources, including client medical reports from treating clinicians, to be used by IOH in carrying out the Services, IOH shall have no liability to the Customer for any loss, damage, costs, expenses or other claims for compensation arising from use of such information sources.

5. Confidentiality

- 5.1. Both IOH and the Customer agree to keep (and to ensure that their respective employees keep) confidential all information disclosed by either party to the other relating to the Contract. This obligation of confidentiality shall apply to information disclosed orally or in writing, and whether or not such information is expressly stated to be confidential or marked as such. Confidentiality extends to information gained by IOH about the Customer's business operations, customers, trading partners and know how.
- 5.2. The obligation of confidentiality in clause 4.1 will not apply where:-
- 5.2.1 either party has consented in advance and in writing to disclosure of the confidential information;
- 5.2.2 that such information becomes public knowledge through no fault of the receiving party provided that the receiving party shall not disclose any such information which is not public knowledge;
- 5.2.3 the receiving party can show, to the reasonable satisfaction of the other, that such information was already known to the receiving party prior to its being disclosed to them; and

- 5.2.4 the receiving party is required by law to divulge such information to some judicial, governmental or other authority or regulatory body (in which case the receiving party shall do so only to the extent required by law and shall use its best endeavors to ensure that the body in question keeps such information confidential and does not use the same except for the purposes for which the disclosure is made).

6. Intellectual Property

- 6.1 IOH acknowledge that in the performance of the services, IOH will become aware of information including knowledge, commercially sensitive information, plans, trade secrets and processes that are the copyright and intellectual property of the Customer and will use all reasonable endeavors to protect those rights of the Customer.
- 6.2 The Customer acknowledges and agrees that all copyright and other intellectual property rights arising from the Services shall remain the exclusive property of IOH and may only be copied, reproduced or disseminated with IOH's express prior written consent. This agreement will be reciprocal with the customer.
- 6.3 The Customer acknowledges and agrees that they will cease to use all materials which are the copyright or intellectual property right of IOH upon the termination of services however caused.

7. Data Protection

- 7.1 It is recognized that in order for IOH to provide Occupational Health Services, Personal Data and Sensitive Personal Data relating to clients will need to be shared between the Customer organization and IOH.
- 7.2 IOH are a Data Controller of information gathered by them and within their domain and are not a Data Processor for the Customer.
- 7.3 Utilisation of IOH services requires Customers to agree to the terms of our Data Sharing Agreement which is attached as Schedule 2.
- 7.4 The Customer shall ensure that it has all consents or permissions necessary under the Data Protection Act 1998 (DPA) and any other prevailing legislation, including the General Data Protection Regulations (GDPR) in pursuance of their responsibilities as Data Controller for that information prior to disclosing to IOH any personal data (including sensitive personal data) relating to Clients and shall comply with IOH's reasonable directions in relation to ensuring compliance in all respects with the GDPR as outlined in the IOH Data Sharing Agreement. Reasonable direction would relate to compliance with the DPA and GDPR in accordance with Guidance Documents, Codes of Practice and Best Practice as may from time to time be released by the Information Commissioner's Office or other such body.
- 7.5 Consent is required by clients for the performance and delivery of Occupational Health interventions. In the event that a client does not engage or consent to the

consultation process, including consent for the release of an Occupational Health report, the fee for OH services will still apply, as outlined in your Service Quote.

8 Medical Records

- 8.1 IOH maintain medical records, as professionally required in the pursuance of the provision of Occupational Health services.
- 8.2 IOH have a process for the transfer of medical records to and from another Occupational Health provider at the commencement or cessation of services, in accordance with industry guidance. Such transfers will require both Occupational Health providers to co-operate and comply with professional standards.
- 8.3 Where records are being transferred from IOH to another provider, the cost of delivery by secure means such as courier service will be met by the Customer.
- 8.4 Access to medical records, such as Subject Access Requests are managed by IOH.

8. GP and Specialist Medical Reports

- 8.1. On occasions a medical report is required from a GP or Specialist in order to give complete and accurate advice to the customer.
- 8.2. The Customer agrees to pay IOH any costs relating to third party services, including GP and Specialist reports and tertiary specialist fees where such services are required, in the view of IOH, in order to provide good medical advice.

SERVICES

9. Occupational Physician Appointments

- 9.1. Appointments will be offered after the receipt of a correctly completed referral form. We will use our best endeavors to appoint as soon as is practicable and in accordance with the following service level:
 - 9.1.1. 95% of appointments will be offered within 10 working days of referral
 - 9.1.2. 95% of reports will be dispatched within 2 working days following the consultation, assuming consent is provided by the employee for release of the report at the time of the consultation.
- 9.2. Service levels relate to the offer of an appointment with any of our Occupational Physicians and the Customer acknowledges that if continuity of OH Physician is required, events such as illness or annual leave of a particular OH Physician may impact on the waiting time.
- 9.3. Referral documents and supplementary information supplied by the Customer needs to be shared in accordance with our Data Sharing Agreement.
- 9.4. It is the Customer's responsibility to ensure that the appointment details are notified to the client.

9.5. Charges applicable for a change or cancellation of an appointment are as follows where times exclude Saturday, Sunday and Public Holidays:

9.5.1. If the notification is more than 48 hours no fee will be due to IOH for the changed or cancelled appointment.

9.5.2. If this notification for a change or cancellation is less than 48 hours then the full fee will still be due.

9.5.3. If a client fails to attend their appointment without cancellation this will be subject to a non-attendance fee equivalent to the full fee.

10. Pre-placement and Night Worker assessment

10.1. Pre-placement and Night worker questionnaires can be scrutinized by IOH upon request.

10.2. IOH will only scrutinize information provided by subjects on IOH documentation where appropriate consents have been given to that processing.

10.3. A fee will be charged for each questionnaire received.

10.4. No subject will be deemed to be medically unfit without an Occupational Health Physician consultation.

10.5. If an Occupational Physician consultation is deemed necessary following IOH scrutiny of the questionnaire, the Customer will be notified of this. It is for the Customer to decide if they wish to proceed with an OH consultation in which case, the usual referral process and fees will be required as for other Occupational Physician consultations.

10.6. Our service level for the processing of completed questionnaires is:

10.6.1. 2 working days where we are able to complete scrutiny based on the information available.

11. Single OH Nurse appointments

11.1. Single appointments for OH Nurse services can be offered at our IOH site.

11.2. The fee for single appointments is as outlined in the Service Quotation, where applicable.

11.3. Appointments will be offered after the receipt of a correctly completed referral form, where applicable.

- 11.4. We will use our best endeavors to appoint as soon as is practicable and in accordance with the following service level:
- 11.4.1. 95% of appointments will be offered within 10 working days of referral
- 11.5. Referral documents and supplementary information needs to be shared in accordance with our Data Sharing Agreement.
- 11.6. It is the Customer's responsibility to ensure that the appointment details are notified to the client.
- 11.7. Charges applicable for a change or cancellation of an appointment are as follows where times exclude Saturday, Sunday and Public Holidays:
- 11.7.1. If the notification is more than 48 hours no fee will be due to IOH for the changed or cancelled appointment.
 - 11.7.2. If this notification for a change or cancellation is less than 48 hours then the full fee will still be due.
 - 11.7.3. If a client fails to attend their appointment without cancellation this will be subject to a non-attendance fee equivalent to the full fee.

12. Ad-hoc on-site nurse clinics

- 12.1. Services delivered by nurses may be provided at a Customer site upon request. Requests for service can be made by telephoning or emailing our Head Office and speaking to our Administration Manager.
- 12.2. If your Service Quotation does not include nurse services, an additional Service Quotation will be provided.
- 12.3. The Service Level for dates to be offered for on-site nurse days is:
- 12.3.1. 15 working days for single days
 - 12.3.2. For block bookings the service level is to agree a timescale for delivery within 10 working days of request with delivery dependent on Customer timescales, volume and IOH nurse availability.
 - 12.3.3. Non cancellation of nurse clinics unless in cases of staff illness or events out with the reasonable control of IOH.
- 12.4. Your Service Quote shows the rates applicable to on-site work.
- 12.5. Where on-site services are requested, it is the Customer's responsibility to ensure employees are notified of the appointment details.
- 12.6. When on-site services are requested, the customer is responsible for the provision of suitable premises in which to conduct the services. The main

requirements are as follows:

- 12.6.1. A private room which cannot be seen into from the outside (screening measures can be used) and where consultations cannot be overheard. Cleanliness and adequate heating and lighting is required and the room should be available for use throughout the scheduled time period, without interruption.
- 12.6.2. A table and 2 chairs (3 if clients are to be accompanied).
- 12.6.3. For noise health surveillance, background noise must be at a low enough level sufficient for the effective provision of audiometry screening tests.
- 12.7. No fees are to be levied against IOH for the use of premises for this purpose.
- 12.8. When on site, IOH staff will abide by all Health and Safety instructions given by the site controller who will usually be the Customer.
- 12.9. The cancellation fees applicable to on-site work are as follows with calculations excluding Saturday, Sunday or Public Holidays:
 - 12.9.1. More than 10 days notice attracts no fee.
 - 12.9.2. Less than 10 days and more than 5 days notice attracts a half fee.
 - 12.9.3. 5 or less days attracts a full fee.

13. Management Fees

- 13.1. Your Service Quote outlines if an Annual Management Fee is applicable for the provision of your services. Annual Management Fees only apply to Health Surveillance programs.
- 13.2. The Management Fee is invoiced at the commencement of Health Surveillance services and annually thereafter.
- 13.3. The services included in your Annual Management Fee are outlined in your Service Quote, if applicable.
- 13.4. There is no refund of the Annual Management Fee in the event of termination of the contract by the Customer before 12 months since the last Annual Management fee was invoiced.

14. Term and Termination

- 14.1. Where no Annual Management Fee has been charged, the term of this agreement is for the period from referral to conclusion of delivery of each individual service referral.
- 14.2. Where an Annual Management Fee has been applied, the term of this contract is for 12 months from the 'Date of Commencement' and is renewable annually

thereafter unless the Customer provides 2 months' notice of termination. In this case:

14.2.1. Either party may terminate this agreement by giving two months notice to the other party.

14.2.2. In the event that termination notice is given by IOH, the balance of the Management Fee will be refunded to the Customer.

15. Business Continuity

15.1. In the event that IOH is unable to deliver services within the Service Levels:

15.1.1. IOH will use all reasonable endeavors to re-establish full services as soon as possible and will provide reduced service meanwhile.

15.1.2. IOH will provide regular updates on our re-establishment plan.

15.1.3. IOH will provide ongoing OH advice to manage acute issues and prioritize cases based on risk, in discussion with the Customer.

15.2. In the event of transfer of the OH services to another OH provider, IOH will, upon notice, provide an exit plan and use reasonable endeavors to manage the transition of the service to the new provider. The exit plan will include:

15.2.1.1. A list of OH records held

15.2.1.2. Transfer of OH records in accordance with industry professional guidance

15.2.1.3. Health surveillance risk registers transferred

16. Occupational Ill Health

16.1. Clinicians at IOH may identify cases of work-related ill health following single OH consultations or as part of a Health Surveillance program.

16.2. All cases of suspected Occupational ill-health will be notified to the employer through a consented OH report following consultations as well as recommendations for further action.

16.3. Where a reportable condition under RIDDOR has been identified by an Occupational Physician, this will be notified to the Customer, with consent, in the form of an OH report.

16.3.1. It is the Customer's responsibility to make a statutory report under RIDDOR in these circumstances.

17. Fees

17.1. All fees quoted in the Service Quote are exclusive of VAT. VAT will be charged in accordance with the tax rules which are issued by HMRC.

17.2. The fees due will be as per your Service Quote.

17.3. If in connection with the work any member of IOH is later called upon to give evidence or expert opinion in court, including an Employment Tribunal, on behalf of the customer, the Customer shall reimburse IOH with its full costs and expenses. For the avoidance of doubt the fee will be £175 per hour or part thereof.

18. Payment

18.1. The customer will pay the invoice in full, including any amount shown in respect of VAT within 30 days of the date of invoice.

18.2. No payment will be deemed to have been received until IOH has cleared funds.

18.3. If payment is not made by the due date, IOH shall be entitled without limiting any other rights that it may have to charge interest on the outstanding amount (both before and after judgment) at the rate of 2% above base rate from time to time of the Bank of Scotland accruing daily from the due date until the outstanding amount is paid in full.

19. General

19.1. Except where this Contract expressly provides otherwise, any subsequent modifications, additions, or deletions to the Services, (or their content) will only have effect if agreed in writing between the parties.

19.2. Any notice required or permitted to be given by either party to the other under this Contract shall be in writing addressed to the other party at its registered office or principal place of business or such other address as may at the relevant time have been notified pursuant to this provision to the party giving the notice.

19.3. No failure or delay by either party in exercising any of its rights under the Contract shall be deemed to be a waiver of that right, and no waiver by either party of any breach of the Contract by the other shall be considered as a waiver of any subsequent breach of the same or any other provision.

19.4. This Contract constitutes the entire agreement between the parties and supersedes any previous agreement or understanding between the parties. In the event of conflict between these Conditions, these Conditions shall prevail. All other terms and conditions, express or implied by statute or otherwise, are excluded to the fullest extent permitted by law.

19.5. If any provision of this Contract is held by any court or other competent authority to be invalid or unenforceable in whole or in part, the validity of the other provisions of the Conditions and the remainder of the provision in question shall not be affected.

19.6. The law of Scotland shall apply to the Contract and the parties agree to submit to the non-exclusive jurisdiction of the Scottish Courts.

Schedule 1

Service Levels

These are the Service Levels for the following services. Not all of these services may be included in your Service Quote.

If you wish to discuss our Service Levels, please contact IOH.

Service Level	Description	Target KPI
OH Physician Appointment	We will offer an appointment with any IOH Occupational Physician at an IOH site or telephone consultation within 10 working days from receipt of referral	95% of appointments
Dispatch of OH Reports	Following OH consultations, reports will be dispatched by encrypted email to the referrer within 2 working days after the consultation, if consent is provided by the client at the time of the consultation	95% of consultation
Pre-employment questionnaire processing	We will issue an outcome report within 2 working days of receipt of questionnaires provided they are complete and we can make contact with any client for any medical clarification, by telephone.	95% of questionnaires
Night worker questionnaire processing	We will issue an outcome report within 2 working days of receipt of questionnaires provided they are complete and we can make contact with any client for any medical clarification, by telephone.	95% of questionnaires
OH Nurse single consultations	We will offer an appointment with an OH nurse at an IOH site for nurse services within 10 working days of receipt of a referral	95% of referrals
Ad-hoc on-site nurse clinics	Single nurse days offered, at an agreed Customer site, within 15 working days.	90% of requests
Block Booking of nurse clinics on-site	We will agree a timescale for delivery within 10 working days with delivery dependent on location, customer preference and OH nurse availability.	95% of requests

Schedule 2

Data Sharing Agreement

Between Integral Occupational Health Ltd and the Customer



1. Definitions

- a. "Customer" means "any person, organisation, group or entity accepted as a customer of IOH to access OH services"
- b. "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"
- c. "Data processor" means "in relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller"
- d. "Data Sharing Agreement" means this agreement governing the arrangements by which personal data will be shared between IOH and the Customer as outlined in Schedule 1.
- e. "Data Sharing" means "the passing of personal data between the Customer and IOH".
- f. "GDPR" means "General Data Protection Regulations"
- g. "ICO" means "Information Commissioner's Office"
- h. "IOH" means "Integral Occupational Health Ltd registered in Scotland with registration number SC348272 with the Registered Office of 4th Floor, Finlay House, 10-14 West Nile Street, Glasgow G1 2PP".
- i. "Originating Party" means "A Data Controller who shares information for which they are a Data Controller with another Data Controller under this Data Sharing Agreement".
- j. "Receiving Party" means "A Data Controller who receives information from an Originating Party under this Data Sharing Agreement".

2. Applicability

- a. This Data Sharing Agreement applies to all Customers who commission OH services from Integral Occupational Health and agreement is a pre-requisite for accessing Integral Occupational Health services.

3. Commencement

- a. This Agreement is deemed to be in force from:
 - i. 25th May 2018 or;
 - ii. any earlier date that the Customer is notified of this agreement or;

- iii. any earlier date online terms and conditions are updated with this agreement

4. Purpose of Data Sharing

- a. IOH is a provider of professional Occupational Health services to the Customer for the ultimate benefit of workers and organisations.
- b. In order for IOH to provide these services, Data Sharing in certain circumstances is required:
 - i. From the Customer to IOH
 - ii. From IOH to the Customer
- c. The nature of the data to be shared includes Sensitive Personal Data and this is detailed in Schedule 1.

5. Organisations involved in Data Sharing

- a. This agreement relates only to Data Sharing between IOH and the Customer and as outlined in Schedule 1.
- b. This agreement does not cover the sharing of data with any other party and the respective Data Controller responsibilities for each party will be responsible for any such further data control.

6. Data Controller Responsibilities

- a. IOH is the Data Controller for information it receives from referring Customers and other sources.
- b. IOH is not the Data Processor of the Customer.
- c. The Customer is not the Data Processor for IOH.

7. Data Sharing responsibilities

- a. Schedule 1 outlines the data to be shared.
- b. The Originating Party is responsible for ensuring they have the appropriate arrangements, notices and consents in place for the release of information to be shared with the Receiving Party. Control measures are listed next to each data flow type in Schedule 1.
- c. Once information has been received by the Receiving Party, they have Data Controller responsibilities for that body of information that has been received.

- d. The Receiving Party should ensure they have the appropriate arrangements, notices and consents in place for that information to be shared within their organisation.

8. Access and Individual's Rights

- a. Each Data Controller should make it clear in Privacy Notices how individuals can access information.
- b. If a subject access request is received by one party and it is believed to relate to information held by another party, the subject should be directed to the other party. This is to ensure there are no unnecessary delays in individual requests being actioned.
- c. Complaints or enquiries relating to data should be directed to the relevant Data Protection Officer for the responsible Data Controller.

9. Information governance

- a. The datasets to be shared between parties is outlined in Schedule 1.
- b. Each Originating Party should take reasonable precautions to ensure the data sent is accurate.
 - i. If an inaccuracy is detected:
 - 1. the Originating Party should be notified (if not discovered by the Originating Party).
 - 2. All parties should rectify the error without undue delay.
- c. The data will be transferred utilising commonly available proprietary means.

10. Data Retention

- a. Sensitive Personal Information outlined in Schedule 1 will be retained by IOH in the following circumstances for the following time periods:
 - i. Where Statutory Health Surveillance has been carried out – 40 years
 - ii. Where no Statutory Health Surveillance has been carried out – 10 years from last OH contact
- b. Retention periods will be notified to data subjects in IOH Privacy Notices.
- c. In circumstances where there is a change of OH provider, IOH will arrange for transfer of records to the new provider directly with them provided the following criteria are met:
 - i. Consent of individuals

ii. Assurance of appropriate security and data governance arrangements

However the transfer of such records is not the responsibility of the Customer and is not within the scope of this data sharing agreement.

11. Data Security

- a. Each Data Controller has responsibility for ensuring the security of data within their Domain.
- b. Each Data Controller shall implement and maintain processes, procedures and controls to protect the confidentiality and security of data in accordance with good industry practice.
- c. Each Data Controller should have appropriate technical and organisational measures in place when sharing personal data including:
 - i. Consent from data subjects
 - ii. Encryption of electronic transmission of sensitive personal data such as using IOH referral portal or password encryption of email attachments.
 - iii. Information sharing within organisations should comply with Data Controller responsibilities.
 - iv. Physical security of data
 - v. Access controls to the data limiting access to only those with a requirement of access
 - vi. A summary of IOH Data Security arrangements is outlined in [Schedule 2](#).

12. Data Breaches

- a. The GDPR outlined responsibilities, including for reporting to the ICO, for Data Breaches.
- b. The Data Controller for the domain where the Breach occurred is responsible for reporting to the ICO and subsequent management.
- c. In the event of a Data Breach, the responsible Data Controller should implement further control measures to reduce the risk or prevent a further breach.

13. Review of Data Sharing arrangements

- a. IOH will audit these arrangements as part of ISO9001:2015 compliance.
- b. Non-conformances will be rectified and notified to relevant parties, which may be the Originating Party.

- c. Material changes in the GDPR or associated guidance may require future amendments.

14. Termination of services

- a. The data shared under this agreement, as outlined in Schedule 1, is on a referral by referral basis.
- b. The effect of the Customer not using IOH services means no more data transfers will occur.
- c. Both parties will still continue to hold Data Controller responsibilities for their information domain including responding to contacts from data subjects.

Schedule 1 – Data to be shared and customer controls

Data From	Data To	Data Type	Description	Customer Controls
Customer	IOH	IOH Referral Form Information	Data fields required for completion of a referral form including Name, DOB, Employee phone number, Employee address, Job Title, reason for referral, background information and specific questions.	Make sure Privacy notices and/or consent is provided by data subjects. Use the IOH online portal for making referrals and providing supplementary information or encrypt all sensitive information if sending my email. Make sure information is accurate e.g. names, addresses etc.
Customer	IOH	Supplementary Information	In addition to the referral form information, additional documents to support the referral such as absence records, job descriptions, medical reports received by the employer, meeting minutes, risk assessments carried out, including Individual Stress Risk Assessment.	Make sure Privacy notices and/or consent is provided by data subjects. Use the IOH online portal for making referrals and providing supplementary information or encrypt all sensitive information if sending my email.
Customer	IOH	Employee Lists for Health Surveillance Services	Names, dates of birth and occupations/exposures of employees in order to create and manage health surveillance call and recall arrangements. Health Surveillance is a statutory requirement.	Make employees aware as part of normal communication regarding health surveillance e.g. in Privacy Notices that their information will be shared this way. Ensure such transmissions are encrypted e.g. password encrypted Excel spreadsheet.
Customer	IOH	Employee lists of those to receive OH services such as vaccination or wellbeing medicals	Names, dates of birth and work location to allow arrangements and documentation to be in place for employees accessing these services.	Make employees aware, as part of the communication regarding availability of the service or in Privacy Notices, that this information will be shared with IOH in order to provide the service.

Schedule 1 (Continued) - Data to be shared and customer controls

Data From	Data To	Data Type	Description	Customer Controls
Customer	IOH	Supplementary Information after a referral has been made	Outwith a referral, there may be a need to provide IOH with risk assessment information, including stress risk assessment (ISRA) information, further meeting minutes etc.	Make individual aware specifically that this information is being shared with OH and only transmit it using secure means e.g. encryption, uploaded via IOH portal
IOH	Customer	Output report	The OH report produced by the IOH clinician is sent to the referring person (as per the referral form) only with explicit consent of the data subject.	Ensure the 'referring person' section on the referral form is correct as this is where the report will be dispatched to. Make sure internal notices and consents allow the sharing of information in OH reports with, for example, managers. Ensure security of this sensitive personal information within your domain.
IOH	Customer	Supplementary reports and advice	Further medical guidance in supplementary reports	Make sure internal notices and consents allow the sharing of information in OH reports with, for example, managers. Ensure security of this sensitive personal information within your domain.
IOH	Customer	Health Surveillance Recall Lists and outcome reports	Lists of workers with name, DOB, date or surveillance done and due, status of each assessment e.g. under review, confirmed problem. Employees consent to IOH notifying employers of this data at the beginning of the process.	Make sure internal notices and consents allow the sharing of information in recall lists with, for example, Health & Safety or HR. Ensure security of this sensitive personal information within your domain.
IOH	Customer	Invoice for services	Invoices for services state the employee name and a very broad grouping of service received e.g. OH consultation, PEQ, NWQ, Supplementary report.	Appropriate confidentiality agreements with staff processing invoices.



INTEGRAL®
OCCUPATIONAL HEALTH

Schedule 2 – IOH Data Security Arrangements

Item	Description
Acceptable Use Policy	All staff are aware of our Acceptable use policy.
Anti-Virus and Anti-malware software	Deployed centrally and updated automatically as soon as they are available. Monitored centrally.
Backup	Data is backed up continuously to our Cloud provider based in the EU. Retrieval and deployment of key assets is tested.
Boundary Firewall	We use a Web Content Filter for our network perimeter
Data Security Training	All staff have Data Security Training updated at least annually
Encryption at rest	All data devices, including smartphone data, is encrypted to recognised standards e.g. Bitlocker. Cloud backup data is encrypted at rest.
Encryption in transit	Personal sensitive information is sent electronically in encrypted format. All communication to and from the cloud backup is encrypted.
Hard copy documents	Documents are stored in locked cabinets out of daytime use.
Non-employees	Admin areas are separate from visitor areas and visitors are always escorted by a staff member when outwith the waiting room.
IT Hardware disposal	Although encrypted at rest, all IT asset data storage is destroyed by an HM Government level certified process.
Leavers	Immediate removal of IT Account
Network Access	There is no Guest network access permitted
Passwords	Alphanumeric, limited attempts and enforced password changes.
Patch Management	Operating System and Application patches are configured to be automatically installed
Penetration Testing	IT Security is tested by an external IT Security consultancy conducting a 'Grey Box' Penetration Test
Premises	Access control by employed staff with no out of hours access other than Director level. Premises secured with 2 monitored alarm systems, main building and building floor as well as digital keypad access.
Removable Media	Removable media is not permitted unless on a registered, encrypted device.
Review of IT Systems	Automatic reporting from Endpoint Protection including delayed AV-AM updates and attack logs.
Secure configuration of computers	Only essential software which is supported. Installing unauthorised software is prohibited.
Server	Physical server is located in a locked communications cupboard with access limited to 3 senior people.
Shredding of Confidential documents	Secure Confidential Waste bins are used until disposal by a contractor in accordance with BSEN15713



Staff Access to Sensitive Personal Data	Only staff that require access to personal data in the performance of their duties have these privileges. This means clinical doctors and nurses and supporting administrative staff, all of whom are covered by our data security policies.
Unmanaged networks	Connection to unsecure networks is not permitted.

Schedule 3 – References

- *Data Controllers and Data Processors* – Information Commissioner’s Office (06.05.2014)
Version 1.0 20140506
- *Data Sharing Code of Practice* Information Commissioner’s Office (5/2011)
- *Encryption*– Information Commissioner’s Office (4.4.17)
Version 1.1.0
- *Guide to the General Data Protection Regulation (GDPR)* Information Commissioner’s Office (21/11/17)
Version 1.0.38
- *Privacy Notices, Transparency and Control: A code of practice on communicating privacy information to individuals* Information Commissioner’s Office (7.10.16)
Version 1.0.38