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.

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 Processers* – 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