Occupational Health guidance for GDPR

How to contact the team

In the first instance, please contact your local OH Advisor either by telephone or by email.

Alternatively for Nuffield Health staff you can email ask.oh@nuffieldhealth.com or telephone 0300 123 1978.

For any other employee you can e-mail ohenquires@nuffieldhealth.com or call them on 0300 123 1978

Nuffield Health provides Occupational Health services to a variety of clients. We are a confidential service holding SEQOHS accreditation. All information is treated in the strictest of confidence and the information held within our secure Occupational Health database.

What is GDPR?

The General Data Protection Regulations (GDPR) replaces the Data Protection Act 1998 and comes into force on the 25th May 2018. It aims to give people greater control of their personal data and strengthens the rules relating to how organisations collect, process, retain and use this information. In addition, a new 2018 Data Protection Act will also come into force to support the GDPR (which remains an EU Regulation).

Fair and Lawful Processing

Each organisation is required to demonstrate that they are processing personal data fairly and lawfully, to do this we must have a 'lawful basis for processing' personal data. Consent is probably the condition that has gained the most attention but we only rely on consent in limited circumstances e.g. to share an employee's report back with their manager, or to consult their GP.

Occupational Health will mainly be processing data based on the following lawful basis for processing:

Article 6 (1)(b) Processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.

Article 6 (1)(f) Legitimate interests: the processing is necessary because of a legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

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, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

What information do we collect?

- Personal data (such as name, date of birth). We will use this data to enable us to identify different individual's records from each other.
- Contact details (such as address, telephone number, email). This is important so that we can contact individuals to arrange appointments, send reports etc.
- Job Role. This is important to know so that when we undertake assessments for work, we understand what the job role is so that appropriate adjustments are recommended
- Attendance / sickness record if applicable to the referral.
- Previous health problems and adjustments that line managers / HR are already aware of to assist the occupational health process.

How will we use personal data and who it might be shared with?

We will not share personal data with anyone who is not involved in your care, including third parties without explicit consent, unless there is a requirement under the law that allows us to.

- **Management Referral**

  All clients have been moved onto the online portal, which provides a secure method for making referrals. When making a referral, managers are asked to confirm that the employee has been made aware of the details of the referral before submitting. The referral will not be able to go ahead if this is not confirmed within the referral. The consent can be verbal, and must be confirmed on the referral form to Occupational Health where prompted. The referral form has been revised to include a statement to prompt for the manager. Any referral received that does not confirm that consent from has been obtained will not be processed and will be returned to the referring manager.

  Employees have the right to see the report before it is sent to their line manager / HR and can request inaccurate factual changes to be corrected. In order to comply with GDPR, consent cannot be assumed. At the time of giving the report to review employees are given a time frame, usually 48 hours if sent by email or 5 days if by post in which to respond. If the employee has not contacted OH in this time frame, a reminder will be sent by email or by telephone where the report has been posted, and a further 24 hours given to respond. If there is still no response then, the line manager / HR will be advised that we do not have consent to release the report and the case has been closed.. If we do subsequently receive consent, perhaps after line manager / HR intervention, the report will be sent in the usual way.

  All reports sent will be in PDF format, password protected and sent by encrypted email.

- **Preplacement Health Questionnaires**

  New joiners are often required to complete a pre-placement health screening in order to determine if an individual is fit for the tasks that they will be performing and to identify any adjustments that may be needed to support an individual to work.

  The preplacement questionnaire includes a detailed statement, which explains how this data is used, stored and retained, and confirms that the data is used solely for the purpose of assessing fitness for work. Medical information is not shared and that a fit form stating fitness to work and any adjustments needed to work is generated for HR / line managers. Consent for this processing is required at the time of completing the pre placement health questionnaire.

- **Vaccinations / Immunity / Travel Health**

  For some roles, vaccinations and blood tests are required because of hazards within the job role or as a requirement to travel for business. Consent for vaccination and blood tests is gained at the time of appointment and it will be documented if vaccination has been given or declined.

  Line managers / HR will not usually need to know the details about any vaccinations or immunity blood tests results. Should there be a valid reason for the manager to be informed; explicit consent from the individual will be obtained.

  If test results suggests that an individual is not able to undertake their role, the line manager / HR will be advised of this, but the results will not be disclosed. This is normally only applicable to health care workers who undertake exposure prone procedures.

- **Health Surveillance**

  For some roles, health surveillance will need to be undertaken where risk assessment indicates that an individual might be exposed to certain hazards within the work place i.e. noise.

Consent to undertake health surveillance is gained at the time of attendance. The employer will be sent a fitness to work certificate following the health surveillance appointment. Individuals cannot refuse consent to provide this information to their employer as this is a legal requirement. Individuals can decline health surveillance, however, they will be advised that they may not be declared fit for work and their employment might be at risk.

- **Billing Information**

  Where exceptionally confirmation of appointments is required for billing purposes, personal data (restricted to the name and appointment type) will be sent to the contract manager only as a password protected document via encrypted email. It will not be included in any invoices and will only be used for billing purposes

How is information stored?

All Occupational health records are stored in a secure occupational health electronic management system.

How long do we hold records for and what do we do with them after this time?

The Occupational Health record will be kept for the length of employment and for 6 years after leaving employment (this applies to Management Referrals, Preplacement Questionnaires and Vaccination / Travel health records). Health surveillance records required under Health and Safety at Work legislation must be retained in line with the retention periods stipulated in the specific regulations. For example, records that fall within the scope of the COSHH Regulations must be kept for 40 years. Following the stipulated time periods, the Occupational Health record will be expunged from the systems and deleted / destroyed.

Within Occupational Health GDPR means potential changes to processes around:

- Transparency and accountability. We will be very clear about what data we hold, how long that data will be held for, who will have access to it and how the data is used.
- Obtaining consent. Where consent is required to process your data, this will always be an active process and data will not be processed without explicit consent.
- Subject Access Requests. We will process requests , free of charge and within 1 month, subject to verification of the requestors identity.

Right to erasure

The GDPR gives the right to request records be erased. This will need to be reviewed on a case-by-case basis, as some records can be exempt from erasure, if it is thought there is any chance of litigation. Health surveillance records are exempt from the right to erasure due to the requirements of Health and Safety Law. Any records for which erasure has been agreed will be undertaken within 30 days.