Heales Medical

General Data Protection Regulations (GDPR)

General

We use the term 'employer' in this document to mean an actual employer or the University/College where you study. We use the term 'work' to mean work you undertake for your employer or the course you may be studying and any placement(s) you may be sent on.

Why we process your data

We store and process your data when an employer makes a referral to us in relation to your work . This may be to advise them on your fitness to work post offer of employment, undertake baseline health surveillance, undertake regular health surveillance because of the risks in your work, provide vaccination services because of the risks in your work, assess your fitness to work if they feel you have performance issues or you are ill, or undertake an assessment if they or you feel you are too ill to work and seek an ill-health retirement assessment or support.

Depending on the type of contract we have with your employer the service may also involve managing referrals for treatment such as musculoskeletal (physiotherapy, ostepathy or chiropractic) or counselling related services.

When you are referred to us we will also advise you on your health in relation to work and provide any support we can (within the contract we have with your employer) for you to remain at or return to work.

Your employer has the legal right to refer you to us, but you can refuse to provide information to us, attend an appointment with us, refuse consent for us to obtain further medical information etc. at any time. This may not to be your advantage however; as your employer will have the right to make their decisions based on the actions you take.

What data we store and process

The data we store and process is provided by your employer or yourself or other health professionals you have given consent for us to contact.

In order to ensure we identify you properly and can communicate with you we store your work details including work address, work number telephone and mobile, your personal address, gender, telephone number, mobile number and e-mail. This information is provided to us by your employer when they make a referral.

We willl also store information provided by your employer or yourself in relation to disability to ensure that we provide the best level of support we can when you attend Occupational Health and in relation to your fitness for work. If the information is provided by yourself it is part of your Occupational Health record and therefore confidential unless you consent to us informing your employer.

We store the referral information from your employer and any further communication between ourselves and your employer including all fitness to work advice and work we have undertaken on their behalf.

We store medical information provided to us by yourself, and if you have consented to us obtaining it, information from your GP and/or Consultants and other specialists we may refer you to and any health practitioners you receive treatment from.

Who sees your data

Within your employer, the manager who referred you to us and certain people in HR may see the information communicated by your employer to us and us to them. Who may view this information is determined by your employer. Your employer cannot see any information communicated by us to you or you to us as this forms part of your Occupational Health record. This information will never be released to your employer without your consent.

Within Heales Medical your data can be viewed by OH staff working on the contract to ensure your data is managed properly and to a satisfactory clinical standard. A member of the OH team may also ask a senior colleague to consult/advise on the case if the case is complex, this is to provide the best advice we can to both you and your employer.

The only other people who will have access to your data are limited members of the Information Technology department who are required to ensure your data is processed and stored securely and to enable them to provide support to system users or yourself with any access difficulties.

After an appointment or receipt of medical information we will normally provide your employer with a certificate to confirm the work we have undertaken on their behalf which will state the procedure carried out and confirm fitness to work. Where we need to provide a more detailed report in relation to your health we will seek your consent before we release the report to your employer.

How to access your data (Subject Access Request)

You may ask to view part or all of the information we process/store on your employer's behalf via telephone, e-mail, fax or post. We will require written confirmation of the information you wish us to provide and we will need to confirm your identity before releasing the information to yourself or a person whom you have given us consent to release it to.

We will not release information without first reviewing it to ensure that it does not contain 3rd party personal information or information that may be considered harmful to yourself.

We will provide the information to you within an encrypted password protected file or via a secure e-mail link allowing you to download the information.

It is helpful to be specific about the information you require as Occupational Health records are likely to contain substantial information. Where the time required to review, potentiall redact and provide this information may be considered excessive, or if you ask for information multiple times, we will estimate a reasonable charge and inform you of this prior to reviewing and releasing your record.

Where your data is held

All sensitive data held by Heales Medical is encrypted and held in a secure private cloud with ICloud hosting who are ISO27001 certified. All data is held and processed within the UK. Data in transit (ie.g. between internet browser and server) is encrypted.

Backup data is held within our cloud or on encrypted hard disk(s) in a secure location.

No data is transferred to a 3rd party unless it is required under law or part of a subject access request.

How long we hold your data for (data retention)

We retain data in accordance with legislation,our Data Retention Policy and Faculty of Occupational Medicine guidance. Data is archived when a client contract ceases or an ad-hoc client has not referred by business to within the previous 2 years. Data is then kept for 6 years before deletion except for clients where data has not been passed to another provider and HSE legislation requires us to keep data for a longer period (for example health surveillance records for Asbestos, HAVS, Ionising Radiation, COSHH and Lead). Data may also be retained for an individual or organisation which has taken, or where is a reasonable expectation of legal action.

When we delete your data (right to erasure/right to be forgotten)

Data will be deleted on request of the Data Controller or an individual where we cannot legally retain the data in accordance with legislation or our Data Retention policy.

N.b. It is unlikely that a request by your employer or yourself to delete your Occupational Health record under clause 17 of the GDPR will be accepted as we retain the right to hold your data under clauses 6 and 9. Data will be deleted in due course in accordance with our Data Retention policy.

References

ICO GDPR site

European Union GDPR site

Faculty of Occupational Medicine Statement