Unity Occupational Health & Wellbeing Limited as an occupational health provider, provide the full range of Occupational Health and Wellbeing Services, therefore we are responsible for the processing of medical and health information in the Occupational Health setting. The GDPR has put in place specific regulations around our type of work.

**What does the GDPR say about processing medical data?**

Article 6 of the GDPR lays out six pre-requisites to make the processing of data lawful. At least one of these must apply for it to be lawful to process data. In summary these pre-requisites are:

* Consent should be given
* Processing is necessary to fulfil contractual obligations and legal obligations
* Processing is necessary to protect vital interests (such as in life and death situations)
* Processing is in the public interest
* There is a legitimate interest pursued by the data controller

However, there are certain categories of data which cannot be processed for these six reasons. These are called ‘special categories’ and as well as information such as ethnic origin or political opinions, this also includes medical data.

Special categories of data, including medical data, cannot be processed unless one of the following applies (Article 9, 2a – 2j):

* Explicit consent is given
* Processing is necessary to carry out obligations in the field of employment
* Processing is necessary to protect the vital interests of someone where they cannot physically or legally give consent
* Processing is necessary as part of legitimate activities by a foundation, association or not-for-profit body
* Data has been made public by the data subject
* Processing is necessary to establish, exercise or defend legal claims
* There is a substantial public interest
* Processing is necessary for preventative or occupational medicine
* Processing is necessary for the benefit of public health
* Archiving or research is in the public interest

Please see Article 9 (2) h for exact wording regarding occupational health.

**What does this mean for your organisation?**

This means that in certain circumstances, namely those mentioned in Article 9, processing the medical data of your employees is acceptable, however there needs to be a legitimate reason, and the data should be processed fairly and securely. So what else do you need to do?

**What should you do if you need to process medical data?**

You and your organisation are responsible for any breaches or misuse of data. The fines for this can be very significant. The GDPR is also very clear about the handling of data.

We would recommend that before processing data, answering the following questions fully should meet the GDPR recommendations.

1. **Is it secure?**

Data can take many different formats, whether it is a hand-written form, a recorded telephone call, a Microsoft Word document, or a record on your database. They are all subject to the same law, so should all be treated with equal consideration. You need to ensure you have taken all reasonable precautions to make your medical data secure. This includes things like password protecting, encryption, not storing on shared areas or using shared email addresses, locking your office, not leaving your computer lying around.

1. **Do I need all the data I am processing?**

You should minimise the data you store on record – only required data (look at Articles 6 and 9 to see whether data is required) should be processed and stored. For example, if you are assessing someone’s fitness for work in relation to their history of asthma, asking for their medical records from 20 years ago relating to a broken leg they once suffered would neither be reasonable or necessary.

1. **How long will I be retaining the data for?**

You should have a retention schedule for all data, particularly your special category data. Typically, this may be the length of someone’s employment, plus a further three years as per your Company Policy unless the information relates to Health Surveillance Records when you will be required to keep them longer as per legislative requirements.

1. **Am I being open about my intentions?**

The data subjects (who will typically be your employees or customers) have a right to know what data of theirs is being processed and for what reason. To avoid any unnecessary confusion, you should be honest and open about your data processing and data retention.

1. **Is it easy to demonstrate?**

Under the GDPR, data subjects (in most instances) have a right to request all the data held about them, have a right to have their data corrected, and have a right to have their data deleted. Therefore, you need to be able to easily demonstrate and release all the data held on record for your staff or customers. If it is currently a long-winded process to gather all of these, looking at streamlining this would be recommended as subject access requests or ‘requests to be forgotten’ are likely to be more common in the future. It is not recommended to store data that, at a later date, you would not wish the subject to see.

Unity Occupational Health and Wellbeing Limited take data protection seriously. We operate according to very strict internal guidelines, and always ensure that medical and health data is processed fairly and lawfully. We are always willing to help our clients handle data relating to their occupational health referrals compliantly.

If you have any questions about how the GDPR relates to your processing of medical data, email us using [mail@unityoccupationalhealth.com](mailto:mail@unityoccupationalhealth.com)  and we’ll do our best to help.

|  |  |
| --- | --- |
| *SEQOHS logo redraw RGB* | 552 Dereham Road, NORWICH NR5 8TU  Telephone: 01603 250015 or 01603 250059  Email : [mail@unityoccupationalhealth.com](mailto:mail@unityoccupationalhealth.com) |