Heales Medical

GDPR

Introduction

The General Data Protection Regulations come into force on 25/5/2018.

Heales has reviewed internal processes and procedures to ensure that they will meet GDPR regulations when introduced. All internal policies/procedures comply and we have or are implementing minor changes in respects of the Occupational Health data we process on behalf of clients.

Detail

Consent

Things we are implementing to better comply with GDPR :-

- We currently assume that an employee is happy to receive e-mail and texts from us unless a referral from a client specifically requests us to send information by post. We are implementing a new procedure to e-mail an employee on referral so that they can positively confirm they are happy to continue to receive e-mails and texts (both are required) and to confirm any changes in their address. There is a risk that this can delay a referral if the employee does not respond so the Management System will e-mail the referrer at 3, 5 and 10 working days where the employee is not engaging. At 10 working days we will post (but this may be a higher cost). *We are looking at whether we can enable this to be done by the referrer prior to the actual referral, and whether to enable an auto copy of the referral to be e-mailed to the employee if the referrer wants to do this.*
- We will send an e-mail for all appointments to the employee to confirm their address details in case of change. As they will have already consented to receive e-mails and texts they will be allowed to tick a box to receive post instead. If they do this the referrer will be informed by e-mail.
- We currently send e-mails (or post) where an employee has requested to view Management Advice prior to it being released to the client. We assume consent after 3 working days (e-mail), 5 working days (post). This process will change so that if the employee does not positively provide consent we will assume refusal of consent to the same timeframe.
- A similar process to the above will apply when the employee requests a change to the Management Advice and it has been accepted or denied by Occupational Health.
- We have introduced a new Health Surveillance Fit for Work form which states the Health Surveillance advised or undertaken and which does not require employee consent. Where there is a health issue affecting the employee or their work Management Advice will be issued which does require employee consent.
- A process similar to the above will be introduced for Pre-employment/Pre-placement.

All processes may be changed/amended at any time to meet client requirements or clarification in the GDPR over time.

Subject Access Request

Client Individuals can already request copies of any part of their Occupational Health record. Staff can already request copies of personal information we hold on them. A Subject Access Request is managed via a specific case on the Management System to provide an audit trail of the written request, the processing and provision of the information.

Provision of Occupational Health information requires a review of the information held by an Occupational Health professional to ensure that information which may be considered harmful to the individual is not released.

Provision of any information requires a review to ensure 3rd party personal details are not released.

What data we process

We hold personal data on individuals referred to us by the client. This consists of information which is necessary to process medical data and avoid breaches of confidentiality such as name, address, date of birth, gender, medical information provided by the individual or obtained from other sources with their consent, medical information obtained by assessment and information contained in non-medical reports for client managers.

Where data is held

All data held by Heales companies which is processed data and/or personal/sensitive data is encrypted at rest and held in a secure private cloud with ICloud hosting who are ISO27001 certified. All data is held and processed within the UK.

Backup data is held within our cloud or on encrypted hard disk at our Head Office in Hitchin Hertfordshire.

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

All data held at rest is encrypted. All data in transit is encrypted. User acces to data is strictly controlled.

Any proposed future changes to the method or location at which data is stored will be reviewed in line with the requirements of GDPR legislation.

Who has access to data

Non-medical data on individuals referred to us may be accessed according to the client requirement. Access is conrolled via permission groups and sets and according to the client organisation hierarchy.

Medical data is only accessible to OH staff assigned to process specific client data. Access to medical data also requires a special permission set assigned to each user and is striclty controlled.

Access to the data requires a three stage logon procedure.

Medical information/Reports (which are not subject to a Subject Access Request) may be sent to individuals who are referred through secure e-mail link.

Reports/information for client managers may also be sent via a secure e-mail link.

All Heales staff and contractors sign confidentiality agreements to confirm they know and understand the importance of processing data.

Data Retention

We retain data in accordance with legislation and our Data Retention Policy. 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 three years before deletion unless for clients where data has not been passed to another provider legislation requires a longer period (for example health surveillance records for Asbestos, Ionising Radiation, COSHH and Lead). Data may also be retained for an individual or organisation which has taken legal action.

Data Deletion

Data will be deleted on request of the Data Controller or an individual where we are not required to retain the data under other legisation.

References

ICO GDPR site

European Union GDPR site

Faculty of Occupational Medicine Statement