smartclinic

CONSENT POLICY

June 2024 – V1

Background

Within occupational health informed consent is incredibly important, however can be interpreted differently by different individuals. So we have always provided very clear training and procedures around obtaining consent, all documented as part of the data protection training. Similarly we have always provided very clear instructions to clients via referral instructions, consent form instructions, informative emails, system prompts, online explainer articles and client webinars / explainer videos.

This policy documents all of this in one single, written document.

Purpose

The purpose of this Occupational Health Consent Policy is to outline the principles and procedures for obtaining informed consent from employees before conducting any occupational health assessments, treatments, or related activities. This policy ensures that all employees understand the nature, purpose, and potential outcomes of the occupational health services they receive and voluntarily agree to participate.

Scope

This policy applies to all employees, contractors, and volunteers of Smart Clinic. It encompasses all occupational health services provided directly by Smart Clinic or through external service providers.

Considerations

This policy takes into consideration a number of laws, regulations and guidance including (but not limited to):

- General Data Protection Regulation 2018
- Data Protection Act 2018
- NMC Code of Conduct (The Code); NMC (2018)
- Ethics Guidance for Occupational Health; Faculty of Occupational Medicine (2018)
- Occupational Health Ethics: From Theory to Practice; Dr Jacques Tamin (2020)
- NICE Guidelines; National Institute for Health and Care Excellence (various)
- Equality Act (2010)
- Protection of Freedoms Act (2012)
- Human Rights Act (1998)
- Occupational Health Law; Diana Kloss (2020, sixth edition)
- ICO guidance (various, but particularly Consent | ICO)
- Various articles, journals and advice from Diana Kloss, including ‘Consent to occupational health reports – Occupational Medicine v65, I9 (2015)
- Various case law, including Elmbridge Housing Trust v O’Donoghue [2004] EWCA Civ. 939, Court of Appeal and Cox v Essex County Fire And Rescue Service (Disability Discrimination : Disability) [2013]

"any **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" - UK GDPR, Article 4(11).

Article 7 also sets out further 'conditions' for consent, with specific provisions on:

- keeping records to demonstrate consent;
- prominence and clarity of consent requests;
- the right to withdraw consent easily and at any time; and
- freely given consent if a contract is conditional on consent.

The above definition provides four clear elements required for consent to be valid. At Smart Clinic, we must translate this into the context of occupational health. Therefore, we consider it as follows:

- Freely given: The individual has provided consent themselves, not via a third party, and in doing so have made their own decision without any undue pressure being placed on them.
- Specific: The details of what the individual is providing consent for are specific, and the instructions back to us providing consent are in direct response to these details.
- Informed: The individual should be made aware, at all times, of what they are providing consent to and what data or information they will be sharing as a result. Individuals must have the mental and legal capacity to provide consent.
- Unambiguous: This individual's consent instruction should be clear and direct, providing a binary (yes / no) type response wherever possible.

In addition to the above, consent must be demonstrable, so should be recorded at our end. Typically this is via a signed form, in writing, using a digital 'opt-in' style of consent, or via a recorded telephone call.

When is consent required?

Consent should be treated as a necessity prior to conducting any occupational health activities. Additionally it should not be considered as a single event, but rather a continuous process of keeping the individual knowledgeable enough to make informed decisions.

Typically we would obtain consent prior to:

- Arranging any type of assessment or appointment
- Beginning an appointment
- Releasing a confidential report or any sort of medical information to a third party, such as an employer or referrer

Withdrawal and refusal of consent

As above, consent is not a singular event, it is an ongoing process. This means that an employee / data subject should have the right and opportunity to withdraw their consent at all times.

They should also be made aware of next steps should they choose to do this, because in the same way that consent should be informed, a withdrawal of consent should also be informed.

At every instance where we obtain consent, we must also recognise and offer the option for the employee to refuse or withdraw their consent. This may be in the form of a selectable option (for example a tick box, or a button on a screen), or through verbal communication (for example during a consultation).

Consultations and appointments must always begin with confirming that the data subject consents to proceed, and this must be documented as part of the clinical notes. Similarly, the clinician needs to be able to explain what the next steps would be should the employee wish not to proceed (thereby withdrawing consent) so that this can be clearly explained and an informed decision can be made.

Common exceptions

There are specific legal exceptions to the requirement for consent. In these circumstances, data can be processed without consent having been obtained. However in such circumstances, only the data required for the activity should be processed, wherever possible the data should be pseudonymised and wherever possible the data protection officer should be consulted beforehand – although we recognise that this may not always be possible. Some likely examples of this include when:

- Processing of data is required for the establishment, exercise or defence of a legal claim – this could be in the event of an employment tribunal or liability claim.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent – this could be in the instance where an individual is at serious and imminent risk to life, or where there are safeguarding concerns.

Obtaining consent

There are four typical mediums by which we would accept proof of consent:

- In written format, such as by email or letter
- In verbal format, such as by recorded telephone conversation
- Completed online processes, such as opt-in style buttons online
- Signed forms, either signed digitally or with a ‘wet’ signature

Accidental breaches of data

In the unlikely and rare event that a data breach has occurred:

Where we are the Data Controller:

- If the breach is likely to result in a risk to the rights and freedoms of the data subject, inform the relevant supervisory authority within 72 hours.
- Document the data breach, the effects, and any remedial actions taken
- If the breach is likely to result in a high risk to the rights and freedoms of the data subject, we’ll communicate the personal data breach to the data subject without undue delay. This will be clear and in plain language. The exceptions to this would be

- If the breached data is unintelligible to any person not authorized to access it (such as encryption)
- There is no longer a high risk to the rights and freedoms of the data subject
- It would take disproportionate effort

GDPR Art. 77-84 details the rights of the data subject, our liability, and any penalties that may be imposed on us as a result.

Where we are the Data Processor acting on the instructions of a Data Controller, we will inform the Data Controller without undue delay, and assist them in any investigations and reporting requirements.

In summary the data subject has the right to:

- Lodge a complaint with a supervisory authority, without prejudice
- An effective judicial remedy against a supervisory authority
- An effective judicial remedy against us
- Representation
- Compensation and liability, proportionate to the material or non-material damage as a result