



Privacy Notice Occupational Health Services

Introduction

North West Boroughs Healthcare NHS Foundation Trust aims to be as transparent as possible and provide people with accessible information about the Trust, why it needs to collect data, what it does with the data, who it will be shared with and how and for how long it will be held.

This privacy notice is intended to answer most common questions, but if further information is required please contact the Trust's Information Governance Team by emailing IG@nwbh.nhs.uk or telephoning 01925 664485.

Who Are We?

North West Boroughs Healthcare NHS Foundation Trust is a public organisation that provides treatment, support and guidance for a range of health needs for people, both children and adults, living in Greater Manchester, Halton, Knowsley, Sefton, St Helens, Warrington and Wigan. The health needs include physical and mental health conditions and learning disabilities.

The Trust has a statutory responsibility and public duty to provide health care services, as instructed and guided by the Department of Health and Social Care (a ministerial department of Government within the United Kingdom).

The Trust's main address is:

Hollins Park
Hollins Lane
Winwick
Warrington
WA2 8WA

The Trust can be contacted at:

Main Switchboard:	01925 664000
Trust Website:	www.nwbh.nhs.uk

The Trust is a Data Controller and, as such, is registered with the Information Commissioner's Office. Its registration number is Z8591053.

The Trust's Data Protection Officer (DPO) is the Information Governance & Security Manager, who is supported in this role by the Information Governance Team. The DPO can be contacted by emailing DPO@nwbh.nhs.uk or IG@nwbh.nhs.uk or phoning 01925 664485.

Why does the Trust need your Information?

Our Occupational Health Service, located at Hollins Park, works to promote and maintain the health and wellbeing of our staff. It provides occupational health and wellbeing services to both Trust staff and external partner organisations (including public and private organisations) and their employees.

The service needs your information to enable it to provide occupational health and wellbeing services and to ensure that health and safety legislation is adhered to through the provision of:

- pre-employment screening,
- general occupational health services to support the employment policies and in particular the wellbeing of employees via Occupational Health physicians, nurses, counsellors and physiotherapists.
- health and wellbeing assessments and monitoring your health and wellbeing to enable effective work and fitness to work,
- immunisations,
- workplace counselling, and
- health surveillance to ensure employee health is not adversely affected by physical, chemical and biological hazards.

The Trust keeps records about your occupational health to ensure your health and wellbeing and ensure you are fit to undertake your role effectively. Whilst the Trust receives information from you when you come into contact with it, it also receives information about you from other individuals or organisations, such as when you are referred to our service. The Trust needs enough information to be able to provide you with appropriate occupational healthcare services.

What will it be used for?

The Occupational Health Service will process your data in order to:

- identify you, create your Occupational Health record and ensure that your occupational health information is filed correctly,
- assess and protect your health and wellbeing and your fitness to work,
- identify a baseline of your health and wellbeing against which to measure and monitor any future changes,
- provide advice to managers on the impact of your health and wellbeing on work and the impact of work on your health and wellbeing,
- promote your abilities and help support any disabilities in the workplace,
- identify any additional support that would help you to improve your health and wellbeing, and
- comply with Health and Safety legislation.

Please note that the Trust does not use automated decision-making services (where decisions are made based on your personal data without any human intervention).

What Data is Held?

There are two types of data that the Trust uses: personal and special category. Personal data means any information relating to a person who can be directly (eg by name or picture) or indirectly (eg by age, gender and post code) recognised. Special category data means any information relating to racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life or details of criminal offences.

Data collected by our Occupational Health Service includes:

- personal information (for example name, address, date of birth, National Insurance number, NHS number, etc),
- personal characteristics (for example gender, ethnicity, etc),
- contact details (for example telephone numbers and/or email address),
- employment information (for example employee number, start date, job title/post, contracted hours, details of role/tasks undertaken, previous roles, occupational exposure, etc),
- absence information (for example dates of absences, reasons for absence, etc),
- health information (for example health questionnaires, immunisations, health surveillance information, nature of ill health, symptoms, relevant medical history, etc), and
- GP and/or specialist contact details and reports containing medical information.

The Trust will maintain a record of your care that consists of things such as:

- any contacts you have with staff (eg visits and appointments),
- notes or a summary of discussions, and
- relevant information provided from other professionals, referrers or those who know or are concerned about you.

Your information will primarily be held electronically. When accessing occupational health services, you are registered and your Occupational Health record is created on our Occupational Health system. Information within this system is held securely and confidentially, with access restricted to only relevant staff and managers.

Some records are still held in paper format, particularly historical occupational health records. These are stored securely and may be transferred to electronic format at some point.

Lawful Basis for Processing

Occupational health records consist of two main distinct components: general transferable information (Part 1) and the confidential clinical record (Part 2).

Part 1 will include basic information relating to employment, history of any reported exposure to hazards and other relevant information such as types and dates of immunisations, accidents in the workplace and environmental monitoring data. This information will generally be accessible to the employee, management and regulatory authorities (eg Health and Safety Executive).

Part 2 will include confidential clinical information about the health of staff during employment and is personal to the employee. It will include occupational health questionnaires, subsequent clinical information, details of any biological monitoring or clinical examinations, and relevant correspondence and details of any health surveillance carried out.

Any decisions on processing, including disclosing and sharing of information, will be considered and made on a case-by-case basis. Confidential clinical information from Part 2 will not be passed on to any other person outside the Occupational Health Service without the written consent of the employee concerned or another appropriate legal basis.

Under current Data Protection legislation (the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)) the Trust will process the following types of information for the legal bases specified.

Type of Information	Legal Basis for Processing (within GDPR)
Occupational health and wellbeing assessments	<p>Personal data processing is necessary for: Article 6(1)(b) – “Contractual necessity” Article 6(1)(c) – “Compliance with legal obligations” or Article 6(1)(e) – “Exercise of official authority”</p> <p>Special category data processing is necessary for: Article 9(2)(a) – “Explicit consent” (when sharing with line managers, employers, etc) Article 9(2)(b) – “Employment and social security” purposes, or Article 9(2)(b) – “Health and social care” purposes (when sharing with GPs, consultants, etc) Article 9(2)(i) – “Public health” purposes</p>
Health surveillance	<p>Personal data processing is necessary for: Article 6(1)(c) – “Compliance with legal obligations” or Article 6(1)(e) – “Public interest”</p> <p>Special category data processing is necessary for: Article 9(2)(i) – “Public health” purposes</p>

Type of Information	Legal Basis for Processing (within GDPR)
Pre-employment screening	<p>Personal data processing is necessary for: Article 6(1)(b) – “Contractual necessity”</p> <p>Special category data processing is necessary for: Article 9(2)(b) – “Employment and social security” purposes</p>
Immunisations, vaccinations and bloods	<p>Personal data processing is necessary for: Article 6(1)(b) – “Contractual necessity” Article 6(1)(c) – “Compliance with legal obligations” or Article 6(1)(e) – “Exercise of official authority”</p> <p>Special category data processing is necessary for: Article 9(2)(a) – “Explicit consent” (when sharing with line managers, employers, etc) Article 9(2)(b) – “Employment and social security” purposes, or Article 9(2)(b) – “Health and social care” purposes (when sharing with GPs, consultants, etc) Article 9(2)(i) – “Public health” purposes</p>

The Trust has an obligation to protect the health of the general public and where this is done your personal data will be processed “for the performance of a task carried out in the public interest” (Article 6(1)(e)). Where your special category data is processed, this is done because it is necessary “for reasons of public interest in the area of public health” (Article 9(2)(i)).

As a healthcare provider, there may be occasions where we need to process personal and/or special category data because someone is at risk of serious harm (eg life or death situations in emergencies or major incidents) and, where we do this, we will process the information to “protect someone’s vital interests” (Articles 6(1)(d) and 9(2)(c)).

Sometimes there are occasions when we are obliged to process information in order to comply with a court order, coroner’s instruction, to prevent or detect crime or to comply with the law (eg to provide the Secretary of State with information and reports on the status, activity and performance of the Trust). If we have to do this with your information, we will ensure there is a legal justification for such processing (eg Article 6(1)(c)).

If we process your information for other purposes that are not described above then we will seek your consent to do so before we process it.

If the Trust wishes to use your personal information for a new purpose that is not covered by this Privacy Notice, then we will provide you with a new notice explaining the new use prior to commencing the processing, setting out the relevant purposes and processing conditions. Where and whenever necessary, we will ensure there is a legal justification for such processing.

Who do we Share Data with?

The types of organisations and people the Trust shares data with include (but are not limited to):

- managers and staff, including those from external organisations, referring individuals to the service,
- Occupational Health employees including administrative staff,
- human resource employees (with a strict business need to know),
- GPs and/or other healthcare professionals,
- employing organisations and organisations we are contracted with to provide services to,
- other healthcare professionals (eg doctors, nurses, ambulance services, etc),
- partner organisations who contribute to your long-term care (eg GPs, social services/local authorities, education, private sector providers, etc),
- other organisations where TUPE rules apply (see the *Privacy Notice – Employee and Volunteer Information* for further information on TUPE),
- bodies with statutory investigative powers (eg NHS Resolution, the Care Quality Commission, General Medical Council, Nursing and Midwifery Council, Audit Commission or Health Service Ombudsman),
- Government departments for national screening programmes and other national initiatives (eg NHS England, Public Health England or the Home Office), and
- police, emergency and out-of-hours services, courts (including coroner's court), solicitors and tribunals and enquiries.

The sharing of your data for the purposes of direct care, both within the Trust and with others outside the Trust, is allowed by law.

Any disclosures will be considered on a case-by-case basis to determine if they are appropriate and what the legal basis is for sharing. Where applicable, your consent will be sought to share information with other organisations for non-care purposes. When asking for this, we will ensure that you are given all the information necessary to make a fully informed decision.

If the sharing goes ahead, only the minimum personal data necessary for the specific purposes and circumstances will be shared, with all suitable security controls in place. Any organisations receiving person-identifiable information from us are legally obligated to protect it.

The Trust will not share your information for marketing, social media or insurance purposes unless it has your consent to do so. If you do consent to this, you have the right to withdraw your consent to the processing at any time.

Information provided under the Freedom of Information Act 2000 will not include person-identifiable details about patients.

Looking after your Information

The Trust takes its duty to protect your personal information and confidentiality very seriously and we are committed to taking all reasonable measures to ensure it is kept confidential and secure and used appropriately. Everyone working for the NHS has a contractual and legal duty to protect your information.

Personal information is held in accordance with the requirements of current Data Protection legislation. Anyone who receives information from us is also under a legal duty to keep it confidential and secure in accordance with Data Protection legislation.

We strive to ensure that all personal information under our control is handled in accordance with all legal, professional and ethical obligations. Policies and procedures are in place to safeguard information, which staff are responsible for adhering to, and all staff are provided with mandatory training to assist them in fulfilling their obligations.

Access to personal information is strictly controlled and restricted to only those with a legitimate work related need to access it.

Safeguarding

Some members of society are recognised as needing protection, for example children and vulnerable adults. If a person is identified as being at risk from harm The Trust must do what it can to protect them.

Where there is a suspected or actual safeguarding issue the Trust will share relevant information that it holds with other relevant agencies, regardless of whether or not the individual or their representative agrees. The laws that allow this processing to be undertaken without consent are the Children Act 1989 (Section 47) and the Care Act 2014 (Section 45).

Your Rights

Right to Access

You have the right to access the data held about you, except for information that:

- has been provided in confidence by someone else without consenting for you to see it,
- relates to serious criminal offences, and/or
- could cause physical or mental harm to you or someone else.

To request access to Occupational Health records held by the Trust, please contact the Occupational Health Service by emailing to OccHealth@nwbh.nhs.uk or phoning 01925 664010.

Right to Data Portability

This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated (Article 6(1)(a) and (b)).

Right to Erasure

You have the right to ask us to erase your personal information in certain circumstances (when processing is being undertaken in compliance with Article 6(1)(a), (b) or (d)).

Right to Object

People who have access to your information will only normally have access to that which they need to fulfil their roles. You have the right to object to processing if the processing forms part of our public tasks, or is in our legitimate interests (Article 6(1)(e)). However, the Trust may still share information even if you have objected where there is a valid legal justification (eg someone is at serious risk).

If you wish to object to the sharing of your information as part of streamlining and the IAT process, please contact the Trust's Resourcing Team.

Right to Rectification

You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. For further information please speak to your line manager in the first instance. Further guidance can be obtained from the Information Governance Team by emailing Records@nwbh.nhs.uk or phoning 01925 664895.

Further Information on your Rights

For further information regarding your rights, please see the ICO's website: <https://ico.org.uk/global/privacy-notice/your-data-protection-rights/>. Alternatively, you can contact the Trust's Information Governance Team by emailing IG@nwbh.nhs.uk or phoning 01925 664485.

Retention Period

The Trust retains the information it holds in line with the Records Management Code of Practice for Health and Social Care 2016¹, following which it usually be confidentially destroyed.

¹ <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

Transferring Information Abroad

The Trust does not routinely transfer information outside the UK, but if there is a need to do so it will be done in a way that ensures the security of the information is to an equivalent standard as that used internally by the Trust when processing your information.

Use of Email

The Occupational Health Service will use secure email to communicate with you. When you receive it, you will be asked to set up an account to access the email. Thereafter, any replies to the encrypted email will be secured.

Closed Circuit TV (CCTV)

The Trust uses Closed Circuit TV to help reduce the fear of crime for patients, staff and visitors to its sites and to protect its premises and assets from criminal activity. In addition, CCTV may be used to monitor difficult to observe areas where patient or public safety could be compromised. If an incident occurs, the CCTV footage may be shared with the police for the purposes of investigating a crime. However, the Trust ensures that the use of CCTV complies with all relevant regulatory acts of law.

Trust Website

You can browse the Trust's website without disclosing personal data. However, the Trust may store information about you using cookies, which are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org.

The Trust also uses Google Analytics² to collect information about how visitors use its website. The information is used to compile reports and to help improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website, where visitors have come to the website from and the pages they visited. To opt out of being tracked by Google Analytics across all websites, visit <http://tools.google.com/dlpage/gaoptout>.

The Trust's website contains links to other (external) sites. The Trust is not responsible for the privacy practices and content of these sites. The Trust encourages you to be aware of this when you leave its site and to read the privacy statements on the other websites.

² <https://policies.google.com/privacy/update>

Right to Complain

The Trust aims to make sure that the services it delivers are provided to the highest standard. If you have any concerns about the way the Trust has handled its data, you can raise your concerns or make a complaint.

- To raise a complaint, please speak to your line manager or your Freedom to Speak Up Champion or Guardian, in the first instance (if you are employed by the Trust).

Alternatively, if you are not employed by the Trust, please contact the Complaints Team by emailing Complaints@nwbh.nhs.uk or phoning 01925 664004.

- To raise a concern, please contact the Information Governance Team by emailing IG@nwbh.nhs.uk or phoning 01925 664485.
- To make an external complaint about the Trust's data handling, please contact the ICO by emailing casework@ico.org.uk or phoning 0303 123 1113.