

Privacy Notice – Patient Information



Optimums Health Limited (Trading as Panacea Pharmacy) is a ‘Data Controller’ under Data Protection Legislation, including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the “GDPR”), and the Data Protection Act 2018.

This means we are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the current and future data protection principles. We must also notify the Information Commissioner about all of our data processing activity.

Panacea takes your confidentiality and privacy rights very seriously. This notice explains how we collect, process, transfer and store your personal information and forms part of our accountability and transparency to you under current Data Protection Legislation.

We recognise the need to treat your personal and sensitive data in a fair and lawful manner. We will process your personal information fairly and lawfully by;

- Only using it if we have a lawful reason and when we do, we make sure you know how we intend to use it and tell you about your rights;
- Only collecting and using your information to provide you with your care and treatment and will not use it for anything else that is not considered by law to be for this purpose;
- Only using enough of your personal information that will be relevant and necessary for us to carry out various tasks within the delivery of your care;
- Keeping your information accurate and up to date when using it and if it is found to be wrong, we will make it right, where appropriate, as soon as we can;
- Only keeping your information in a way that it will identify you for as long as we are legally required to, whilst ensuring your rights;
- Having secure processes in place to keep your personal information safe when it is being used, shared, and when it is being stored.

What types of information do we collect about you?

We collect basic “personal” data about you which does not include any special types of information or location-based information, however we will also collect sensitive confidential data known as “special category personal data”, and during the services we provide to you and or linked to your healthcare through other health providers or third parties.

This “personal” and “special category” information may include:

- Basic details such as name, address, date of birth, phone number, and email address
- Your next of kin and contact details
- Your religious beliefs, ethnicity and sex (if required in a healthcare setting)
- Notes and reports about your physical or mental health condition and any treatment, care or support you need and receive
- Results and images of your tests and diagnosis
- Relevant information from other professionals, relatives or those who care for you or know you well

- Records of any contacts you have with us such as home visits or outpatient appointments or with other health professionals or service providers
- Information on medicines, side effects and allergies
- Information on your personal preferences relating to your care
- Patient experience feedback and treatment outcome information you provide
- Recordings of telephone calls, meetings (where advised)
- CCTV Images form within the estate of the Trust whilst on site
- And other health information that is relevant to us providing your care

The information which you provide us and which we hold about you may be in an electronic or paper format, or a mixture of both.

What is our purpose of processing your data?

Health and social care professionals working with you – such as pharmacists, doctors, nurses, support workers, psychologists, occupational therapists, social workers, administrators and other staff involved in your care including administrators – keep records about you, your health and any care and treatment you receive.

Your information is used to guide and record the care you receive and is vital in helping us to;

- provide quality healthcare to you as a patient / user of our services
- have all the information necessary for assessing your needs and for making decisions with you about your care.
- confirm your identity to provide our services
- assess the quality of care we give you and provide to others
- ensure we can properly investigate if you and your family have a concern or a complaint about your healthcare
- ensure we meet our statutory and legal obligations under the Health and Social Care Act 2016
- to protect the health of the public and to help us manage the NHS
- to protect staff, patients visitors and Trust property (CCTV Images)

Professionals involved in your care will also have accurate and up-to-date information and this accurate information about you is also available if you:

- Move to another area
- Need to use another service
- See a different healthcare professional

We do not rely on consent to use your information as a 'legal basis for processing'.

We rely on specific legal provisions under Article 6 and 9 of the GDPR to provide you with Healthcare, for the purposes described in this notice we will be lawfully using your information in accordance with:

Personal Data – under **Article 6(1)(e)** *“Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.*

Sensitive (Special Category) Personal Data – under **Article 9(2)(h)** *“processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”.*

However, you do have the right to say 'NO' to our use of your information but this could have an impact on our ability to provide you with the services you require.

Who might we share your information with?

Your information will be shared with the team who are caring for you and are providing treatment to you, including with the teams whom provide administration services to enable your care and only where necessary.

In order for the TRUST to fulfil its functions, information may also be shared between various organisations with strict agreements on how it will be used, examples of these include:

General Practices (GP's), Other Acute Hospitals, Community Services, Mental Health Care Providers, Walk-in Centres, Urgent Care Centres, Ambulance Services, dentists, pharmacists, NHS England, NHS Digital, General Medical Council (GMC), Nursing and Midwifery Council (NMC) information can also be shared directly by service users and many others.

Information may also need to be shared with other non-NHS organisations, from which you are receiving care and other agencies that are supporting your care, examples of these include:

Social care services, education services, hospices, nursing homes, respite centres, voluntary sector providers and private healthcare organisations with whom we work together or with other professionals and services involved in your care.

We do this in order to provide the most appropriate treatment and support for you, and your carers, or when the welfare of other people is involved. We will only share your information in this way if it is considered necessary and we have a legal basis to do so.

There are times when we need to share information with other organisations such as our local authority partners, outside healthcare providers, clinical commissioning groups, the Department of Work and Pensions and the DVLA. We will only share information in this way if we have your permission, or we have a legal basis and it is considered necessary.

In the circumstances where we rely on consent as our legal basis to share then you have the right to refuse/withdraw your consent to information sharing at any time.

However, a person's right to confidentiality is not absolute and there may be other circumstances when we must share information from your patient record with other agencies. In these rare circumstances we are not required to have your consent.

Examples of this are:

- If there is a concern that you are putting yourself at risk of serious harm
- If there is concern that you are putting another person at risk of serious harm
- If there is concern that you are putting a child at risk of harm
- If we have been instructed to do so by a Court
- If the information is essential for the investigation of a serious crime
- If you are subject to the Mental Health Act (1983), there are circumstances in which your 'nearest relative' must receive information even if you object
- If your information falls within a category that needs to be notified for public health or other legal reasons, such as certain infectious diseases

Sharing to improve Health, Care and Services through planning - To help us monitor our performance, evaluate and develop the services we provide, it is necessary to review and share minimal information, for example with the NHS Clinical Commissioning Groups. The information we share would be anonymous so you cannot be identified and all access to and use of this information is strictly controlled.

In order to ensure that we have accurate and up-to-date patient records, we carry out a programme of clinical audits. Access to your patient records for this purpose is monitored and only anonymous information is used in any reports that are shared internally within our Trust.

Sharing to improve Health, Care and Services through Research - The Trust actively promotes research with a view to improving quality of services for the future. You may have the opportunity to participate in an important research study. If you would like to get involved in our research please discuss this with the team who are providing your treatment. If we use your patient information for research, we remove your name and all other personal data which would identify you. If we need the information in a form that would personally identify you, we would ask for your permission first.

Great North Care Record/ Medical Interoperability Gateway (MIG) - New models of service delivery are being implemented, with closer working with GPs and other healthcare and social care providers. To assist this, the use of other electronic patient record systems to share your information will be implemented. You will be given the opportunity to say no and to opt-out of this sharing. To do this, please speak to your GP or the team providing your treatment.

Sharing for the Prevention and Detection of Crime - We may also use the information we hold about you to detect and prevent crime or fraud and where appropriate and where we have a legal basis share with relevant agencies. We may also share this information with other bodies that inspect and manage public funds.

Sharing for safeguarding - Advice and guidance is provided to care providers to ensure that adult and children's safeguarding matters are managed appropriately. Access to identifiable information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

In some circumstances we may also rely on GDPR **Article 6(1)(d) and Article 9(2)(c)** as our legal basis to process and share your information but only *"when it is necessary to protect the vital interest of a person who is physically or legally incapable of giving consent"*.

National Patient Surveys & Audits - is part of the government's commitment to ensure patient feedback is used to inform the improvement and development of NHS services. We may share your contact information with an NHS approved contractor to be used for the purpose of national surveys and audits. You do not have to participate in these surveys and the information will contain contact details to opt out..

You have the right to object to us sharing your information to NHS Digital – this will not affect your care in any way. For information about how you can Opt-Out of sharing your data with NHS Digital please visit the NHS Digital National Data Opt-Out Programme Website.

Data Processors - Panacea have entered into contracts with other organisations to provide services for us. These range from software companies to provide our Electronic Patient Records to contractors who provide specialist clinical services that help provide a better service to you. These contractors may hold and process data including patient information on our behalf.

These contractors are known as '**Data Processors**' and subject to the same legal rules and conditions for keeping personal information confidential and secure. We are responsible for making sure that staff in those organisations are appropriately trained and that procedures are in place to keep information secure and protect privacy. These conditions are written into legally binding contracts, which we will enforce if our standards of information security are not met and confidentiality is breached.

How do we keep information safe?

We are committed to keeping your information secure and have operational policies and procedures in place to protect your information whether it is in a hardcopy or electronic format. We ensure that we comply with current data protection legislation including the Data Protection Act (DPA) and General Data Protection Regulation (GDPR)

All of the Information Systems used by Panacea are implemented with robust information security safeguards to protect the confidentiality, integrity and availability of your personal information. The security controls adopted by the Trust are influenced by a number of sources including the 10 National Data Guardian Standards and guidelines produced by NHS Digital and other Government standards.

Everyone working for Panacea is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for the purposes advised and/ or consented to, unless

it is required or permitted by the law. All of our staff receives annual Data Security training to ensure they remain aware of their responsibilities. They are obliged in their employment contracts to uphold confidentiality, and may face disciplinary procedures if they do not do so.

We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing.

Your information is never collected or sold for direct marketing purposes.

Do we process information overseas?

Data collected will not be sent to countries where the Laws do not protect your privacy to the same extent as the law in the UK, unless rigorous checks on the security and confidentiality of that data are carried out in line with legal requirements.

Your information is not currently processed overseas and we do not transfer personal information to a country outside of the European Union (EU) and this is checked on a regular basis. If it is found that we intend to share information outside of the EU, appropriate and suitable safeguards will be put in place, which you will be told about.

How long do we retain information?

Your information is retained in compliance with the Records Management Code of Practice for Health and Social Care 2016 which details retention periods for your records. This is available on the NHS Digital website at <https://digital.nhs.uk/information-governance-alliance> or on the Trust's website <https://www.nth.nhs.uk>

Currently we keep adult health records for a minimum of eight years, maternity records are kept for a minimum of 25 years and children's records until their 26th birthday.

We keep CCTV images for 28 days from the day of capture.

We keep a paper copy of your prescription for a minimum of 2 years, this may increase dependent upon the classification of the medicines supplied against that prescription

Your rights and how we adhere and protect them?

Data Protection law gives individuals rights in respect of the personal information that we hold about you and these apply in circumstances where the relevant conditions are met.

These rights are,

1. **Right of access by the data subject** - You have the right to request a copy of the information we hold about you and supplementary information about what we process and the legal basis for processing. Further information on this process can be found in this privacy notice under the '**How can I access my information?**' section. This is also commonly known as a Subject Access Request.
2. **Right to rectification** – Data must be accurate; you have the right to request correction of any data that you believe is incorrect. However, where we not the author

/creator/originator of the information this request will be forward to the relevant party for them to take forward.

Any requests for information to be rectified will be considered on a case by case basis and requests should be made initially to the Data Protection Officer.

3. **Right to erasure ('right to be forgotten')** - A data subject has the right to have personal data concerning them erased without undue delay where one of the following applies:
- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
 - The data subject (you) withdraws the consent or explicit consent on which the processing is based and where there is no other legal ground for the processing.
 - Where the data subject exercises their 'right to object' regarding processing in the public interest or legitimate interests of the DC, (Article 21(1)) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes, (Article 21(2))
 - The personal data have been unlawfully processed
 - The personal data must be erased for compliance with a legal obligation
 - The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) relating to a child's data.

Any requests for information to be destroyed will be considered on a case by case basis and requests should be made to the Data Protection Officer.

4. **Right to restriction of processing** - You have the right to request restriction of process where one of the following applies:
- Accuracy of personal data is contested
 - Processing is unlawful
 - The Trust no longer requires the information but the data subject has requested it is retained to enable them to establish, exercise or defense of legal claims
 - Pending verification of the outcome of the Right to object
 - Where processing has been restricted

Any requests for information to stop processing will be considered on a case by case basis and requests should be made to the Data Protection Officer. The Trust will advise any other organisation we have shared data with the correction, destruction or restriction of processing that data.

5. **Right to data portability** - The right to data portability allows data subjects (you) to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
6. **Right to object** - You have the right to object to the processing of personal and/or sensitive data that is likely to cause or is causing damage or distress when obtaining consent has been chosen as the lawful basis for processing.

All requests will be considered on a case by case basis and requests should be made to the Data Protection Officer.

7. **Rights in relation to automated decision making and profiling** - You also have the right to object to any automated decision-making including profiling. Currently Panacea does not undertake any automated decision-making or profiling.
8. **Right to Lodge a complaint to the Information Commissioner Office (ICO)** - You have the right to lodge a complaint if you are not content with the outcome of your confidentiality and data protection complaint and/or concern raised with the Trust.

Post: The Information Commissioner's Office,
Wycliffe House, Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

Helpline: 0303 123 1113 (Local Rate) or +44 1625 545 745 (outside UK)

Online: www.ico.org.uk

More Information about Your Rights

There are additional restrictions to the above rights of individuals and these are listed in GDPR Article 23 and can be obtained from the Trust on request.

For further information on your rights please visit the ICO website www.ico.org.uk or contact the Trust Data Protection Officer.

How can I access my information?

You have the right to obtain from us confirmation as to whether or not personal data concerning you is being processed, and, where that is the case, **access to the personal data** and the following information if required:

- (a) the purposes and legal basis of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the Trust rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with the ICO;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling giving meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (i) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Once your request has been received and your identity / entitlement verified, your request will usually be completed within one calendar month. However, if your records are extensive we may take longer to process your request but will inform you from the outset where possible, and in any case within 30 days.

To submit a formal request for information, please contact:

Medical Legal Team (Panacea Requests)
Medical Records Department
University Hospital of North Tees
Hardwick Road
Stockton-On-Tees
TS19 8PE

Telephone: 01642 383516
(Monday and Friday, 8.30am to 5pm)

Data Protection Officer

The Trust's Data Protection Officer (DPO) is responsible for ensuring that the Trust complies with the GDPR. The DPO is the person to contact if you would like to know more about how we use your information, if you require information in any accessible format or language, you wish to make a complaint or if (for any reason) you do not wish to have your information used in any of the ways described.

The DPO contact details are:

Data Protection Officer
Information Governance Department
University Hospital of North Tees
Hardwick Road
Stockton-On-Tees
TS19 8PE

Telephone: 01642 624470

Or email to information.governance@nth.nhs.uk

Customer Services and Complaints

We welcome comments about your care and about how we use your information. If you have any comments or complaints please contact:

Patient Experience Team (Panacea Requests)
University Hospital of North Tees
Hardwick
Stockton on Tees
TS19 8PE

Telephone: 01642 624719
Monday – Friday, 9.00 am – 4.00 pm

In addition, the Patient Advice and Liaison Services (PALS) are available to assist you with your comments, concerns and complaints. The PALS team act independently of clinical teams to ensure your concerns are investigated and responded to in an effective and timely manner. Details of the various ways to contact the PALS team, at our various locations, can be found on the Trust's website: <https://www.nth.nhs.uk>

Further Information

Should you have any further queries on the uses of your information, please speak to your health professional or our Data Protection Officer.

Changes

It is important to point out that we may amend this Privacy Notice from time to time.

Last Reviewed: 14 December 2018