

Winterton Medical Practice

Data Protection Privacy Notice for Patients

Version	Review Update	Published /Reviewed date	Published/Reviewed by	Job Title	Review Due
1.0	First Version	June 2019	Gail Holland	Practice Manager	June 2020
1.1	Review	January 2021	Gail Holland	Practice Manager	January 2022
1.2	Review – Update DPO	May 2021	Gail Holland	Practice Manager	May 2022
1.3	Review – Added Re: Recording of Telephone Calls	Feb 22	Gail Holland	Practice Manager	Feb 23
1.4	Review – Updated CSU to ICS	April 23	Gail Holland	Practice Manager	April 24
1.5	Reviewed – Changes to DPO email and address	January 2025	Victoria Carnaby	Assistant PM	January 2026
1.6	Insertion regarding Heidi AI	May 25	Gail Holland	Practice Manager	January 2026

Introduction:

This privacy notice lets you know what happens to any personal data that you give to us, or any that we may collect from or about you.

This privacy notice applies to personal information processed by or on behalf of the practice.

This Notice explains

- Who we are, how we use your information and our Data Protection Officer
- What kinds of personal information about you do we process?
- What are the legal grounds for our processing of your personal information (including when we share it with others)?
- What should you do if your personal information changes?
- For how long your personal information is retained by us?
- What are your rights under data protection laws?

The General Data Protection Regulation (GDPR) became law on 24th May 2016. This is a single EU-wide regulation on the protection of confidential and sensitive information. It enters into force in the UK on the 25th May 2018, repealing the Data Protection Act (1998).

For the purpose of applicable 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 (currently in Bill format before Parliament) the practice responsible for your personal data is the Winterton Medical Practice.

This Notice describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights

How we use your information and the law.

Winterton Medical Practice will be what's known as the 'Controller' of the personal data you provide to us.

We collect basic personal data about you which does not include any special types of information or location-based information. This does however include name, address, contact details such as email and mobile number etc.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious belief (if required in a healthcare setting) ethnicity, and sex during the services we provide to you and or linked to your healthcare through other health providers or third parties.

Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g. NHS Trust, GP Surgery, Walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

NHS health records may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Records which the Practice hold about you may include the following information;

- Details about you, such as your address, carer, legal representative, emergency contact details
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments, etc.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals, relatives or those who care for you
- Contact details (including email address, mobile telephone number and home telephone number)

To ensure you receive the best possible care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS. Information may be used within the GP practice for clinical audit to monitor the quality of the service provided.

How do we lawfully use your data?

We need to know your personal, sensitive and confidential data in order to provide you with Healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with: -

Article 6, 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;"

Article 9, (h) processing is necessary for the purposes of preventive 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

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from a number of sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information is only provided back to your

GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way.

Medicines Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments.

Patient Communication

The Practice will use your name, contact details and email address to inform you of NHS services, or provide information about your health/information to manage your healthcare or information about the management of the NHS service. There may be occasions where authorised research facilities would like you to take part in research in regard to your particular health issues, to try improve your health, your contact details may be used to invite you to receive further information about such research opportunities.

Telephone Call Recording

All telephone calls into and out of the practice will be recorded. The practice will retain this data for a period of 12 months and then it will be deleted.

The recordings will be available to practice staff to review and to patients to request under a Subject Access Request.

The recordings will not be shared outside the practice other than when there is a specific legal basis such as if requested by the police or any other formal investigation which could include medical purposes such as a clinical investigation or CQC action.

Safeguarding

The Practice is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied with the wellbeing of all, at the heart of what we do.

Our legal basis for processing For the General Data Protection Regulation (GDPR) purposes is: -

Article 6(1)(e) ‘...exercise of official authority...’.

For the processing of special categories data, the basis is: -

Article 9(2)(b) – ‘processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law...’

Research

Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here: -

<https://cprd.com/transparency-information>

The legal bases for processing this information

CPRD do not hold or process personal data on patients; however, NHS Digital (formally the Health and Social Care Centre) may process 'personal data' for us as an accredited 'safe haven' or 'trusted third-party' within the NHS when linking GP data with data from other sources. The legal bases for processing this data are:

- Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) - public interest in the area of public health
- Medical research and statistics: Article 6(e) and Article 9(2)(j) - public interest and scientific research purposes

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

Categories of personal data

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is necessary or possible to obtain in order to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Sources of the data

The Practice will either receive or collect information when someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

Recipients of personal data

The information is used by the Practice when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e. their GP or mental health team).

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice will use carefully selected third party service providers. When we use a third party service

provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately.

Examples of functions that may be carried out by third parties includes:

- *Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.*
- *Delivery services (for example if we were to arrange for delivery of any medicines to you).*
- *Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).*

Further details regarding specific third-party processors can be supplied on request.

How do we maintain the confidentiality of your records?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The General Data Protection Regulations 2016
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Our practice policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the General Data Protection Regulations (GDPR) and all UK specific

Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Winterton Medical Practice an appropriate contract (art 24-28) will be established for the processing of your information.

In Certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the Data Protection Officer in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information to

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details and email address to inform you of other services that may benefit you, we will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt in to such programmes.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.

This information is not shared with third parties or used for any marketing and you can unsubscribe at any time via phone, email or by informing the practice DPO as below.

National Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning.

Who can use your confidential patient information for research and planning?

It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

Making your data opt-out choice

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Will choosing this opt-out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt out securely online or through a telephone service.

You can change your choice at any time. To find out more or to make your choice visit nhs.uk/your-nhs-data-matters or call 0300 303 5678

Where do we store your information electronically?

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

No 3rd parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place. We have a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations.

- NHS Trusts / Foundation Trusts
- GP's
- North Primary Care Network
- Safecare – GP Federation
- NHS Medicines Optimisation Team
- NHS Integrated Care Systems
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Other 'data processors' which you will be informed of

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

Computer System

This practice operates a Clinical Computer System on which NHS Staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history, including allergies and medication.

To provide around the clock safe care, unless you have asked us not to, we will make information available to trusted organisations. Wherever possible, their staff will ask your consent before your information is viewed.

We consider patient consent as being the key factor in dealing with your health information.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to other systems. The general principle is that information is passed to these systems unless you request this does not happen, but that system users should ask for your consent before viewing your record.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for

[Practice Name] an appropriate contract (art 24-28) will be established for the processing of your information.

The Yorkshire & Humber Care Record

The Yorkshire & Humber Care Record is a shared system that allows Healthcare staff within the Humber, Coast and Vale Health and Social Care community to appropriately access the most up-to-date and correct information about patients; to enable us to deliver the best possible care.

The Yorkshire & Humber Care Record Guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing.

If you would like any further information, or would like to discuss this further, please contact the data protection officer whose contact details are shown below.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- where there is a serious risk of harm or abuse to you or other people;
- where a serious crime, such as assault, is being investigated or where it could be prevented;
- notification of new births;
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
- where a formal court order has been issued;
- where there is a legal requirement, for example if you had committed a Road Traffic Offence.

How long will we store your information?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at (<https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>)

How can you access, amend move the personal data that you have given to us?

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to

your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project), or consent to market to you, you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will Delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP to GP data transfer and transfer of your hard copy notes

Primary Care Network

The objective of primary care networks is for group practices together to create more collaborative workforces which ease the pressure of GP's, leaving them better able to focus on patient care.

Primary care networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Use of Heidi AI in NHS GP Consultations

This section explains how our GP practice uses patient data when incorporating Heidi Health, an AI-powered medical scribe, into consultations. Heidi Health assists clinicians by transcribing medical consultations to improve documentation and reduce administrative workload while maintaining patient care quality and confidentiality.

Purpose of Processing The use of Heidi Health aims to

- Enhance accuracy and efficiency in medical record-keeping.
- Reduce administrative workload for clinicians.
- Improve patient-clinician interaction by allowing clinicians to focus on care rather than note-taking.

How Data is Collected and Processed

- During a consultation, Heidi Health transcribes real-time discussions between patients and clinicians.
- The transcribed information is reviewed and validated by the clinician before being added to the patient's medical record.
- Data is processed within a secure environment, ensuring compliance with NHS Digital and UK GDPR requirements.

Data Sharing and Security Measures

- Heidi Health does not share patient data with third parties without explicit consent, except where legally required (e.g., safeguarding, legal obligations).
- Data is encrypted and stored securely in the UK, in compliance with NHS data governance policies.
- Access to patient data is restricted to authorised healthcare professionals within the practice.

Patient Rights Under data protection laws, patients have the following rights

- Right to Access: You can request a copy of your consultation records by contacting the practice.
- Right to Rectification: If you believe your records contain inaccuracies, you can request corrections.
- Right to Object: You can object to the use of Heidi Health in your consultation by informing your clinician.
- Right to Restrict Processing: In certain circumstances, you may request limitations on how your data is processed.

Legal Basis

Legal Basis for Processing The legal bases for processing personal data under UK GDPR and the Data Protection Act 2018 include:

- Article 6(1)(e) – Performance of a task carried out in the public interest or in the exercise of official authority.
- Article 9(2)(h) – Processing necessary for the provision of health or social care.

Recipient Or Categories of Recipients of The Shared Data Categories of Data Processed

The following types of personal data may be processed when using Heidi Health:

- Patient identifiers (name, date of birth, NHS number)
- Consultation transcripts (including symptoms, diagnoses, and treatment plans)
- Voice recordings (if applicable)

Retention Period Retention Period

- Transcribed consultation records are stored as part of the patient's electronic medical record and retained in accordance with NHS retention guidelines.
- Any temporary data processed by Heidi Health is securely deleted once incorporated into the medical record. This is set to delete within 1 day. No data is held by Heidi Health.

Opt-Out Option

If you prefer not to have your consultation transcribed by Heidi Health, you can opt out at any time by informing your clinician before or during your appointment.

Access to your personal information

Data Subject Access Requests (DSAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

- Your request should be made to the Practice – for information from the hospital you should write direct to them
- There is no charge to have a copy of the information held about you
- We are required to respond to you within one month
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located information we hold about you at any time.

What should you do if your personal information changes?

You should tell us so that we can update our records please contact the practice reception team as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

Objections / Complaints

Should you have any concerns about how your information is managed at the GP, please contact the GP Practice Manager or the Data Protection Officer as above. If you are still unhappy following a review by the GP practice, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

Information Commissioner:
Wycliffe house
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745
www.informationcommissioner.gov.uk

If you are happy for your data to be extracted and used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact the Practice Data Protection Officer.

If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as below.

Data Protection Officer:

The practice has appointed Barry Jackson to be their Data Protection Officer. This service is provided through a company called N3i. The contact details for the DPO are:

Barry Jackson
Head of Information Governance
Email: N3i.dpo@nhs.net

For queries and urgent responses contact through N3i service desk:
Phone 0300 002 0001

Changes:

It is important to point out that we may amend this Privacy Notice from time to time. If you are dissatisfied with any aspect of our Privacy Notice, please contact the Practice Data Protection Officer.

See also:

Winterton Medical Practice GDPR CCTV Privacy Notice