



Wootton
Medical Centre

WMC Privacy Notice (England):

Document Control:

A. Confidentiality Notice:

This document and the information contained therein is the property of Wootton Medical Centre.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Wootton Medical Centre.

B. Document Details:

Policy:	WMC Privacy Notice (England)
Author & Role:	Sharon Bailey, Practice Manager
Organisation:	Wootton Medical Centre
Document Reference:	PN/SB/2
Current Version Number:	2
Current Document Approved By:	Dr Sarah Moore
Date Approved:	29/06/21

C. Document Revision & Approval History:

Version	Date	Version Created By:	Version Approved By:	Comments
1	01/03/19	S Bailey	Dr S Moore	Review March 2021
2	29/06/21	S Bailey	Dr S Moore	Review June 2023
3	06.11.23	Jude Michie	Lisa Marotta	Minor updates
4	04.03.25	Lisa Marotta	Alina Burada	Anima and Heidi added

1. Introduction:

1.1 Policy statement:

NHS Digital collects information with the purpose of improving health and care for everyone. The information collected is used to:¹

- Run the health service
- Manage epidemics
- Plan for the future
- Research health conditions, diseases and treatments

1.2 Principles:

NHS Digital is a data controller and has a legal duty, in line with the UK General Data Protection Regulation (UK GDPR), to explain why it is using patient data and what data is being used. Similarly, Wootton Medical Centre (WMC) has a duty to advise patients of the purpose of personal data and the methods by which patient personal data will be processed.

1.3 Status:

The surgery aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in respect to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.4 Training & support:

The surgery will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy.

¹ [NHS Digital – How we look after your health and care information](#)

2. Scope:

2.1 Who it applies to:

This document applies to all employees and GP Partners of the surgery and other individuals performing functions in relation to the surgery, such as agency workers, locums and contractors.

2.2 Why & how it applies to them:

Everyone should be aware of the practice privacy notice and be able to advise patients, their relatives and carers what information is collected, how that information may be used and with whom the practice will share that information.

The first principle of data protection is that personal data must be processed fairly and lawfully. Being transparent and providing accessible information to patients about how their personal data is used is a key element of the General Data Protection Regulation.

3. Definition of terms:

3.1 Privacy notice:

A statement that discloses some or all of the ways in which the practice gathers, uses, discloses and manages a patient's data. It fulfils a legal requirement to protect a patient's privacy.

3.2 Data Protection Act 2018 (DPA18)²:

The Data Protection Act (DPA18) will ensure continuity by putting in place the same data protection regime in UK law pre- and post-Brexit.

3.3 Information Commissioner's Office (ICO)³:

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

² [Data Protection Act 2018](#)

³ [ICO](#)

3.4 General Data Protection Regulation (GDPR)⁴:

The GDPR replaced the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way in which organisations across the region approach data privacy. The GDPR came into effect in May 2018.

Post-Brexit, in January 2021, the GDPR became formally known as UK GDPR and was incorporated within the Data Protection Act 2018 (DPA18) at Chapter 2.

3.5 Data controller:

The entity that determines the purpose, conditions and means of the processing of personal data.

3.6 Data subject:

A natural person whose personal data is processed by a controller or processor.

4. Compliance with regulations:

4.1 UK GDPR:

In accordance with the UK GDPR, this practice will ensure that information provided to subjects about how their data is processed will be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge

4.2 Article 5 compliance:

In accordance with Article 5 of the GDPR, the surgery will ensure that any personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject

⁴ [GDPR](#)

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Article 5 also stipulates that the controller shall be responsible for, and be able to demonstrate compliance with, the above.

4.3 Communicating privacy information:

At WMC, the privacy notice is displayed on our website and through signage in the waiting room. We will:

- Inform patients how their data will be used and for what purpose
- Allow patients to opt out of sharing their data, should they wish

4.4 What data will be collected?

At WMC, the following data will be collected:

- Patient details (name, date of birth, NHS number)
- Address and next of kin information
- Medical notes (paper and electronic)
- Details of treatment and care, including medications
- Results of tests (pathology, x-ray etc.)
- Any other pertinent information

4.5 National data opt-out programme:

The national data opt-out programme affords patients the opportunity to make an informed choice about whether they wish their confidential patient information to be used just for their individual care and treatment or also used for research and planning purposes.⁵

⁵ [NHS Digital National data opt-out programme](#)

Patients who wish to opt out of data collection will be able to set their national data opt-out choice online. An alternative provision will be made for those patients who are unable to do so or who do not want to use the online system.

Individuals who have opted out using the existing Type 2 opt-out will be automatically transferred to the new national data opt-out system and will be notified on an individual basis of the change.

4.6 Patients in secure settings

Patients in the detained and secure estate who want to register a national data opt-out need a healthcare professional to fill in a proxy form on their behalf. The following information and guidance on proxy forms details who can complete it and how it should be filled in.

The national data opt-out information is held centrally on the NHS Spine and will not be updated in the SystmOne prison module so you will not see the national data opt-out in the patient's record.

Further reading can be sought from NHS Digital.

The following resources are available to staff at WMC:

- [National Data Guardian for Health and Care – review of data security, consent and opt outs](#)
- [National data opt out – data protection impact assessment](#)
- [National data opt out training](#)
- [Compliance with the national data opt out](#)
- [Guidance for health and care staff](#)
- [Supporting your patients – information and resources](#)
- [Information for GP practices](#)
- [Understanding the national data opt out](#)

Should any queries arise regarding the national data opt-out programme, the Reception Supervisor email the query to the national data opt-out enquiries mailbox - newoptoutenquiries@nhs.net.

4.7 WMC privacy notice:

See Appendix A.

5. Summary:

It is the responsibility of all staff at WMC to ensure that patients understand what information is held about them and how this information may be used. Furthermore, the surgery must adhere to the DPA18 and the GDPR to ensure compliance with extant legal rules and legislative act



Practice Privacy Notice:

Wootton Medical Centre (WMC) has a legal duty to explain how we use any personal information we collect about you, as a registered patient, at the surgery. Staff at the practice maintain records about your health and the treatment you receive in electronic and paper format.

What information do we collect about you?

Information held by this organisation may include the following:

- Your contact details (such as your name, address and email address)
- Details and contact numbers of your next of kin
- Your age range, gender, ethnicity
- Details in relation to your medical history
- The reason for your visit to the organisation
- Any contact the organisation and/or your practice has had with you including appointments (emergency or scheduled), clinic visits, etc.
- Notes and reports about your health, details of diagnosis and consultations with our GPs and other health professionals within the healthcare environment involved in your direct healthcare
- Details about the treatment and care received
- Results of investigations such as laboratory tests, x-rays, etc.
- Relevant information from other health professionals, relatives or those who care for you
- Recordings of telephone conversations between yourself and the organisation

Information collected about you from others

We collect and hold data for the purpose of providing healthcare services to our patients and we will ensure that the information is kept confidential. However, we can disclose personal information if:

- It is required by law
- You provide your consent – either implicitly for the sake of your own care or explicitly for other purposes
- It is justified to be in the public interest

To ensure you receive the best possible care, your records are used to enable the care you receive. Information held about you may be used to help protect the health of the public and to help us to manage the NHS.

A patient can object to their personal information being shared with other healthcare providers but if this limits the treatment that you can receive then the doctor will explain this to you at the time.

How we will use your information:

Your data is collected for the purpose of providing direct patient care; however, we can disclose this information if it is required by law, if you give consent or if it is justified in the public interest. The practice may be requested to support research; however, we will always gain your consent before sharing your information with medical research databases such as the Clinical Practice Research Datalink and QResearch or others when the law allows.

In order to comply with its legal obligations, this practice may send data to NHS Digital when directed by the Secretary of State for Health under the Health and Social Care Act 2012. Additionally, this practice contributes to national clinical audits and will send the data that is required by NHS Digital when the law allows. This may include demographic data, such as date of birth, and information about your health which is recorded in coded form; for example, the clinical code for diabetes or high blood pressure.

Processing your information in this way and obtaining your consent ensures that we comply with Article 6(1)(c), 6(1)(e) and 9(2)(h) of the GDPR.

Maintaining confidentiality & accessing your records:

We are committed to maintaining confidentiality and protecting the information we hold about you. We adhere to the General Data Protection Regulation (GDPR), the NHS Codes of Confidentiality and Security, as well as guidance issued by the Information Commissioner's Office (ICO). You have a right to access the information we hold about you, and if you would like to access this information, you will need to complete a Subject Access Request (SAR). Please ask Reception for a SAR form and you will be given further information. Furthermore, should you identify any inaccuracies, you have a right to have the inaccurate data corrected.

Our organisational policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the UK General Data Protection Regulation (UK GDPR) and all UK specific data protection requirements. Our policy is to ensure all personal data related to our patients will be protected.

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
- Safeguarding matters and investigations
- 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.

Third party processors

To enable us to deliver the best possible services, we will share data (where required) with other NHS bodies such as hospitals. In addition, the organisation 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 include:

- Companies that provide IT services and support, including our core clinical systems, systems that manage patient facing services (such as our website and service accessible through the same), data hosting service providers, systems that facilitate appointment bookings or electronic prescription services and document management services etc.
- Further details regarding specific third-party processors can be supplied on request to the data protection officer as below.

Risk stratification:

Risk stratification is a mechanism used to identify and subsequently manage those patients deemed as being at high risk of requiring urgent or emergency care. Usually this includes patients with long-term conditions, e.g. cancer. Your information is collected by a number of sources, including WMC; this information is processed electronically and given a risk score which is relayed to your GP who can then decide on any necessary actions to ensure you receive the most appropriate care.

Invoice validation:

Your information may be shared if you have received treatment to determine which Clinical Commissioning Group (CCG) is responsible for paying for your treatment. This information may include your name, address and treatment date. All of this information is held securely and confidentially; it will not be used for any other purpose or shared with any third parties.

Opt-outs:

You have a right to object to your information being shared. Should you wish to opt out of data collection, please contact a member of staff who will be able to explain how you can opt out and prevent the sharing of your information; this is done by registering to opt out online (national data opt-out programme) or if you are unable to do so or do not wish to do so online, by speaking to a member of staff.

Primary care networks

The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces that ease the pressure of GPs, leaving them better able to focus on patient care. All areas within England are covered by a PCN.

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 integrate with the wider health and care system more easily.

All GP practices have come together in geographical networks covering populations of approximately 30–50,000 patients to take advantage of additional funding attached to the GP contract. This size is consistent with the size of the primary care homes that exist in many places in the country but are much smaller than most GP federations.

This means that WMC may share your information with other practices within the Primary Care Network to provide you with your care and treatment.

Safeguarding

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

Our legal basis for processing for UK General Data Protection Regulation (UK 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...’

Safeguarding information such as referrals to safeguarding teams is retained by [insert organisation name] when handling a safeguarding concern or incident. We may share information accordingly to ensure a duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e., the mental health team).

Shared care

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems.

You can opt out of this sharing of your records with our partners at any time if this sharing is based on your consent.

Summary care records

During the height of the pandemic changes were made to the Summary Care Record (SCR) to make additional patient information available to all appropriate clinicians when and where they needed it to support direct patient care, leading to improvements in both care and outcomes.

These changes to the SCR will remain in place unless you decide otherwise.

Regardless of your past decisions about your SCR preferences, you will still have the same options that you currently have in place to opt out of having a SCR, including the opportunity to opt back in to having a SCR or opt back in to allow the sharing of additional information.

You can exercise these choices by doing the following:

- Choosing to have a SCR with all information shared. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed SCR, including core and additional information if they need to provide you with direct care.
- Choosing to have a SCR with core information only. This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your SCR if they need to provide you with direct care.
- Choosing to opt-out of having a SCR altogether. This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

Retention periods:

In accordance with the NHS Codes of Practice for Records Management, your healthcare records will be retained for 10 years after death or, if a patient emigrates, for 10 years after the date of emigration.

What to do if you have any questions:

Should you have any questions about our privacy policy or the information we hold about you, you can:

- Contact the practice's data controller via email at wootton.medicalcentre@nhs.net, GP practices are data controllers for the data they hold about their patients⁶

⁶ [BMA GPs as data controllers under the GDPR](#)

- Write to the data controller at Wootton Medical Centre, 36-38 High Street, Wootton, Northampton NN4 6LW

The Data Protection Officer (DPO) for WMC is;

Paul Couldrey

PCDC

NBV Enterprise Centre

6 David Lane

Nottingham

Nottinghamshire

NG6 0JU

0115 838 6770

info@pcdc.org.uk

Complaints:

In the unlikely event that you are unhappy with any element of our data-processing methods, you have the right to lodge a complaint with the ICO. For further details, visit ico.org.uk and select 'raising a concern'.

Changes to our privacy policy:

We regularly review our privacy policy and any updates will be published on our website and on posters to reflect the changes. This policy is to be reviewed June 2025.

Addendums to our Privacy Notice from July 2024

We are working closely with St Andrew's Healthcare to provide outreach services for patients with severe mental health illnesses who require annual physical health checks. Relevant clinical information will be shared for direct patient care.

Addendums to our Privacy Notice from March 2025

Heidi AI

As part of the Digital First National programme of work, GP Practices are required to record accurate data about patient interaction, especially within consultations. To assist with this administrative task, the practice is using a new technology known as Heidi AI.

The primary purposes include improving clinical documentation, aiding healthcare professionals in notetaking, and generating consult summaries. Heidi technology enables clinicians to focus on patients during the consultation, contributing to improved patient care. It also acts as a valuable tool for medical practitioners, saving them hours of administrative time per week.

Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impression

and/or management plans before, during and after the healthcare encounter. The clinician can also add additional contextual notes about the healthcare encounter.

This system is designed to alleviate the administrative burden on healthcare professionals, allowing them to focus more on patient care rather than paperwork. The Heidi Scribe will leverage natural language processing (NLP), speech recognition technology, and machine learning algorithms to understand and interpret complex medical dialogue, identify key health information, and categorise data into the appropriate sections of an Electronic Health Record (EHR).

Your consent will be sought for consultations that are transcribed using the Heidi AI tool. Heidi also uses aggregated de-identified information from these consults to improve its models and outputs, ultimately improving both patient care and clinician experience.

All Data that identifies you stays within the practice and its servers which are UK based, no identifiable data is used by the Heidi tool for machine learning.

Heidi AI will not make decisions about your care, it only transcribes verbal interactions with the practice, with your consent.

More information about the model can be found on the Heidi website here: -

<https://www.heidihealth.com/uk>

Addendums to our Privacy Notice from April 2025

Anima

Anima Privacy Policy

For patients whose GP practice uses Anima to manage and process online consultations, Anima acts as a 'data processor' on behalf of your GP practice. This means that we only process personal data to the extent that is required for your GP practice to provide you with the care that you need. When you submit a request through Anima, your personal data is not shared with any third parties, nor are you subject to any advertising when using Anima.

Some clauses in our privacy policy only apply to users of our website, and this is so we can account for advertising services and cookies that may be present in users' browsers.

Anima is certified to NHS and UK government standards for data security and information governance: all data processed through Anima is secure (encrypted) both in transit (when it is sent) and at rest (when it is received), and all data is stored in the UK. No patient data is shared outside the UK.