



## PRIVACY NOTICE

### INTRODUCTION

Welcome to Whitley House Surgery's privacy notice.

Whitley House Surgery respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data in all circumstances where we collect your personal data. This notice also informs you about your privacy rights and how the law protects you.

### 1. IMPORTANT INFORMATION AND WHO WE ARE

#### PURPOSE OF THIS PRIVACY NOTICE

This privacy notice aims to give you information on how Whitley House Surgery collects and processes your personal data through your interactions with us, whether that be in person, by telephone, by email, mail or through this website.

It is important that you read this privacy notice so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices that we provide and is not intended to override them.

#### CONTROLLER

Whitley House Surgery is the controller and responsible for your personal data (collectively referred to as "Whitley House Surgery", "Practice", "we", "us" or "our" in this privacy notice).

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

#### CONTACT DETAILS

Our full details are:

Name of DPO: Stephen Avila

Email address: [stephen@goodyburrett.co.uk](mailto:stephen@goodyburrett.co.uk)

Postal address: Goody Burrett Solicitors, St Martin's House, 63 West Stockwell Street, Colchester, Essex, CO1 1HE

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues ([www.ico.org.uk](http://www.ico.org.uk)). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

## **CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES**

This version was last updated on 20<sup>th</sup> November 2023.

As a practice we abide by the principles of the UK GDPR (GDPR) as tailored by the Data Protection Act 2018 (the Data Protection Laws").

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during whilst you remain a patient of the Practice, and or during your relationship with us.

## **2. THE DATA WE COLLECT ABOUT YOU**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- Contact Data includes billing address, email address and telephone numbers.
- Financial Data includes bank account and payment card details.
- Health Data includes details relating to your health.
- Transaction Data includes details about payments to and from you and other details of products and, or services you have purchased from us.
- Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- Usage Data includes information about how you use our services and this website.
- Communications Data includes your preferences in receiving practice updates from us and your communication preferences.

We will only use information that may identify you (known also as personal confidential data) in accordance with the Data Protection Laws.

### **3. HOW IS YOUR PERSONAL DATA COLLECTED?**

We use different methods to collect data from and about you including through:

- Direct interactions. You may give us your Identity, Contact, Health and Financial Data by engaging with us regarding your health matters, filling in forms or by corresponding with us by post, phone, email, and telephone or otherwise. This includes personal data you provide when you:
  - Enquire and or register as a patient;
  - request information to be sent to you;
  - give us some feedback.
- Automated technologies or interactions. As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.
- Third parties or publicly available sources. We may receive personal data about you from various third parties, for example another health care professional..

#### **Call Recording**

Please note that this practice records its calls for training and quality purposes.

#### **CCTV**

Please note that this practice uses CCTV.

### **4. HOW WE USE YOUR PERSONAL DATA**

We will only use your personal data when the Data Protection Laws allows us to. Most commonly, we will use your personal data in the following circumstances:

- To provide care services to you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to sending practice updates to you via email or text message. You have the right to withdraw consent to such updates at any time by [Contacting us](#).

## **LAWFUL BASIS FOR WHICH WE WILL USE YOUR PERSONAL DATA**

Your personal data is collected and processed by us to provide care services to you and to comply with our legal obligations.

The following sections of the UK GDPR set out the lawful basis on which we collect and process your personal data:

Article 6(1)(c) – ‘processing is necessary for compliance with a legal obligation to which the controller is subject...’

Article 6(1)(e) ‘...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...’; and

Article 9(2)(h) – ‘processing is necessary for the purpose of preventative...medicine...the provision of health or social care or treatment or the management of health or social care systems and services...’

In addition to the above we may rely on consent to provide the lawful ground for processing your data, where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

We will also respect and comply with their obligations under the common law duty of confidence.

Please [Contact us](#) if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

## **SHARING DATA WITH THIRD PARTIES**

We may share your data with third parties to deliver our services to you. These may include:

### **NHS Digital**

- NHS Digital is a national body which has legal responsibilities to collect information about health and social care services.
- It collects information from across the NHS in England and provides reports on how the NHS is performing. These reports help to plan and improve services to patients.
- This practice must comply with the law and will send data to NHS Digital, for example, when it is told to do so by the Secretary of State for Health or NHS England under the Health and Social Care Act 2012.
- More information about NHS Digital and how it uses information can be found at: <https://digital.nhs.uk/home>.

If you do not want NHS Digital from sharing your identifiable patient data for planning and research purposes you can request that your data is not used in this way. Details on how to do this can be found here: <https://www.nhs.uk/your-nhs-data-matters/>.

### **Care Quality Commission (CQC)**

- The CQC regulates health and social care services to ensure that safe care is provided.
- The law says that we must report certain serious events to the CQC, for example, when patient safety has been put at risk.
- For more information about the CQC see: <http://www.cqc.org.uk/>

### **Integrated Care Boards**

- An integrated care board (or ICB) is a statutory NHS organisation which is responsible for developing a plan for meeting the health needs of the population, managing the NHS budget and arranging for the provision of health services in a geographical area.
- ICBs assist in co ordinating patient care across various health care providers, for example where a patient is subject to a care plan. In such circumstances it will be necessary to share patient data with the ICB.

### **Public Health**

- The law requires us to share data for public health reasons, for example to prevent the spread of infectious diseases or other diseases which threaten the health of the population.
- We will report the relevant information to our local health protection team or Public Health England.

For more information about Public Health England and disease reporting see: <https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report>

### **Third Party Healthcare Staff**

It may be necessary to share your information with third party care providers. For example, local hospitals, out of hours services, diagnostic and treatment centres, and other primary healthcare providers. It is important that staff who are treating you in an emergency know if you have any allergic reactions. This will involve the use of your Summary Care Record.

For more information see: <https://digital.nhs.uk/summary-care-records>.

### **Our Patient CRM Provider**

- SystemOne – owned and managed by The Phoenix Partnership (TPP).

Our Patient messaging service Provider

- PATCHS – Owned and managed by Spectra Analytics Limited.

Practice Staff

- In providing our services to you it will be necessary for your personal data to be shared with Practice staff.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law.

### **PRACTICE UPDATES**

We strive to provide you with choices regarding certain personal data uses relating to Practice updates.

You can ask us or third parties to stop sending you marketing messages at any time by [Contacting us](#) at any time.

### **THIRD-PARTY MARKETING**

Your personal data will never be used for third party marketing purposes.

### **COOKIES**

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see our [cookies policy](#) on our website.

### **THIRD-PARTY LINKS**

Our website may include links to third-party websites and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

## **6. INTERNATIONAL TRANSFERS**

In some instances some of the external third parties that we use as part of the provision of our service are based outside the European Economic Area (EEA) so their processing of your personal data will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see [European Commission: Adequacy of the protection of personal data in non-EU countries](#).
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see [European Commission: Model contracts for the transfer of personal data to third countries](#).
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see [European Commission: EU-US Privacy Shield](#).

Please [Contact us](#) if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

## **7. DATA SECURITY**

We have a legal duty to protect any information we collect from you.

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those members of staff, contractors and other third parties who have a legitimate need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

## **8. DATA RETENTION**

HOW LONG WILL YOU USE MY PERSONAL DATA FOR?

GP medical records will be kept in line with the law and national guidance. Information on how long records are kept can be found at: <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

or speak to the practice.

In some circumstances you can ask us to delete your data: see below for further information.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

## **9. YOUR LEGAL RIGHTS**

Under certain circumstances, you have rights under data protection laws in relation to your personal data. Please click on the links below to find out more about these rights:

**Right to complain.**

You have the right to complain to the Information Commissioner's Office. If you wish to complain follow this link <https://ico.org.uk/global/contact-us/> or call the helpline 0303 123 1113

**Request access to your personal data.**

You have the right to access your medical record, and any other records that we hold containing your personal data. Please speak to a member of staff.

**Request correction of your personal data.**

You have the right to have any errors or mistakes in the personal data that we hold corrected.

**Request erasure of your personal data.**

We are not aware of any circumstances in which you will have the right to restrict our use of your personal data, or delete correct information from your medical record; although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.

**Object to processing of your personal data.**

There are very limited rights to object when the law requires information to be shared but government policy allows some rights of objection as set out below.

**NHS Digital**

- Your information will be shared with NHS Digital for reasons other than your own direct care.
- Since September 1<sup>st</sup> 2021 it is no longer possible to opt out from your data being shared with NHS Digital.
- This means you will not be able to object to your data being shared with NHS Digital when it is legally required under the Health and Social Care Act 2012.
- You can however still register a National Data Opt-out, which will prevent NHS Digital from sharing your identifiable patient data for planning and research purposes as we explain above in section 4 of this policy.

**Public health**

- Legally information must be shared under public health legislation. This means that you are unable to object.

**Care Quality Commission**

- Legally information must be shared when the Care Quality Commission needs it for their regulatory functions. This means that you are unable to object.

**Court order**

- Your information must be shared if it ordered by a court. This means that you are unable to object.

**Right to withdraw consent**

We are not aware of any circumstances in which you will have the right to withdraw consent to our use of your personal data for the provision of primary care services. You are entitled to restrict the methods that we use to communicate with you and the receipt of practice updates from us.,



If you wish to exercise any of the rights set out above or have any questions regarding our Privacy Notice please [Contact us](#).

Updates since last review:

Data sharing with ICB

AccuRx to PATCHS