**PATIENT PRIVACY NOTICE**

**DETAILED VERSION**

**(including Data Protection Impact Assessments - PIAs)**

**Coronavirus (COVID-19) pandemic and your information**

The ICO recognises the unprecedented challenges the NHS and other health professionals are facing during the Coronavirus (COVID-19) pandemic.

The ICO also recognise that 'Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health.' The Government have also taken action in respect of this and on 20th March 2020 the Secretary of State for Health and Social Care issued a Notice under Regulation 3(4) of The Health Service (Control of Patient Information) Regulations 2002 requiring organisations such as GP Practices to use your information to help GP Practices and other healthcare organisations to respond to and deal with the COVID-19 pandemic.

In order to look after your healthcare needs during this difficult time, we may urgently  need to share your personal information, including medical records, with clinical and non clinical staff who belong to organisations that are permitted to use your information and need to use it to help deal with the Covid-19 pandemic. This could (amongst other measures) consist of either treating you or a member of your family and enable us and other healthcare organisations to monitor the disease, assess risk and manage the spread of the disease.

Please be assured that we will only share information and health data that is **necessary** to meet yours and public healthcare needs. The Secretary of State for Health and Social Care has also stated that these measures are temporary and will expire on 30th September 2020 unless a further extension is required. Any further extension will be will be provided in writing and we will communicate the same to you.

Please also note that the data protection and electronic communication laws do not stop us from sending public health messages to you, either by phone, text or email as these messages are not direct marketing.

It may also be necessary, where the latest technology allows us to do so, to use your information and health data to facilitate digital consultations and diagnoses and we will always do this with your security in mind.

If you are concerned about how your information is being used, please contact our DPO using the contact details provided in this Privacy Notice.

**------------------------------------------------------------------------**

Version: 1.4

Created by: Anita Summerfield

Created Date: 4/1/21

Last Review Date: 31/10/23

**Privacy Notice for National COVID-19 and Flu Vaccination Programmes**

NHS England has established a centralised service for the management of both the COVID-19 and seasonal flu vaccination programmes. This service is supported by a central system, the Immunisation Management System.

When you attend for your Covid-19 vaccination a record will be made that you have been vaccinated and when. Normally, vaccinations are undertaken in GP settings. However, the delivery of the Covid-19 vaccine is being undertaken in a variety of care settings.

NHS England is responsible for processing your personal data for the purposes of the national vaccination programme.

To find out more, you can access the NHS England privacy notice at:

<https://www.england.nhs.uk/contact-us/privacy-notice/>

Contents

[Introduction 4](#_Toc60669318)

[What information we hold 4](#_Toc60669319)

[How we collect it 5](#_Toc60669320)

[How it is stored and retention period 5](#_Toc60669321)

[Why do we [and other organisations] need access to your personal data? 6](#_Toc60669322)

[What do we mean by ‘Direct Care’? 7](#_Toc60669323)

[How we share your personal data [our practice default] 7](#_Toc60669324)

[Your choice 9](#_Toc60669325)

[How do we maintain the confidentiality of your records? 10](#_Toc60669326)

[How to access your personal information 10](#_Toc60669327)

[Consent information 11](#_Toc60669328)

[How to object 11](#_Toc60669329)

[Changes in your details 11](#_Toc60669330)

[Registration with the Information Commissioners Office 12](#_Toc60669331)

[Data Protection Impact Assessment (PIA) 12](#_Toc60669332)

[Who is the Data Controller? 12](#_Toc60669333)

[Legal basis for holding and processing personal data 12](#_Toc60669334)

[Data Subjects rights 13](#_Toc60669335)

[Complaints/concerns/queries 14](#_Toc60669336)

[Further information is available from: 14](#_Toc60669337)

[Appendix 1 15](#_Toc60669338)

[INFORMATION FLOWS – details about each flow 15](#_Toc60669339)

[Appendix 2 23](#_Toc60669340)

[Completed Data Protection Impact Assessments (PIA) 23](#_Toc60669341)

[Appendix 3 25](#_Toc60669342)

[Individual companies we use – Privacy Notices and/or information: 25](#_Toc60669343)

# Introduction

The new General Data Protection Regulation (GDPR) requires the Practice to ensure that our patients are aware of what personal data we hold on them, how we collect that data, how it is stored and with whom it is shared.

Therefore this fair processing notice explains why Rooley Lane Medical Centre collects information about you and how that information may be used.

All health care professionals who provide you with Direct 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.

Please see the list below of information that we hold on you, how it is collected, how it is stored and why we may share it. Please note that throughout the documentation patients are referred to as ‘Data Subjects’.

# What information we hold

As your registered GP practice we hold your health record. This contains sensitive information about you, your health and your wellbeing. The following list provides an example of the type of information (both past and present) that can be held within your record:

**Group 1 (basic information)**

* Details about you e.g. your name, date of birth, address, marital status, contact telephone numbers, your next of kin and/or carer information (if applicable) and a contact number for them, an email address.

**Group 2 (information regarding your health)**

* Any contact you have had with the surgery; such as appointments, home visits, telephone consultations, etc.
* Notes and reports about your health
* Details about your treatment and care
* Results of investigations such as laboratory tests, x-rays etc
* Referral information
* Prescription information
* Past medical history
* New patient registration information including family history

**Group 3 (3rd party clinical information which is held electronically)**

* Relevant information from other health professionals. For example if you are seen by a clinical 3rd party e.g community staff (District Nurses, Physiotherapist, Midwives, Health Visitors etc). This information will also be added to your electronic clinical record (unless you decline consent to share this information).
* When you are seen at a hospital this information is also added to your clinical record electronically by the letter being received at the practice and scanned into your clinical record.
* Relevant information from relatives or those who care for you

**Group 4 (3rd party non-clinical ad-hoc information)**

Any other ad-hoc information which has been received at the practice will also be entered into your clinical record e.g.

* Insurance and/or solicitor information
* Letters from a patient to the practice
* Research and/or trial information
* Coroners reports
* Recorded telephone calls
* CCTV images

**Group 5 (paper Medical Record Envelope - MRE)**

* Prior to electronic records all health records where held in paper format. So information prior to 2003 will be held in your paper MRE.

# How we collect it

**Group 1:**

The information in this group will be collected when you registered at the Practice and/or when changes occur in your circumstances and you inform us of these changes.

**Group 2:**

The information in this group will have been collected when you registered at the Practice and from your previous medical history/patient records. The information will also be added to and/or updated each time you have contact with the practice, information regarding a referral request, investigations/examinations carried out, prescription requests/received etc.

**Group 3:**

The information in this group will have been collected and/or updated from other external health care professionals e.g. each time you are seen at the hospital, or by a member of the community teams such as District Nurses, Physiotherapists etc.

**Group 4:**

The information in this group will have been collected when you have made contact with the practice e.g. in the form of a letter sent in to us, or if you have instructed a 3rd party to act on your behalf e.g. a solicitor or insurance company etc. If you have instructed a Solicitor, Insurance Company or Research Company to act on your behalf we would never release any information about you without your explicit written consent.

Depending on the circumstances when a patient dies the clinicians may have to complete a report on certain deaths.

For monitoring and/or training purposes we recorded all incoming calls to the practice.

For security and the health and safety of all stakeholders (patients/staff/guests etc) we also have CCTV in and around the building in public areas.

**Group 5:**

The information in this group will have been collected from any of the 4 groups above and this information would have been gathered prior to 2003 so would have been in a paper format. This information will be stored in your paper MRE.

# How it is stored and retention period

**Storage:**

All 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.

**Retention Period:**

The Data Protection Act 2018 – Retaining personal data (Principle 5) - does not set out any specific minimum or maximum periods for retaining personal data. Instead the extract below is from the Information Commissioners Office website and says that:

*Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*

*This is the fifth data protection principle. In practice, it means that you will need to:*

* *review the length of time you keep personal data;*
* *consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;*
* *securely delete information that is no longer needed for this purpose or these purposes; and*
* *update, archive or securely delete information if it goes out of date.*

Although other factors need to be considered as follows:

*Personal Data will need to be retained for longer in some cases than in others. How long you retain different categories of personal data should be based on individual business needs. A judgement must be made about:*

* *the current and future value of the information;*
* *the costs, risks and liabilities associated with retaining the information; and*
* *the ease or difficulty of making sure it remains accurate and up to date.*

*At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful where many records of the same type are held.*

*However, there is a significant difference between permanently deleting a record and archiving it. If a record is archived or stored offline, this should reduce its availability and the risk of misuse or mistake. However, you should only archive a record (rather than delete it) if you still need to hold it. You must be prepared to give subject access to it, and to comply with the data protection principles. If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on that system.*

*The word ‘deletion’ can mean different things in relation to electronic data.*

Please click on the following link for more information on this:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/>

# Why do we [and other organisations] need access to your personal data?

This information means we can provide you with high quality direct care in a safe and effective manner. Being able to see your detailed record allows for an overall picture of your health and wellbeing to be assessed. This then helps us to diagnose and prescribe appropriate courses of treatment to you. This means that the most safe and efficient care is provided to you. We do not want you to have to repeat your medical history and remember every detail, which may or may not be relevant, to every health professional involved in your care. Lack of access to your information may lead to misdiagnosis, inappropriate prescribing of medication or tests and/or ineffective treatment.

We recognise that you will benefit from other health providers that care for you (either currently or in the future) having access to your electronic health record. This is because they can then make fully informed decisions about the care you require. The reasons for access to the detailed record, mentioned above, apply across the health profession. A shared record ensures that care providers always have the most accurate, up to date information.

In a case where patient data is required for research purposes, we do not provide patient identifiable information. Any data we provide is anonymised or pseudonymised, unless you have given explicit consent.

Anonymised data, is data about you but from which you cannot be personally identified. Anonymised data is any personal data which has been processed so that all identifiers (such as name or NHS number) are removed, minimising the likelihood that the data will identify individuals.

Pseudonymised data is any personal data which has been processed so that all identifiers such as name, address, date of birth and NHS number is removed and replaced with a code which makes it anonymous to those who should not see your identifiable data, but would allow others such as those responsible for providing care to identify an individual.

Personal identifiable data, is data which relates to a living individual who:

* can be identified either from that data; or
* from that data in conjunction with other information within the possession of the data controller

# What do we mean by ‘Direct Care’?

The term ‘Direct Care’ means a clinical health activity concerned with the prevention and investigation and treatment of illness. It includes supporting your ability to function and improve your participation in life and society. It also includes the assurance of safe and high quality care and treatment undertaken by one or more registered and regulated health professionals and their team with whom you have a legitimate relationship for your care purposes.

It does not include access to information for purposes such as insurance, advertising or marketing.

# How we share your personal data [our practice default]

As your GP practice we have set the following practice settings for all our registered patients whose detailed electronic health record is in our possession and within the clinical computer system, SystmOne. However, we recognise that each of our patients have differing health care needs and you may wish to control yourself how your personal data is shared. This can be done via ‘**Your Choice**’ stated below.

1. **Implied consent to make your record available to all organisations (without verification/security process) for direct care purposes**

We assume that you are happy to share your detailed electronic health record to those that care for you. We therefore, make your record available to all NHS commissioned services using the clinical record computer system, SystmOne. This allows for anyone at these organisations who have the appropriate controls to retrieve your electronic record once you are registered for care. However, these individuals should only legitimately access your record to provide you with care services. They must also record your permission to view your record.

**AND/OR**

1. **Explicit consent to make your record available to all organisations (without verification/security code process) for direct care purposes**

We will obtain your explicit consent (permission) to share your detailed electronic health record to those that care for you. By providing your permission, we make your record available to all NHS commissioned services using the clinical record computer system, SystmOne. This allows for anyone at these organisations who have the appropriate controls to retrieve your electronic record, once you are registered for care. However, these individuals should only legitimately access your record to provide you with care services. They must also record your permission to view your record.

Your individual sharing preference will overwrite our organisation’s default sharing setting.

**Example of services who might need to view your record**

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations. These are mainly organisations that will be involved in your direct care and therefore need access to your health record:

* All GP practices
* Referral triage and Out of Hours call centres (services determining which organisations should care for you)
* Child Health
* Urgent Care (for example A&E, Minor Injury Units and Out of Hours services)
* Palliative Care
* Prisons and custody suites or offender health
* Substance misuse service
* All NHS hospitals – acute and community
* Bradford Teaching Hospitals Foundation Trust
* Bradford District Care Trust services
* NHS Mental Health Services
* Community pharmacies
* Police & Judicial Services
* CQC – Care Quality Commission
* Health and Social Care Information Centre (HSCIC)
* Social Care Services
* Independent Contractors such as dentists, opticians, pharmacists, coroners
* Ambulance Trusts
* Voluntary Sector Providers working with or for the NHS, providing services such as social prescribing, local support groups, health education, advice services, etc.
* Private Sector Providers working with or for the NHS, such as dentists, pharmacies, opticians and care homes.
* Other ‘data processors’ which you will be informed of

You will be informed who your data will be shared with and in most cases asked for explicit consent for this to happen when this is required. The only time this would not happen is in regards to life or death situations etc as mentioned above. Under the header - ‘How do we maintain the confidentially of your records’.

In the future we may also use external companies to process personal information, such as for archiving purposes. These companies will be bound by contractual agreements to ensure information is kept confidential and secure.

The full list of organisations can be seen and updated in your patient online record.

*To find out more about these types of organisations please go to the following webpage:* [*https://tpp-uk.com/products/*](https://tpp-uk.com/products/) *or talk to a member of your GP practice.*

# Your choice

Youmay not agree with the health and social care organisations we have chosen to have access to your detailed electronic health record (the practice default). You can therefore control this yourself. **Your choice will override our settings**. You have the following options:

* **No organisations require you to provide a security code (Allowed List)** - You can give your permission to allow all NHS commissioned services and local authorities providing health services, using the clinical record computer system, SystmOne, to access your record. This allows for any individual at these organisations (who have the appropriate access controls) to retrieve your electronic record, only after you are registered with them for care. These individuals should only legitimately access your record to provide you with care services and they should always request and gain your consent before doing so.
* **All organisations require you to provide a security code (Verification List)** - You can require that all health organisations must ask you for a PIN number on your first visit to that service. This allows you to verify/confirm that each individual organisation should have access to your record, as they are legitimately involved in your care. You will require access to either a mobile phone or email account, as a PIN will be sent to you. Alternatively, you will need access to SystmOnline to accept or reject a share request sent to your account by the organisation wishing to view your record. *Please contact your GP if you are not enabled for SystmOnline.*
* **Custom lists** - You can put together your own custom lists for access, adding organisations to each of 3 lists i.e. does not require a security code (allowed list), requires a security code (verification list) and cannot access (prohibited list). The functionality for each list will act as described above, but it is you who can determine the level of access, which applies to them. This should be done in conjunction with your GP to ensure you understand the full implications of your decisions.
* **Dissent/Refusal of your permission** - You can refuse your permission for your record to become available to all NHS commissioned services and local authorities providing health services, using the clinical record computer system, SystmOne, which prevents us sharing your clinical record to any other organisation involved in your care. *Please carefully consider the benefits of sharing your record before choosing this option.*
* **Marking items as private** – If you have had a consultation about a particularly sensitive matter, you can ask for this section of your record to be marked as private. That way, even if you consent for another service to see your record, that consultation will not be shown outside the organisation that recorded it.

**You can make changes to the above\* at any time by contacting us or by logging onto your SystmOnline account**. (\*you cannot add an organisation to the prohibited list yourself, you must speak with your GP first if you wish to do this.)

**Available audits**

Audits are useful for your understanding about the types of organisation and individual(s) who are viewing your record. They allow you to raise any concerns about potential illegitimate or unnecessary access of your personal data with the relevant person or organisation. The ability to audit record access is a significant benefit of electronic records over paper records as it allows for a visible trail to be available to you in the following ways:

* **Alerts** - You can opt to receive an alert via SMS or email every time an individual at any health and social care organisation attempts to record your consent to view your record. This means that you can be confident that the appropriate people are viewing your record and you can raise concerns with any organisation where you feel this is not the case.
* **SystmOnline Record Audit** – You can view which organisations have accessed your electronic health record within SystmOnline. Ability to access this audit in SystmOnline is controlled by your GP. Any concerns about access can be raised with the relevant organisation.
* **Record Sharing List** – You can ask your GP practice to show you a list of all health and social care organisations currently caring for you and whether they have recorded your consent or dissent to view your record. If you disagree with the consent options recorded then you, or your GP, should contact those organisations and ask them to amend the setting.

# 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:

• GDPR

• 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. All Rooley Lane Medical Centre staff sign a confidentiality agreement at the start of their employment. They then carryout annual mandatory Information Governance training, which includes all aspects of confidentiality, Data Protection, keeping information secure etc.

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 new 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. They should be supported by the policies of their employers, regulators and professional bodies.

# How to access your personal information

You have a right under the GDPR 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. In order to request this, you need to do the following:

• Your request must be made in writing to the Practice – for information from the hospital you should write directly to them

• We are required to respond to you within 30 days

• 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

# Consent information

When asking for your consent to process your information we will follow the following points:-

* Consent will always be obtained if it is the most appropriate lawful basis for processing your information.
* The request for consent will be prominent and separate from our terms and conditions.
* We will ask you to positively opt in, this means we will not uses pre-ticked boxes or any other type of consent by default.
* We will always use clear, plain language that is easy to understand. If you are uncertain of what anything means, please ask for an explanation prior to signing your consent.
* We will always specify why we want the data and what we’re going to do with it.
* We give granular options to consent to independent processing operations e.g it will be specific for each processing operation, not vague or blanket consent.
* We will name our organisation and any third parties involved as part of the consent form.
* You have the right to withdraw your consent at any time; this will be included on the consent form.
* You have the right to refuse consent without detriment.
* We do not make consent a precondition of a service if appropriate.
* We offer online services directly to children this will include age-verification and parental consent measures are in place. Once a child becomes 11 years old the parental consent will be withdrawn (in line with NHS England guidance) and a Gillick Competency test will be carried out on the child. The 'Gillick Test' helps clinicians to identify children aged under 16 who have the legal capacity to consent to medical examination and treatment. They must be able to demonstrate sufficient maturity and intelligence to understand the nature and implications of the proposed treatment, including the risks and alternative courses of actions.
* We will record how and when we gained your consent and exactly what you were told at the time.
* We will regularly review consents to check that the relationship, the processing and the purposes have not changed.
* We will refresh consents as appropriate e.g. when changes occur this will include parental consent.
* Any withdrawals of consent will be acted on as soon as we can.

# How to object

Should you have any concerns about how your information is managed at the Practice, please contact the Practice Manager. If you are still unhappy following a review by the Practice, you can then complain to the Information Commissioners Office (ICO) via their website (www.ico.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.

# Changes in your details

It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

# Registration with the Information Commissioners Office

The GDPR requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information.

This information is publicly available on the Information Commissioners Office website www.ico.org.uk

The practice is registered with the Information Commissioners Office (ICO).

# Data Protection Impact Assessment (PIA)

To assess the risk to the data subject all information flow at Rooley Lane Medical Centre will have had a Data Protection Impact Assessment (PIA) carried out and a completed Risk Template to determine the risk. From this we will then make changes as appropriate to mitigate the risk. Each PIA and Risk template carried out will be shown with the associated heading in this Privacy Notice.

# Who is the Data Controller?

The Data Controller is: Rooley Lane Medical Centre

The Data Protection Officer: can be contacted via the Practice Manager Anita Summerfield (tel 01274 223118)

# Legal basis for holding and processing personal data

All Healthcare providers hold data subject information under a duty of confidence and all NHS staff are bound by confidentiality rules. Healthcare providers generally operate on the basis of implied consent to use data subjects’ information for the purpose of Direct Care, without breaching confidentiality. Therefore consent for direct care is industry practice in that context. Due to the changes in the law in regards to GDPR this type of assumed implied consent is not appropriate as a clear affirmative to qualify as explicit consent for special category data. Therefore we have to identify another lawful basis e.g. Article 9 (2) (h) below.

Under GDPR, GP Practices have to establish both a lawful basis and a special category condition to process special category data. The information below is an extract from the Information Commissioners Office Website. Please click on the link below for more information.

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)

*The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:*

*(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.*

*(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.*

*(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).*

*(d) Vital interests: the processing is necessary to protect someone’s life.*

*(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.*

*(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)*

Due to the nature of the data we hold e.g. special category data; we also have to comply with the conditions for processing special category data Article 9 (2) of the GDPR. The information below is an extract from the Information Commissioners Office Website and lists the articles that are applicable to GP practices. Please click on the link below for more information on all the articles.

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)

*(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;*

*(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*

*(e) processing relates to personal data which are manifestly made public by    the data subject;*

*(f)  processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

*(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 and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

*(i)  processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

# Data Subjects rights

You (the patient) are the data subject in this context.

Under GDPR Data Subjects (Patients) have the following rights:

* **The Right to Data Portability**

This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the ‘midata’ and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

* **Right of Erasure**

The right to erasure is also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing. *GP practices and other healthcare providers are EXEMPT form this.*

* **Right of Rectification**

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

* **Right of Access**

Under the General Data Protection Regulation (GDPR), individuals will have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information. These are similar to existing subject access rights under the DPA. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

* **Right to Restrict Processing**

Under the DPA, individuals have a right to ‘block’ or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

* **Right to be Informed**

The right to be informed encompasses your obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

* **Right to Object**

Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

* **Rights Related to Automated Decision Making and Profiling**

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Information regarding each of these rights can be found on the Information Commissioners website or by clicking on the link below:

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

# Complaints/concerns/queries

Whilst you are registered at Rooley Lane Medical Centre, we are only the gatekeeper of YOUR health record. If you have any complaints, concerns or queries about any aspect of how your personal data is collected, held, stored or who it is shared with you have the right to discuss this with us. You also have the right to change your mind at any time to anything that you have consented to or not consented to. Please speak to the Practice Manager if you have any concerns, questions or complaints about any aspect of this Patient Privacy Notice.

If you are still unhappy following a review by the Practice you can then complain to the Information Commissioners Office (ICO). [**https://ico.org.uk/make-a-complaint/**](https://ico.org.uk/make-a-complaint/), telephone: 0303 123 1113 (local rate)

# Further information is available from:

[www.tpp-uk.com](http://www.tpp-uk.com)

[www.ico.org.uk](http://www.ico.org.uk)

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance>

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>

# Appendix 1

## INFORMATION FLOWS – details about each flow

**Referral process**

The practice is frequently required to share data subjects’ personal data – more specifically, personal details and healthcare records between organisations e.g. sharing of data between Rooley Lane Medical Centre and one of the NHS hospitals or Private Clinics. These could be in the West Yorkshire area or further afield depending on the patients choice. This is a requirement to ensure that data subjects receive the necessary care and treatment appropriate with their clinical condition(s). The options for the referral will always be discussed between the Clinician and the Data Subject. The Data Subject will then give consent (if appropriate) as stated above – sharing in-out. If the share is agreed this end the ‘referred to’ organisation would still ask the data subject for consent to access the Data Subjects health record.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI01)

**Patient Call Board**

The Practice has an electronic patient call board in the waiting room which is used to call patients into the consulting room. This is used to save time for the clinicians so that they can call you instantly. The information shown on the screen includes your name and which clinician you are seeing. If you have any objection to this information being shown on the screen, please inform the receptionist at the point of booking the appointment so that a note can be added to your appointment.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI02)

**Recording telephone calls**

For monitoring and training purposes our phone system records all phone calls made into the practice and this information is kept on a standalone PC which has no internet connection. The information is kept for 6 months and is then overwritten with newer information so it is a constant 6 month cycle. If you do not want this information recorded we do have a phone in the main office which does not record calls so please ask the receptionist to transfer your call to this phone.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI03)

**Recording CCTV images/external hard drive**

For safety and security purposes we have a number of cameras in and around the Practice. All information is recorded and stored in real time. This information is on a 30 day cycle so it is constantly being overwritten with newer images. These images are never looked at unless we have an incident e.g. a theft etc. If there is a need to look at any of the images, this will only be carried out by a member of the Management team. If necessary the image from the time of the incident may be stored on an external drive, the images would then always be deleted as soon as they are no longer needed.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI04)

**Consented information**

You may have consented to information being shared about you e.g. you have signed up to one of the following services:-

* Online services
  + Systm online – this is where you have access to your electronic clinical record which includes ordering your prescriptions electronically, booking appointments electronically and accessing your coded clinical record (e.g. long term health conditions). This information is accessed by you registering for this service; you are then given a username and password. It is then YOUR responsibility who you allow to access this information. The practice would always encourage you to not allow anybody else to have access to this information as it is confidential to you, although it is ultimately your choice if you choose to share this access with anybody else.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI05)

* + SMS – this is where you agree to receive a text messaging service from the practice e.g. receiving confirmation of booked appointment, a reminder service for booked appointments. Any ad-hoc relevant messages that the practice may send you e.g. flu injections. You have to complete a consent form to sign up to this service.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI07)

* + Email address – you can sign up to receive the Practice Newsletter electronically. If patents would like to receive the newsletter electronically they can do so by completing an explicit consent form. By signing this form you can specify what you are giving consent to receive e.g. just the practice newsletter or the practice newsletter and anything else relevant to the practice. This would include practice events, new services, information regarding surveys or requests from the practice for patient views on different aspects of the services we provide. PPG and PHC members have also agreed and signed a consent form to state that they are happy to receive emails regarding events and minutes etc.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI20)

* Repeat dispensing and/or Electronic Transfer of Prescriptions (ETP) - again this is what you would have signed a consent/nomination form for. By signing the form you are agreeing that the practice can send your prescriptions electronically to the Pharmacy of your choice (nomination). You have the right to change your nominated Pharmacy at any time and it should always be your choice of preferred Pharmacies. If you do want to change your nominated Pharmacy you need to sign a form with the new Pharmacy of your choice. It does not get changed by the Practice.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI06)

* Summary Care Record (SCR) – this was introduced a number of years ago. Prior to it being introduced nationally, it was heavily publicised so that all patients where made aware that they had the option to opt-out of there SCR being shared. If you have a SCR this can provide those involved in your care with faster secure access to key information about your health from your GP record. This means if you happen to be seen anywhere else in the country the person providing the care is able to access your basic care record which includes your name, a summary of your health, any allergies you may have and your acute and current medication. The reason for this information being shared is so that the person treating you is then able to make a thorough assessment of your health needs with the knowledge of your past medical history. Since this was introduced all new patients now have the option to opt-in or opt-out of this at the point of registration.

Enriched Summary Care Record (eSCR) – this is a more detailed SCR, it includes all the information listed above but can include other information which you consent to being included. The reason for this is so that the person providing the care to you has all the relevant history about you not just the items listed above. The only way this information can be added to your SCR is by you having a discussion with a member of the clinical team and you giving your explicit consent to the relevant information being added to your basic SCR.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI08)

* Sharing in-out with other clinical teams – Following the Information Commissioners Office requirements and our Clinical Commissioning Group recommendations our practice has set the following default setting for all our registered patients whose detailed electronic health (and where applicable social care) record is in our possession and within the clinical computer system, SystmOne.
  + Implied Consent to make your record available to all organisations (without verification/security process) for direct care purposes.

And/Or

* + Explicit consent to make your record available to all organisations (without verification/security code process) for direct care purposes.

If the record is shareable, the clinical details will only be viewable by clinical teams who are treating the Data subject and only once they have asked the Data subject for permission to access the clinical record.

Data subjects also have the right to make any part of their record private e.g. not shareable. All accesses are recorded and auditable.

More information regarding Choice can be found on Page 7 above.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI09)

**Ways we receive mail**

Electronically

Every day the practice will receive electronic mail regarding patients. This is sent to us electronically via a secure email account. The mail is then imported into our clinical system and deleted from the email account.

Some mail is also imported directly into our clinical system e.g. as discussed above in regards to sharing in and out.

Internal mail

Hospital letters – we have a van man who works on behalf of the hospital trust who brings us our internal mail from the local hospitals. He also takes our samples with him back to the relevant laboratories to be tested.

Internal mail from Primary Care Support England (PSCE) – this is the body that transports, collects and stores the medical records for all movements from one GP practice to another. They also store the records for deceased patients and patients who have moved abroad (although these records are only kept for a certain number of years). Below is a description of what occurs when a patient registers or moves away from the practice.

* When you register you will complete some documentation, we will then add you onto our clinical system. Your information will be sent to the clinical server at PCSE, they will then request your previous medical records from your previous practice.
* Once your previous practice receive the request to send on your medical notes these will be collected by City Sprint (who work on behalf of PCSE). They will then be taken to PCSE who will then arrange for the records to be sent on to us – again via City Sprint.
* When a patient is added or removed from a Practice the electronic patient record will be sent automatically via GP2GP if the two computer systems are compatible with each other. This means your electronic patient record is with your new practice straight away instead of waiting for your paper records to be delivered. For non-compatible computer systems we will upload all your clinical record onto an encrypted disk which is password protected and this will be sent with your paper records to your new GP practice. The new practice will then need to request the password from Rooley Lane Medical Centre once they have received your paper records.

PCSE – also record information on certain areas of your health care e.g. when a smear test was carried out or when children have vaccinations etc. This information is relevant to keep your information up-to-date and to allow for patients to be added to the appropriate recalls so that you are sent letters when you are due tests/vaccinations etc. This information can be accessed via the Practice and we keep this up-to-date although these letters are not sent via the Practice.

External mail

Royal mail – we may receive mail regarding patients in the Royal Mail. This includes any mail that patients have sent to us e.g. prescription requests etc. We may also receive mail from other NHS organisations or Health care organisations that do not have an internal method of sending mail to us.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI10)

**Payments and invoicing for Enhanced Services carried out at the Practice**

Certain elements of the services we provide are classed as enhanced services and are paid for on a cost per patient basis. This means your information may be shared if you have received treatment, to determine which Clinical Commissioning Group (CCG) is responsible for paying for you treatment. This information may include any of the following: your name, address, NHS number 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 3rd parties.

As a practice we also purchase and provide certain injections that are then administered to patients. For some of the injections we then have to send a prescription (which will include the patients name and address) to the Prescription Pricing Authority. This has to be sent via external mail so it is always sent by a secure method e.g. recorded delivery.

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

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI11)

*Please* [*click here*](#_Individual_companies_we) *to find the Prescription Pricing Authority information under Business Standards in appendix 3*

**Mail sent out by the Practice**

Royal Mail

Sometimes we have to send mail out to patients e.g. if we are unable to contact patients via the telephone. If we are unsure of an address we would normally send out a registration questionnaire to an address that does not include any patient identifiable information. The reason for sending this out is so that we can be sure that we have correct address information for our patients. Ultimately it is the patients’ responsibility to keep us informed of where they are living so that no mail is sent out to an incorrect address.

DocMail

We often have to send out recall letters to patients who are due reviews, injections etc. This type of letter would often be sent via a 3rd Party company that we use called DocMail. The only information they are sent is your name, address and the body of the letter. They have no access to any other parts of your medical record. They have strict guidelines that they have to follow in regards to your confidentiality and have to comply with GDPR also. They only hold the information from the data we send for a maximum of 28 days, therefore all information is permanently deleted from their system within 28 days of us sending it.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI12)

*Please* [*click here*](#_Individual_companies_we) *to find DocMail Privacy Notice in appendix 3*

**Meetings and minutes**

Patients can sometimes be discussed at practice meetings. As a practice we have to minute every meeting so this may include patient information. If this occurs the information will only include the patients NHS number, the minutes are then only available to relevant staff members. Minutes are only kept for a certain amount of time and then destroyed in our confidential waste. This could also include complaints raised by a patient or on behalf of a patient.

Patients attending meetings – we have a Patient Participation Group and Practice Health Champions, both group members attend meetings at the practice. The minutes from the meetings have to be made available on our Practice Website so the minutes will only include the patients Initials – this is always agreed with the patient when joining the groups. The groups can also work in our practice waiting room on behalf of the practice e.g. informing patients how to use the Ipad, assisting with completing patient surveys, forms etc. This work could involve gaining patients personal information, prior to any of the groups helping with this sort of work a DBS check is carried out on the group member and they also read, agree and sign our confidentially agreements.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI13)

**Medicine Management**

To assist with the clinical workload and to relieve work pressure on GPs to allow them to spend more time with patients with complex medical needs, the Practice have employed two pharmacists from a 3rd Party organisation called Prescribing Support Service (PSS).

Having a pharmacist as part of the clinical team within a practice can free up significant GP time as they can manage prescribing, which includes reviewing medicines, reconciliation of letters and discharge forms, addressing patient compliance and managing repeat prescribing systems.

Key activities the Pharmacist will carry out:-

* Managing repeat prescribing
* Medication reviews
* Processing hospital discharge summaries and letters
* Responding to acute prescription requests
* De-prescribing of unused and unnecessary items
* Complex polypharmacy reviews
* Complex chronic disease reviews
* Medication queries from clinicians, practice team, patients
* GP registrar/medical student education

The company - Prescribing Support Service (PSS) - are bound by contractual agreements to ensure your information is kept confidential and secure. All staff members will also read, agree and sign our Practice Confidentiality agreement.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI15)

*Please* [*click here*](#_Individual_companies_we) *to find PSS Privacy Notice in appendix 3*

**Research**

From time to time the practice may be involved in certain research groups if we feel that it would benefit our patients or the NHS. If we do participate in this it will be either anonymised data e.g. statistical information being passed on to the research company or it may be patient involvement. If it is patient involvement the research company may want to invite patients who have certain conditions to participate in a trial and/or research. This will happen by us running a search to identify the patients; all patients will receive a letter explaining about the research and asked if they would like to take part in the research/trial. If they do they will then have the option to send the consent form to the research company. At no point prior to the patient consenting to participate in the research, will the company have any patient identifiable information. All staff involved in the research will be bound by strict confidential guidelines to make sure that your confidential information is kept secure.

The following link takes you to the NHS Health Research Authority website which gives you information on how your information is processed by the research company. <https://www.hra.nhs.uk/about-us/governance/>

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI16)

**Destruction – confidential waste**

Rooley Lane Medical Centre takes the destruction of confidential waste very seriously. All staff are aware of the importance of confidentiality and complete annual training in this area. To assist with the destruction of confidential waste we have employed a specialist company to destruct our confidential waste.

All confidential waste is placed into a locked console (only the Practice Manager has the key). This is then collected and destroyed on our Practice site by a specialised Shredding Company (Shred-It) every 4 weeks. This company is also bound by contractual agreements to ensure confidentiality of all information that is being destroyed, please see Shred-Its Privacy Notice below for more information regarding the security measures they have in place to safely destroy our confidential waste.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI17)

*Please* [*click here*](#_Individual_companies_we) *to find Shred-It Privacy Notice in appendix 3*

**Photocopier and Scanners**

The practice uses different office equipment, which is used to process data subject information as follows:-

Photocopier – this has a hard drive but this is not used/accessed for what we use the machine for e.g. just to photocopy documents. The hard drive is there for using the machine to its full capacity e.g. it can be used for storing fax numbers, email addresses, linking up to PCs etc. We have no intention of using the machine this way, so no information is stored. This machine is not linked up to the internet either so there is no way that anyone could gain unauthorised access to the photocopier.

Scanners – data subject information can be scanned on the scanners and then the information is directly stored straight into our computer system. Therefore no data subject information is stored on the scanners.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI18)

**Clinical Machinery**

We have a number of clinical machinery that is used in Practice as follows:

1. Finger Pulse Oximeter – this is transmitted live to a device as a totally anonymous reading. It is then emailed to a secure NHS email account so that it can be printed off. The Data subjects name is then handwritten on the printout and scanned into the data subject’s clinical record. The email is then deleted straight away. The Finger Pulse Oximeter does keep the ECGs but it is entirely anonymous e.g. just a reading no other data is stored.
2. Electronic weighing scales – no mechanism to store any data
3. Electronic waiting room Blood Pressure Machine – this machine prints out the data subjects BP reading and pulse, but it is only the reading no other data is added. This machine has no facility to store the data at all.
4. Hand held Blood pressure machines that we loan out – these machines have no facility to store any data.
5. Spirometry – this machine is linked directly to our computer system so the data is directly imported into the computer system. Therefore no data is held on the Spirometer.
6. DCA Machine (Diabetes Testing Machine) – this machine produces a reading to determine if a patient is diabetic, but no data is stored on the machine.
7. 24 hour Blood Pressure – this machine is linked to a ‘cloud’ (a means of storing and accessing data and programs over the internet) through a company called Technomed. So no data subjects information is held on the machine itself. Instead the information is stored in the ‘cloud’; this is then linked directly onto our computer system. Please see below for more information.
8. ECG – data subject information is added to a docking station (this is an electronic device), this is then linked to the ‘cloud’ and then imported into the data subject computer record. The information is then immediately deleted from the docking station so it is not stored on the machine.

The machinery listed in 1-6 does not hold, store or retrieve any data subject information so they do not require a PIA completing.

Items 7-8 use a ‘cloud’ to store information so that it can then be accessed and imported into our Clinical System. We use a CCG recommend company called Technomed for this service.

Please [click here](#_Completed_Data_Protection) to find the completed PIA and Risk template in appendix 2 (PI19)

*Please* [*click here*](#_Individual_companies_we) *to find Technomed Privacy Notice and web link in appendix 3*

**Practice Website – Data Collection & Cookies Policy**

We employ a 3rd party company to hold and maintain our Practice Website called My Surgery Website. For the website to function correctly it uses cookies. You can delete cookies at any time. Information regarding cookies and what to do to delete them can be found at the bottom of the home page on our Practice website [www.rooleylanemedicalcentre.co.uk](http://www.rooleylanemedicalcentre.co.uk)

You can also view the 3rd party companies Privacy Notice and other information on our Practice Website this will include Data Collection, storage etc.

*Please* [*click here*](#_Individual_companies_we) *to find My Surgery website Privacy Notice in appendix 3*

# Appendix 2

## Completed Data Protection Impact Assessments (PIA)

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref No** | **Name** | **Impact Assessment** | **Risk Template** |
| PIO1 | Referral Process |  |  |
| PI02 | Call Board |  |  |
| PI03 | Recording Telephone Calls |  |  |
| PI04 | CCTV |  |  |
| PI05 | Systm Online |  |  |
| PI06 | Repeat Dispensing and Electronic Transfer of Prescriptions |  |  |
| PI07 | SMS |  |  |
| PI08 | SCR and eSCR |  |  |
| PI09 | Sharing in/out of health records |  |  |
| PI10 | Ways we receive mail |  |  |
| PI11 | Payments and invoicing |  |  |
| PI12 | How we send mail out |  |  |
| PI13 | Meetings and Minutes |  |  |
| PI15 | Medicines Management |  |  |
| PI16 | Research |  |  |
| PI17 | Confidential Waste |  |  |
| PI18 | Office Machinery |  |  |
| PI19 | Clinical Machinery |  |  |
| PI20 | Collection of email address |  |  |
| PI21 | Accelerated Online Access |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Appendix 3

**Further information and useful web links – including Privacy Notices and information regarding the companies that we use**

If you would like further information please look at the following links

**Information Commissioners Office:**

[www.ico.org.uk](http://www.ico.org.uk/)

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/>

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/)

[www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/](http://www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/)

**NHS & IT systems:**

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance>

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>

**Our Clinical Computer system:**

www.tpp-uk.com

**NHS Research:**

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/>

## [Individual companies we use – Privacy Notices and/or information:](#_Appendix_3)

|  |  |  |  |
| --- | --- | --- | --- |
| **Company** | **Connected to PIA ref number** | **Privacy Notice** | **Additional information** |
| **My Surgery Website (Practice Website)** | **Not applicable** |  |  |
| **DocMail (How we send out letters)** | **PI12** |  |  |
| **Shred-It (destruction of confidential waste)** | **PI17** |  |  |
| **Business Standards Authority** | **PI11** |  | [**www.nhsbsa.nhs.uk/privacy**](http://www.nhsbsa.nhs.uk/privacy) |
| **Technomed (ECG Cloud)** | **PI19** | [**https://ecg-od.com/privacy-policy/**](https://ecg-od.com/privacy-policy/) | [**www.technomed.co.uk/product/cardioline-ecg-webapp?category=ecg-data-management-systems**](http://www.technomed.co.uk/product/cardioline-ecg-webapp?category=ecg-data-management-systems) |