

# Grey Gable Surgery (the Practice)

## Data Protection Privacy Notice for Patients

### Introduction:

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

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

This Notice explains

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

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 became law on 25th May 2018. The GDPR is a single EU-wide regulation on the protection of confidential and sensitive information, the DPA 2018 deals with elements of UK law that differ from the European Regulation. These came into force in the UK on the 25th May 2018, repealing the previous Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 the practice responsible for your personal data is Grey Gable Surgery.

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

### How we use your information and the law.

Grey Gable Surgery will be what's known as the 'Controller' of the personal data you provide to us.

We collect basic personal data about you which does include special types of information and location-based information. This does include name, address, medical conditions, contact details such as email and mobile number etc.

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

## Why do we need your information?

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

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

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

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

## How do we lawfully use your data?

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

*Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"*

*Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

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

## **Risk Stratification**

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information is only provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way.

## **Medicines Management**

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

## **Patient Communication**

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

## **Safeguarding**

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

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

*Article 6(1)(e) '...exercise of official authority...'*

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

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

## **Categories of personal data**

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

## **Sources of the data**

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

## **Recipients of personal data**

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

## Research

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

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

### The legal bases for processing this information

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

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

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

## General Practice Data for Planning and Research

This practice is supporting vital health and care planning and research by sharing your data with NHS Digital. For more information about this see the [GP Practice Privacy Notice for General Practice Data for Planning and Research](#)

The NHS needs data about the patients it treats in order to plan and deliver its services and to ensure that care and treatment provided is safe and effective. The **General Practice Data for Planning and Research** data collection will help the NHS to improve health and care services for everyone by collecting patient data that can be used to do this. For example, patient data can help the NHS to:

- monitor the long-term safety and effectiveness of care.
- plan how to deliver better health and care services.
- prevent the spread of infectious diseases.
- identify new treatments and medicines through health research.

GP practices already share patient data for these purposes, but this new data collection will be more efficient and effective. We have agreed to share the patient data we look after in our practice with NHS Digital who will securely store, analyse, publish, and share this patient data to improve health and care services for everyone. This includes:

- informing and developing health and social care policy
- planning and commissioning health and care services
- taking steps to protect public health (including managing and monitoring the coronavirus pandemic)
- in exceptional circumstances, providing you with individual care.
- enabling healthcare and scientific research

This means that we can get on with looking after our patients and NHS Digital can provide controlled access to patient data to the NHS and other organisations who need to use it to improve health and care for everyone.

Contributing to research projects will benefit us all as better and safer treatments are introduced more quickly and effectively without compromising your privacy and confidentiality.

NHS Digital has engaged with the [British Medical Association \(BMA\)](#), [Royal College of GPs \(RCGP\)](#) and the [National Data Guardian \(NDG\)](#) to ensure relevant safeguards are in place for patients and GP practices.

### What data is shared about you with NHS Digital?

Data will be shared from **1 September 2021**. Data may be shared from the GP medical records about:

- any living patient registered at a GP practice in England when the collection started - this includes children and adults.
- any patient who died after this data sharing started and was previously registered at a GP practice in England when the data collection started.

We will not share your name or where you live. Any other data that could directly identify you, for example your NHS number, General Practice Local Patient Number, full postcode, and date of birth, is replaced with unique codes which are produced by de-identification software before the data is shared with NHS Digital.

This process is called **pseudonymisation** and means that no one will be able to directly identify you in the data. NHS Digital will be able to use the same software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. Only NHS Digital has the ability to do this. An example would be where you consent to your identifiable data being shared with a research project or clinical trial in which you are participating, as they need to know the data is about you.

For more information about when NHS Digital may be able to re-identify the data, and how NHS Digital will use your data see the [NHS Digital General Practice Data for Planning and Research Transparency Notice](#).

### Opting Out

If you don't want your identifiable patient data to be shared for purposes except for your own care, you can opt-out by registering a [Type 1 Opt-out](#) or a [National Data Opt-out](#), or both. These opt-outs are different, and they are explained in more detail below. Your individual care will not be affected if you opt out using either option.

**Type 1 Opt-Outs** - If you do not want your identifiable patient data to be shared outside of the GP practice for purposes except your own care, you can register an opt-out with the GP practice. This is known as a Type 1 Opt-out. Type 1 Opt-outs were introduced in 2013 for data sharing from GP practices, but may be discontinued in the future as a new opt-out has since been introduced to cover the broader health and care system, called the [National Data Opt-out](#). If this happens, patients who have registered a Type 1 Opt-out will be informed. There is more information about National Data Opt-outs below.

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-in line with current policy. If this changes patients who have registered a Type 1 Opt-out will be informed.

If you do not want your patient data shared with NHS Digital for the purposes above, you can register a Type 1 Opt-out with your GP practice. You can register a Type 1 Opt-out at any time. You can also change your mind at any time and withdraw a Type 1 Opt-out.

If you have already registered a Type 1 Opt-out with us your data will not be shared with NHS Digital. If you wish to register a Type 1 Opt-out with your us before data sharing starts with NHS Digital, this should be done by [returning this form](#) to us practice **by 1 September 2021** to allow time for processing it. If you have previously registered a Type 1 Opt-out and you would like to withdraw this, you can also use the form to do this. You can send the form by post or email to your us at the GP Practice or call **0300 3035678** for a form to be sent out to you.

If you register a Type 1 Opt-out after your patient data has already been shared with NHS Digital, no more of your data will be shared with NHS Digital. NHS Digital will however still hold the patient data which was shared with them before you registered the Type 1 Opt-out.

If you do not want NHS Digital to share your identifiable patient data with anyone else for purposes beyond your own care, then you can also register a [National Data Opt-out](#).

## National Data Opt-Out

If you don't want your confidential patient information to be shared by NHS Digital with other organisations for purposes except your own care - either GP data, or other data it holds, such as hospital data - you can register a [National Data Opt-out](#).

If you have registered a National Data Opt-out, NHS Digital will not share any confidential patient information about you with other organisations, unless there is an exemption to this, such as where there is a legal requirement or where it is in the public interest to do so, such as helping to manage contagious diseases like coronavirus. You can find out more about [exemptions on the NHS website](#).

From **1 August 2022**, the National Data Opt-out will also apply to any confidential patient information shared by the GP practice with other organisations for purposes except your individual care. It will not apply to this data being shared by GP practices with NHS Digital, as it is a legal requirement for us to share this data with NHS Digital and the National Data Opt-out does not apply where there is a legal requirement to share data.

You can find out more about and register a National Data Opt-out or change your choice on [nhs.uk/your-nhs-data-matters](https://nhs.uk/your-nhs-data-matters) or by calling **0300 3035678**.

You can also set your opt-out preferences via the NHS App if you are registered to use this application.

### [The legal bases for processing this information.](#)

The Health and Social Care Act 2012 covers the sharing and collection of health and care data. It says that when the Secretary of State for Health and Social Care needs to collect and analyse data to help the health service, they can tell NHS Digital to do this for them. The instruction, which NHS Digital must act on, is called a **direction**. In this case:

- 1.) The Secretary of State for Health and Social Care sent a direction to NHS Digital, instructing them to collect and analyse general practice data for health and social care purposes including policy, planning, commissioning, public health, and research purposes.
- 2.) NHS Digital sent all GP practices a document called a Data Provision Notice, giving details of the data it needs GP Practices like ours to share so it can comply with the direction. All GP Practices in England are required to share data with NHS Digital when they are sent a Data Provision Notice.

Under data protection law, we can only share patient data if we have a legal basis under Articles 6 and 9 of the UK GDPR. Our legal basis for sharing patient data with NHS Digital is **Article 6(1)(c) - legal obligation, as we are required under the 2012 Act to share it with NHS Digital**.

When we are sharing patient data about health, we also need a legal basis under Article 9 of the UK GDPR. This is:

- **Article 9(2)(g)** – as we are sharing patient data for reasons of substantial public interest, for the purposes of NHS Digital exercising its statutory functions under the [General Practice Data for Planning and Research Directions](#). It is substantially in the public interest to process patient data for planning and research purposes to improve health and care services for everyone. This is permitted under paragraph 6 of Schedule 1 of the Data Protection Act 2018 (DPA).
- **Article 9(2)(h)** – as we are sharing patient data for the purposes of providing care and managing health and social care systems and services. This is permitted under paragraph 2 of Schedule 1 of the DPA.
- **Article 9(2)(i)** - as patient data will also be used for public health purposes. This is permitted under paragraphs 3 of Schedule 1 of the DPA.
- **Article 9(2)(j)** - as patient data will also be used for the purposes of scientific research and for statistical purposes. This is permitted under paragraph 4 of Schedule 1 of the DPA.

## **Worcestershire Integrated Electronic Patient Record**

Herefordshire and Worcestershire Health and Care NHS Trust (HWHCT) and General Practices (GPs) in Worcestershire are working collaboratively to deliver an integrated electronic health record linkage that would enable the sharing of personal health data between health professionals to facilitate the transformation of healthcare services in Worcestershire. By Deed of Accession this integration includes The Worcestershire Hospices (The Kemp Hospice, Kidderminster and Primrose Hospice, Bromsgrove)

### **What is integrated electronic health record?**

An integrated electronic health record is made up of relevant data from HWHCT & GPs. Which is then made available through two versions of the EMIS clinical system (“EMIS Community” which is used by HWHCT, and “EMIS GP” which is used by Worcestershire GPs) to provide a read-only view of a patient’s health information via the secure Health and Social Care Network (HSCN). This enables healthcare professionals who are directly involved in your healthcare to access the information needed to provide you with the best possible care.

### **Why are you developing an integrated electronic patient record and what are the benefits?**

Integrating your electronic health record will enable healthcare professionals who are directly involved in your healthcare to provide you with the best possible care. Currently healthcare providers you visit may each hold a different set of records about you. These records often contain duplicate information; or one record may hold information about a specific treatment or medication, and the other may not.

The primary benefits to having an integrated electronic health record linkage are:

- Avoidance of duplicate investigations or repeating the same information to different clinicians, thus improving patient experience
- Clinicians will have an increased awareness of key patient information e.g. prescribed medications.
- Improved communication between services and reliability of referrals
- Reduced hospital attendances/admissions as clinicians will have awareness of pre-existing conditions and treatment plans
- Reduced repeat testing with the availability of results across care settings
- Clinicians will be able to check previous referrals and appointments
- Enhanced transfer of care between services
- Enable healthcare professionals to access up-to-date information in circumstances where intervention is necessary to save or protect life or prevent a patient from serious/immediate harm. For example, during a collapse, unconsciousness, serious injury or accident.

### **The legal bases for processing this information**

*Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;”*

*Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

## **Birmingham and Solihull, Coventry & Warwickshire, Hereford & Worcestershire Collaborative Shared Care Record**

Birmingham and Solihull Integrated Care System (ICS), Coventry and Warwickshire ICS and Herefordshire and Worcestershire ICS are working collaboratively to develop an integrated health and care system (known as the Collaborative Shared Record) that would enable the sharing of health and social care data to facilitate the transformation of health and care services across traditional organisational and technological boundaries.

The Collaborative Shared Record programme aims to provide 'view only' access to identifiable data for purposes of direct care provision and administration by all parties, taking into account the complexity of people's lives and their over-lapping health and social needs.

The primary benefits of the sharing, particularly for Direct Care and Administration are anticipated to be:

- Better outcomes and more efficient health social care delivery for patients/service users/client irrespective of technological or organisational boundaries.
- Better use of resources so that residents receive the right care the first time around thereby reducing referrals, Accident & Emergency (A&E) attendances and inpatient admissions through improved data sharing and early intervention.
- Improved availability of data for health and care professionals to enable them to make more informed decisions about the health/care of their patients
- Avoidance of duplicate investigations improving patient experience
- Improved safety for patients and care professionals due to increased awareness of key patient information e.g. prescribed medications.

### **The legal bases for processing this information**

Article 6(1) of the GDPR is the condition for lawfully processing data for delivering direct care as part of the Collaborative Share record:

6(1) for the performance of a task carried out in the public interest or in the exercise of official authority...

Article 9(2)(h) of the GDPR is the condition for processing 'data concerning health' (personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) for direct care as part of the Collaborative Share record:

9(2)(h) medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...

Additional lawful basis that receiving parties may rely on in specific circumstances: Emergency situations where the data subject is incapable of giving consent

- Art 6(1)d ('vital interests')
- Art 9(2)c ('vital interests')

Safeguarding of vulnerable adults and children

- Art 6(1) c ('legal obligation to which the controller is subject')
- Art 9(2) g GDPR ('where the processing is necessary for the purposes of substantial public interest (protection of vulnerable individuals')



## Summary Care Records (SCR)

All patients registered with a GP have a Summary Care Record, unless they have chosen not to have one. The information held in your Summary Care Record gives registered and regulated healthcare professionals, away from your usual GP practice, access to information to provide you with safer care, reduce the risk of prescribing errors and improve your patient experience.

Your Summary Care Record contains basic (Core) information about allergies and medications and any reactions that you have had to medication in the past.

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 patients 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 Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

You can exercise these choices by doing the following:

1. Choose to have a Summary Care Record with all information shared. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.
2. Choose to have a Summary Care Record 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 Summary Care Record if they need to provide you with direct care.
3. Choose to opt-out of having a Summary Care Record 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.

To make these changes, you should inform your GP practice or complete this form and return it to your GP practice.

The legal bases for direct care via SCR is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider:

For the processing of personal data:

Article 6.1 (e) of the uK GDPR: ‘... performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’.

For the processing of “Special Category Data” (which includes your medical information):

Article 9.2 (h) of the UK GDPR: ‘... the purposes of preventive or occupational medicine.....’

## Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties includes:

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

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

## How do we maintain the confidentiality of your records?

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

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

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

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

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

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

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

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

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

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

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

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

## **Where do we store your information Electronically?**

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

No third parties have access to your personal data unless the law allows them to do so, and appropriate safeguards have been put in place such as a Data Processing agreement. We have a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category data.

### **EMIS Web**

The Practice uses a clinical system provided by a Data Processor called EMIS, with effect from 10<sup>th</sup> June 2019, EMIS will start storing your practice's EMIS Web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services ("AWS").

The data will remain in the UK at all times and will be fully encrypted both in transit and at rest. In doing this, there will be no change to the control of access to your data and the hosted service provider will not have any access to the decryption keys. AWS is one of the world's largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the very highest levels of security and support.

**Closed Circuit Television (CCTV) is in place throughout the surgery and its perimeter. This data is stored on site for two weeks before being overwritten.**

- **Under General Data Protection Regulations, the lawful basis for storing and processing CCTV image information is:** *Article 6(1)( e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller... and Article 9(2) (f) Processing is*

*necessary for the establishment, exercise or defence of legal claims....*

## **Who are our partner organisations?**

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

- NHS Trusts / Foundation Trusts
- GP's
- Primary Care Networks
- Integrated Care Systems
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers (for example, Onside Advocacy)
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Private Sector Providers
- Other 'data processors' which you will be informed of

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

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for the practice an appropriate contract (art 24-28) will be established for the processing of your information.

### **Organisations other than those listed above that we currently hold contracts with and share data:**

**AccuRx Texting service – your name and mobile telephone number are shared for purposes of sending appointment reminder messages, links to specific healthcare advice, recall requests and questionnaires. The lawful basis for this information sharing is as detailed on page 2.**

**AccuRx Video consulting – your name, mobile number and NHS number are shared for purposes of video consulting. The lawful basis for this information sharing is as detailed on page 2.**

**AccuRx Vaccine booking and Recording Solutions – your name, mobile number, gender, date of birth, NHS number, message content, vaccination appointment booking information, vaccination status and records of vaccinations and adverse events are shared for the purposes of vaccination booking and recording. The lawful basis for this information sharing is as detailed on page 2.**

**Accurx Patient Triage – your name, date of birth, contact details and details of your query are securely transmitted to the practice. No patient data is stored. This system directs patients towards relevant online information or to complete a form which is transmitted to the practice. The lawful basis for this information sharing is as detailed on page 2.**

**Clinical Practice Research Datalink (CPRD) – anonymised patient data is supplied to CPRD for the purposes of Public Health. You have the right to opt out of this research. The lawful basis for this information sharing is as detailed on page 2.**

**Health Intelligence – childhood vaccination and immunisation data is supplied to Health Intelligence (contracted by NHS England (West Midlands)) to support Child Health Services. The lawful basis for this information sharing is as detailed on page 2.**

**National Diabetes Audit – your NHS number, date of birth, postcode and information about your diabetes care is extracted by NHS Digital to help the NHS improve care. You have the right to opt out of this audit. Further information can be found in the National Diabetes Audit poster at the practice or on our website [www.greygablesurgery.com](http://www.greygablesurgery.com). The lawful basis for this information sharing is as detailed on page 2.**

**UK Mail Ltd – your name, address, NHS number and information relating to appointment invitations, referrals or other written information about your healthcare. The lawful basis for this information sharing is as detailed on page 2.**

**GP Connect Service – your NHS number. This software enables Out of Hours services to book an appointment with the GP directly into the practice’s appointment system. The lawful basis for this information sharing is as detailed on page 2 and additionally Article 6(1)(c) the processing is necessary to comply with a legal obligation.**

**Map My Diabetes – digital patient self-management resource – your name, address, email address, DOB, gender, telephone number, IP address, ethnicity, physical health information, conditions. The lawful basis for this information sharing is as detailed on page 2.**

**Your Covid Recovery – a web-based application encompassing the Covid-19 rehabilitation programme. Your demographic details (name, address, DOB, gender, marital status, employment status), email address, health data relating to rehabilitation, content of communications with – or regarding- patients sent via the web-based app . The lawful basis for this information sharing is as detailed on page 2.**

**Pharmaself24 (prescription vending machine) – with your consent - your name, address, NHS number, mobile number or email address. The lawful basis for this information sharing is as detailed on page 2.**

**X-On Surgery Connect (telephone system) - records all telephone calls. Recordings are retained for up to three years and are used periodically for the purposes of seeking clarification where there is a dispute and for staff training. Access to these recordings is restricted to named senior staff. Callers may request recording to be suspended at any point during a call. The lawful basis for this information sharing is as detailed on page 2.**

**Interface Clinical Services – EMIS number (patient reference within the surgery), NHS Number, address gender, medications and conditions. An audit service which aids diagnosis (case finding) and carries out reviews of some conditions such as COPD in order to optimise medications. The lawful basis for this information sharing is as detailed on page 2.**

**OpenSAFELY – Covid-19 analysis – Pseudonymised data and Anonymous data – not identifiable, for example trends and statistics. Demographic information (age, sex, area of residence, ethnicity). Clinical information pertaining to Covid-19 care and outcomes. Clinical information pertaining to wider health conditions, medication, allergies, physiological measures (eg BMI), prior blood tests and other investigation results, and other recent medical history (eg smoking). The legal basis for this are section 254 of the Health and Social Care Act 2012, to establish and operate such systems as are required for the collection and analysis of information for COVID-19 Purposes, such systems are to be known as COVID-19 Public Health Information Systems; and regulation 32 of the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013 (the Regulations), to exercise such system delivery functions of the Secretary of State as may be requested by the Secretary of State from time to time for COVID-19 Purposes.**

**Analyse Rx – practice identifier (not name or nhs number), gender, month and year of birth, medications, conditions, investigations held within clinical system. This programme is embedded with the practice’s clinical system. It enables the team to identify, prioritise, co-ordinate, track, manage and record medicines optimisation**

opportunities. The lawful basis for this information sharing is as detailed on page 2.

**NHS Type 2 Diabetes Remission Programme – patient name, phone number, email address, nhs number, DOB, gender, ethnicity, health data, relevant records and GP surgery details. This is an NHSE commissioned service to which eligible patients can be referred. The lawful basis for this information sharing is as detailed on page 2.**

**Dictate IT – Speech recognition solution – patient name, DOB, nhs number, health data. GPs may use this solution, which has been designed for the medical setting, to dictate clinical notes and referral letters. A real time solution allows the clinician to ‘dictate to cursor’ providing an efficient method of creating longer consultations and letters. The lawful basis for this information sharing is as detailed on page 2.**

### **Data Provision Notices**

The Health and Social Care Act 2012 (the Act) gives NHS England statutory powers under section 259(1), to require data from health or social care bodies, or organisations that provide health or adult social care in England. Data will be required, where it has been Directed to establish an information system by the Department of Health (DH) or NHS England (NHSE).

When a direction is received, NHS England can issue a Data Provision Notice to the appropriate providers of the required data who are then legally required, under section 259(5) of the Act, to provide the data in the form, manner and period as requested. Data is collected to ensure that adequate information is available to support the commissioning and planning of services.

Data Provision Notices in place currently include:

- Female Genital Mutilation
- National Diabetes Audit
- National Obesity Audit
- Pandemic Planning and Research

## Primary Care Network

The objective of Primary Care Networks (PCNs) is for groups of Practices to work together to create more collaborative workforces which ease the pressure on GPs, leaving them better able to focus on patient care. As of July 2019 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 more easily integrate with the wider health and care system.

Grey Gable Surgery is part of the Vale Health Network which is made up of 7 Practices in total and which covers approximately 62,000 patients. The Vale Health Network also includes Community-based Healthcare staff such as District Nurses, Specialist Nurses, Physiotherapists and Occupational Therapists who are employed by the Worcestershire Health and Care NHS Trust.

This means the Practice may share your information with other Practices and other staff within the PCN to provide you with your care and treatment.

Members practices of The Vale of Evesham Primary Care Network:

- Abbey Medical Practice
- Barn Close Surgery
- Bredon Hill Surgery
- DeMontfort Surgery
- Grey Gable Surgery
- Merstow Green Medical Practice
- Riverside Surgery

## Computer System

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

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisations (as listed above). Wherever possible, their staff will ask for your consent before your information is viewed.

## Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to other systems. You can opt-out of this sharing of your records with our partners at any time if this sharing is based on your consent.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for GREY GABLE SURGERY an appropriate contract will be established for the processing of your information.

## 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.

## How long will we store your information?

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

More information on records retention can be found in the NHS Records Management Code of Practice 2020

[https://www.nhs.uk/media/documents/NHSX\\_Records\\_Management\\_Code\\_of\\_Practice\\_2020\\_3.pdf](https://www.nhs.uk/media/documents/NHSX_Records_Management_Code_of_Practice_2020_3.pdf)

## Destruction

This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal, we have the following responsibilities:

- to ensure that information held in manual form is destroyed using a cross-cut shredder or contracted to a reputable confidential waste company Shredpro that complies with European Standard EN15713 and obtain certificates of destruction.
- to ensure that electronic storage media used to store, or process information are destroyed or overwritten to national standards.

## Your rights over your personal information

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

**Right to be informed:** You have the right to be informed on how we handle, process and share your personal information; this privacy notice ensures as a practice we satisfy this.

**Right to object:** If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

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

**Right to rectification:** The correction of personal data when incorrect, out of date or incomplete will be acted upon within one calendar month of receipt of such a request.

**Right to erasure:** In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be



allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will Delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

**Right to restrict processing:** Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that you can limit the way that the practice uses your data. This is an alternative to requesting the erasure of your data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction.

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

**Rights in relation to automated decision making and profiling:** Automated individual decision-making is a decision made by automated means (i.e., a computer system) without any human involvement. If any of the processes we use rely on automated decision making, you do have the right to ask for a human to review any computer-generated decision at any point.

## **Access to your personal information**

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

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

**Online Access to your Medical Records:** From 1 November 2022, online access to your full prospective medical records is activated by default. That is, all records held by the surgery dated 1 November 2022 and onwards will be visible to view online. Records dated before 1 November 2022 have restricted online visibility due to the risk of releasing third party or harmful information. For online access to historic records, please contact the practice.

There may be occasions when information may be withheld if the practice believes that releasing the information to you could cause serious harm or distress. Information may also be withheld if another person (ie third party) is identified in the record and they do not want their information disclosed to you. However, if the other person mentioned in your records was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that information.

## **What should you do if your personal information changes?**

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

## **Objections / Complaints**

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

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

Tel: 01625 545745  
<https://ico.org.uk/>

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

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

**IG Lead:**  
**Dr Rahul Unnikrishnan**

**Caldicott Guardian:**  
**Dr Rahul Unnikrishnan**

### **Data Protection Officer:**

The Practice Data Protection Officer is Hayley Gidman of MLCSU (Midlands & Lancashire Commissioning Support Unit). Any queries regarding Data Protection issues should be addressed to:

Email: [mlcsu.dpo@nhs.net](mailto:mlcsu.dpo@nhs.net)  
Tel: 01782 916875  
Postal: Head of Information Governance  
Midlands and Lancashire CSU  
Heron House  
120 Grove Road  
Fenton  
Stoke on Trent  
ST4 4LX

### **Changes:**

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

### **Useful Links**

Please find below some links to external webpages which you may wish to access to find out additional information:

- [Information Commissioners Office](#)
- [Information Governance Alliance](#)
- [NHS Constitution](#)
- [NHS Digital Guide to Confidentiality in Health and Social Care](#)
- [Health Research Authority](#)
- [Health Research Authority Confidentiality Advisory Group \(CAG\)](#)

- [National Data Opt-Out](#)