Dr H A D Martin
Dr Gemma Carruthers
Dr O Adali
Dr Daisy Clegg
Dr Laskshmi Santharam
Dr Laura Kirkland
Dr Christine Sitaranjan

Grange Street Surgery
2 Grange Street
St Albans
Herts
AL3 5NF
Tel: (01727) 833550
E-mail: enquiriesgss@nhs.net
Website: www.grangestreetsurgery.co.uk

Privacy Policy

1. About us

We are Grange Street Surgery and we are the data controller for the information we hold about you. A data controller is the organisation that makes decisions about the personal data that is being collected and processed and we are ultimately in charge of and responsible for the processing.

You can contact us in relation to this policy and any queries about it and/or to access your rights by contacting us using the below details.

2 Grange Street, St Albans, Hertfordshire, AL3 5NF

Telephone: 01727 833550

Enquiriesgss@nhs.net

Please use these details, should you wish to speak to our Data Protection Officer.

We are registered with the Information Commissioners Office (ICO) and our registration number is: Z5712962

At Grange Street Surgery, we are committed to protecting and respecting your privacy, informing you of your rights under Data Protection legislation and giving you access to these rights.

This Privacy Policy sets out important details about information that Grange Street Surgery and staff responsible for your care and treatment may collect and hold about you, how that information may be used and your legal rights.

We will review this Privacy Policy on a regular basis, and we advise you to check back on our website for the latest version.

2. Who has information about me?

For your healthcare, several care providers hold and share information about you, in order to provide safe and effective care.

Information is shared for your direct care purposes. There may be instances where we are required under legislation to share information, but we will only do so if we have a legal basis.

3. Information we hold about you

We hold 2 types of data about you.

a) Personal data (data which identifies you)

• Personal data only includes information relating to natural persons, i.e. name, phone number, email address, address, date of birth, etc.

• Personal data may also include special categories of personal data or criminal conviction and offences data. These are more sensitive, and Grange Street Surgery may only process them in more limited circumstances.

• Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

b) Special Category (sensitive data)

This sort of data could include:

• racial or ethnic origin

• political opinions

• religious or philosophical beliefs

• trade union membership

• genetic data

• biometric data (where used for identification purposes)

• health

• sex life

• sexual orientation

4. How we collect your information

The information we collect and process about you has either been provided by you or by others involved in your care and treatment (i.e., hospital, community, employers).

This is likely to include your personal data (see 3. a))

We may also hold more sensitive information about you (see 3.b)))

We may collect information from you when:

a) You contact us via telephone calls which may be recorded and retained for a limited period for training and monitoring purposes and to help improve our services.

b) You communicate with us via email, social media or our website.

c) You visit the practice for an appointment.

Sometimes we obtain information about you from:

• other health care providers,

• credit reference agencies,

• debt collection agencies, and

• government agencies such as HMRC or the Home Office.

5. How we use your information

We use information about you in connection with

• treatment and/or care,

• tests or assessments, and

• medical examinations

We may use your phone number (or email address where you have provided it to us) to contact you in advance of an appointment for reasons connected with your care or treatment. Where you have provided us with your mobile number or email address, we may send you confirmations/reminders of your appointments via text message or email and we may respond to your email enquiries via email.

We may also use information about you for:

• quality assurance,

• maintaining our business records,

• developing and improving our products and services, and

• monitoring outcomes where we believe there is a business need to do so and our use of information about you does not cause harm to you.

This may include our staff planning and workload management systems to help support our staff and clinicians to develop and plan the most appropriate levels of care to our patients and to ensure we have got the right levels of productivity and

efficiency and good outcomes for patients.

We may also use information about you where there is a legal or regulatory obligation on us to do so (such as the prevention of fraud or safeguarding) or in connection with legal proceedings.

We may also use information about you where you have provided your consent to us doing so.

We do not carry out automated decision making or profiling.

6. Staff access to your personal and sensitive data.

We carefully control who has access to your information. Staff only have access where they are required to do so to provide direct care or support (i.e., receptionist and secretary). Where possible we limit the access that staff have on our clinical systems. We also carry out spot checks and audits to see if there has been any inappropriate access. Where that occurs, disciplinary action may be taken against the staff, and in serious cases court action. If a data breach includes access to your information, we will contact you. We also have an obligation if it is a serious data breach to inform the Information Commissioners Office.

In order to reduce risk of a data breach we have in place robust policies and procedures and we carry out training for all staff on an annual basis.

All clinical staff providing direct care are registered with the appropriate professional and regulatory bodies, i.e., GMC, NMC, CSP and have a responsibility to uphold the highest standards when handling patient/client information.

7. How we keep your information safe and secure

• Grange Street Surgery is required to complete the NHS Digital Data Security & Protection Toolkit. This is a tool that provides assurance that we are meeting standards on handling patient/client information.

• We have Data Protection Policies in place to ensure staff understand the 'must' or 'must not do' with patient/client data.

• Staff are required to complete induction training in Information Governance and to complete annual update training.

• Spot checks are carried out across the practice.

• Our IT is managed by ITS Digital Limited IT Team who ensure that all safeguards are

in place to protect data held on IT systems are protected and secure from unauthorised access, loss or damage and hold a Cyber Security Plus certification.

• Passwords are changed on a regular basis.

• Where incidents do happen, our investigations will include actions we take and lessons learnt.

8. Sharing your information

We set out these reasons for sharing your information below and assure you that in each case, we share only such information as is appropriate, necessary and proportionate.

a) We will share your medical information with those involved in your health assessment, care or treatment (such as doctors, nurses and physiotherapists) for direct care purposes. Some of our nursing staff and the resident doctors in our practice are provided by specialist staffing agencies. We ensure there is a single patient record for each patient who is seen at our practice.

b) We will also share information about you with other members of staff involved in the delivery of your direct care for administration purposes (such as our, medical secretaries, receptionists). This will be limited to what is required for them to fulfil their role.

c) Local NHS hospitals and independent pathology/clinical laboratory services provide name of practice with support services (such as blood tests) and we may share information about you with these hospitals where required in connection with your care.

d) We may also share relevant parts of your medical information with your dentist, other private organisations and the organisation paying for your treatment (for example your insurance company). For our health assessment clients who come to us through their employer's health assessment benefit scheme, please be assured that we will not share your medical information with your employer without your consent.

e) We may share information about you with anyone you have asked us to communicate with or whose details you have provided as an emergency

contact (such as your next of kin).

9. Sharing information with third parties who are not involved in your health assessment, care or treatment

We may share information about you with external organisations such as:

• our lawyers,

• auditors,

• Insurance companies

• NHS organisations, and

• regulatory bodies such as the CQC and ICO.

We will only do this where we have a legal basis to do so or with your consent.

We may also share information about you with third party suppliers, which provide us with

• electronic patient record systems

• radiology imaging archiving and reporting systems.

• Other

We may also share information about you with those providing us with information technology systems, this includes:

• an incident management and recording system, and

• a system for electronic prescribing as well as

• other clinical and non-clinical software applications (and related services)

In each case, we would share only such information as was relevant, necessary and proportionate.

9. Sharing with regulators or because of a legal obligation

We may share information about you with our regulators, including the

• Care Quality Commission.

• Medicines and Healthcare products Regulatory Agency (which ensures medicines and medical devices used in the UK work and are acceptably safe).

• NHS England (which leads the NHS in England) and the Department of Health (the government department responsible for health and adult social care policy).

• Health & Safety Executive.

• Public Health England.

Sometimes, we are required to disclose information about you because we are legally required to do so. This may be because of a:

• court order

• regulatory body has statutory powers to access patients' or health assessment clients' records as part of their duties to investigate complaints, accidents, or health professionals' fitness to practise.

Before any disclosure will be made, we will satisfy ourselves that any disclosure sought is required by law or can be justified in the public interest.

Information about you may also be shared with the police and other third parties where reasonably necessary for the prevention or detection of crime. On occasion, this may include the Home Office and HMRC.

10. Audits, surveys, and initiatives

In common with all healthcare providers (both NHS and private), we also look at the quality of the care we provide:

• to patients and health assessment clients and participate in national audits and initiatives,

• to ensure that patients are getting the best possible outcomes from their treatment and care, and

• to help patients make informed choices about the care they receive.

We can assure you that your personal information always remains under our control.

Any information we provide for national audits and initiatives outside of Grange Street Surgery will not contain any information in which any patient can be identified unless it is required by law. Any publishing of this data will be in anonymised statistical form. The Practice may partake in local audits where there has been a Serious Incident in order to identify any potential clinical risks to yourself or other patients

11. Legal basis for using your information

Data protection law requires that we set out the legal basis for holding and using information about you. We have set out the various reasons we use information about you and alongside each, the legal basis for doing so. Given that some information we hold about you is particularly sensitive (as described above), we need

an additional legal basis which we have set out in the third column (entitled 'legal basis for more sensitive information') explaining our reason for this.

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

c) processing is necessary for compliance with a legal obligation to which the controller is subject.

d) processing is necessary to protect the vital interests of the data subject or of another natural person.

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.

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

For the purpose of delivering your direct health care within the practice and sharing your information we use Article 6 of the UK GDPR (11. e)) above.

Where we have to share your information because we are required to do so under law, we use Article 6 of the UK GDPR (11. c)) above.

Where we process any more sensitive (special category data) we do this on and additional legal basis under article 9 of the UK GDPR:

g) Health or social care (with a basis in law).

12. Where and for how long we store your information

The information about you that we hold, and use is held securely in the United Kingdom and stored electronically and in paper format and on secure servers.
No records are stored outside the EEA.
We retain your records for certain periods (depending on the record) under our retention of records policy. Grange Street Surgery follows the recommend best practice contained in the NHS Records Management Code of Practice. This is to ensure that information is properly managed and is available whenever and wherever there is a justified need for that information, including:

- to support patient care and continuity of care.
- to support evidence-based clinical practice.
- to assist clinical and other audits.
- to support our public task
- to meet legal requirements.

Your records may not be retained in hard copy form where a digital copy exists.
If you would like more detailed information on this, please contact our Practice Manager (contact details above).

13. Your information rights

Under certain circumstances, you have rights under data protection laws in relation to any personal information that we hold about you. Please note that for some purposes, especially within health and care, some of your rights under UK GDPR have applicable exemptions. You can find out more about your rights and exemptions on the ICO website.
If you wish to exercise any of the rights set out below, please contact the Practice Manager using the contact details set out above.
You have:
a) The right to be informed. This privacy notice forms part of that, but we also aim to keep you fully informed during your consultations, via posters in the practice and leaflets when appropriate.
b) The right to access your personal information. You are usually entitled to a copy of the personal information we hold about you and details about how we use it.

Your information will usually be provided to you in the form you request, if we are unable to do that, we will inform you. If you have made the request electronically (e.g. by email) the information will be provided to you by electronic means where possible.

Under data protection law we must usually confirm whether we have personal information about you. If we do hold personal information about you, we usually need to explain to you:

• The purposes for which we use your personal information.

• The types of personal information we hold about you.

• Who your personal information has been or will be shared with.

• Where possible, the length of time we expect to hold your personal information. If that is not possible, the criteria we use to determine how long we hold your information for.

• If the personal data we hold about you was not provided by you, where we obtained the information from.

• Your right to ask us to amend or delete your personal information (if appropriate).

• Your right to ask us to restrict how your personal information is used or to object to our use of your personal information (if appropriate).

• Your right to complain to the Information Commissioner's Office.

• We also need to provide you with a copy of your personal information.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity (this will be proportionate) and ensure your right to access your personal information (or to exercise any of your other rights). We may also contact you to ask you for further information in relation to your request to speed up our response.

We respond to all requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of

requests. In this case, we will notify you and keep you updated.

c) The right to request correction of your personal information

We take reasonable steps to ensure that the personal information we hold about you is accurate and complete and up to date. However, if you do not believe this is the case, you can ask us to update or amend it.

d) The right to request erasure of your personal information

In some circumstances, you have the right to request the erasure of the personal information that we hold about you. This is also known as the 'right to be forgotten'. However, there are exceptions to this right and in certain circumstances we can refuse to delete the information in question.

e) The right to object to the processing of your personal information

In some circumstances, you have the right to object to the processing of your personal information. This would usually apply to processing for other purposes other than your direct health care i.e., research

f) The right to request a transfer of your personal information

In some circumstances, we must transfer personal information that you have provided to us to you or (if this is technically feasible) another individual/ organisation of your choice. The information must be transferred in an electronic format.

g) The right to object.

You can ask us to stop sending processing your information for any other purposes other than your health care.

h) The right not to be subject to automatic decisions (i.e., decisions that are made about you by computer alone)

You have a right to not be subject to automatic decisions (i.e., decisions that are made about you by computer alone) that have a legal or other significant effect on you.

i) The right to withdraw your consent

You have the right to withdraw your consent where we rely upon this as a legal ground for processing your information.

To apply any of the Individual Rights above please contact the Practice Manager.

14. CCTV

We have installed CCTV to:

• ensure the security of our and your property and the security of our patients and staff

• monitor the security of our premises.

All CCTV is maintained and overseen by our practice manager. They are responsible for carrying out compliance audits and reviewing the need for CCTV. CCTV footage may be shared for the detection and/or prevention of crime or fraud.

15. General Practice Data for Research

The data held in the GP medical records of patients is used to support health research in England, helping to find better treatments and improve patient outcomes for everyone. Any data that could directly identify you (such as NHS Number, date of birth, full postcode) is replaced with unique codes which are produced by deidentification software before the data is shared with NHS England.

This process is called pseudonymisation and means that patients will not be identified directly in the data.

If you do not want your patient data to be shared for purposes except your own care, you can opt-out of this process.

For further information please access the website here https://digital.nhs.uk/services/national-data-opt-out or contact the practice.

16. My Care Record

My Care Record enables health and care professionals to access the information they need to look after you, even if they work for different organisations or in different locations.

Grange Street Surgery is part of My Care Record, an approach to improving care by joining up health and care information. Health and care professionals from other services will be able to view information from the records we hold about you when it is needed for your care. Please see www.mycarerecord.org.uk for more information.

For further information please access the website My Care Record - Home or contact the practice.

17. Health Information Exchange Gateway

Joining up health and care information via the HIE (Health Information Exchange) used across the region to enable heath and care professionals to access up-to-date information held by different organisations or in different locations. This will result in more effective care and secure information sharing for direct care purposes.

Each organisation will determine the content of their own information feed into the Shared Care Record. This will be based on the nature of the records that the organisation holds.

The Cerner HIE (Shared Care Record) system displays the feeds from partner organisations in a single user accessible dashboard, in real time.

18. Recordings

• Telephone calls are being recorded for training and monitoring purposes only.

• When the Surgery carries out video consultations. The consultation is not stored or recorded within the system; the clinical staff member is required to record observations and outcomes of the consultation directly into your patient's record in the same way as during a face-to-face consultation

19. Primary Care Network (PCN)

We are a member of Alban Primary Care Network (PCN). This means we will be working closely with several other GP Practices and health and care organisations to provide healthcare services to you. No health data is automatically shared. Patient records remain with the practice that the patient is registered with, the record would only be accessed by another practice if the patient has booked and agreed an extended access appointment or clinical services delivered in a GP Practice, the patient is advised of this at the time of accepting the appointment

Other Practices in our PCN are:

• Midway Surgery

• Parkbury House Surgery

20. Integrated Care Systems (ICS)

As the country moves to an integrated care system based on geographical areas (East & North Herts, Herts Valleys and West Essex) Information may be available to other care providers in order to provide safe, effective and cost-efficient care. Robust

training, policies, procedures, controls, audits and technical measures will be in place to safeguard against inappropriate access and disclosure.

21. Integrated Care Board (ICB)

The Integrated Care Board's are responsible for securing, planning, designing and paying for your NHS services, including planned and emergency hospital care, mental health, rehabilitation, community and primary medical care (GP) services. This is known as commissioning. We do share data with Herts and West Essex ICB who is working with GP practices, local hospitals and other providers, generating Population Health Management information and link all the information together but then remove information that identifies you. The linked and pseudonymised information will help the ICB learn to use the data. The information will be reviewed and decisions made about the whole population.

As part of the review, a group of individuals or a single individual might be identified that could benefit from some additional care or support. The information will be sent back to the us (your GP) and we will use the unique code to identify you and offer you relevant services (direct care).

The ICB are legally obliged to protect your information and maintain confidentiality in the same way as us (your GP) or hospital provider.

22. Using your data to plan and support better care

Your GP data, including age, gender and medications prescribed, is used to plan health and care services for the local area, as well as help your GP provide better personalised care.

This process is called risk stratification and is a statutory (legal) requirement.

If however, you don't want your data to be used in this way, you can opt-out, but need to be aware that this can affect the proactive provision of your care.

What is risk stratification?

In Hertfordshire and West Essex, we take part in two types of risk stratification:

• Risk stratification for case-finding

• Risk-stratification for commissioning

In both cases risk stratification tools use patient data, such as age gender, diagnoses, hospital attendance and admissions, which is collected by NHS Digital

from NHS hospitals and community care services. This is then linked to data from GP practices and analysed. It is important to note that your name is not used when the data is being analysed. Only your NHS number is used during this process. GP practices will then be able to view your name when it is appropriate to do so to improve the services available to you.

Risk stratification for case-finding

This is a process GPs use to help them spot and support patients with long-term conditions and help prevent unplanned hospital admissions or reduce the risk of developing other diseases.

Your GP will use computer calculations to pick out registered patients who are at the most risk.

Your GP will do this on a routine basis. It will be done electronically and will produce a report that will be reviewed by a clinical team at your practice. You might then be contacted if changes to your care are identified.

Risk stratification for commissioning

This is a process Hertfordshire and West Essex Integrated Care Board (HWE ICB) use to understand the needs of the local population so they can commission the right care services.

Data is sent by NHS England and/or GP practices directly into a risk stratification tool provided by an NHS England-approved supplier.

ICB staff only have access to anonymised or aggregated data. You will not be personally identifiable nor will any ICB staff have access to your personal or confidential data.

Your rights

It is a statutory requirement for NHS England to collect identifiable information.

There is Section 251 of the NHS Act 2006 which allows the Secretary of State, to set aside the common law duty of confidentiality for defined medical purposes. Approval is obtained through the Confidentiality Advisory Group of the Health Research Authority, that means HWE ICB can receive this data in line with specific technical and security measures in place.

Opt-out

If you are happy for your data to be used in this way, you don't need to do anything. However, if you don't want your data included, you can choose to opt out by contacting your GP Practice who will advise on how to opt out of local specific projects. You may also wish to opt out of your information being used for research or planning purposes nationally by visiting: https://www.nhs.uk/your-nhs-data-matters/

To find out more about which risk stratification tools are used, how your personal data is handled and your rights, you can view the HWE ICB Privacy Notice available at the web address provided below or your GP Practice privacy notice available on the GP practice website or as a leaflet in the reception area.

https://hertsandwestessex.icb.nhs.uk/website/privacy-notice-1

24. The right to complain to the Information Commissioner's Office

You have the right to complain to the Information Commissioner's Office if you are unhappy with the way that we have dealt with a request from you to exercise any of these rights, or if you think we have not complied with our legal obligations under data protection law.

Making a complaint will not affect any other legal rights or remedies that you have.

More information can be found on the Information Commissioner's Office website: https://ico.org.uk/ and the Information Commissioner's Office can be contacted by post, phone, or email as follows:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 (if you prefer to use a national rate number)

Fax: 01625 524 510

Email: casework@ico.org.uk

For further questions or to exercise any rights set out in this Privacy Policy, please

contact us on the contact details provided above to request to speak to the Data Protection Officer.

Please note that this privacy policy applies to our practice and the information we collect about you only. For any services, other parties or websites mentioned in this privacy policy or on our website, we do not accept liability and we advise you to read their privacy policies.