**Coggeshall Surgery**

Data Security and Protection Policy for Patients

**What is a Privacy Notice?**

This privacy notice explains why we, as a Practice, collect information about our patients and how

we use that information.

Providing a ‘Privacy Notice’ is a way of stating the Practice’s commitment to being transparent and

is a part of fair processing. It includes information on:

* what information are we collecting?
* who collects the data?
* how is it collected?
* why do we collect it?
* how will we use the data?
* who will we share it with?
* what is the effect on the individuals?
* your rights as an individual to object or complain?

**Principles**

The principles of data protection are broadly the same under the old Data Protection Act 1998

(DPA) and the new General Data Processing Regulation (GDPR). The Practice must process personal

data in a fair and lawful manner. In practice, this means that the Practice must;

* have legitimate reasons for the use or collection of personal data
* not use the data in a way that may cause adverse effects on the individuals (e.g. improper
* sharing of their information with 3rd parties)
* be transparent about how you the data will be used, and give appropriate privacy notices
* when collecting personal data
* handle personal data only as reasonably expected to do so
* make no unlawful use of the collected data

**Data Controller and Data Officer**

Under GDPR, the Data Controller is the person who has responsibility for ensuring that the data we

collect, process and share is handled lawfully. The Data Controller is the Practice and Dr Jennifer Johnson represents the Practice.

Under GDPR, the Data Protection Officer is an expert who can provide guidance and support for organisations. This Practice is part of Mid Essex Clinical Commissioning Group and the Data Officer is Jane Marley, Head of Information Governance and Data Protection Officer Essex CCGs. Her contact details are as follows:

Tel: 01268 594531

Tel: 07854 441295

Jane.marley@nhs.net

**Notification**

Organisations that store or process personal data have to register 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).

**What information do we collect and how is it stored?**

The health care professionals who provide you with care maintain records about your health and

any treatment or care you have received (e.g. NHS Hospital Trust, GP Surgery, Out of Hours

Services, etc). These records help to provide you with the best possible healthcare. NHS health

records may be processed electronically, on paper or a mixture of both; a combination of working

Practices and technology are used to ensure that your information is kept confidential and secure.

Records held by this GP Practice may include the following information:

* details about you, such as date of birth, address and next of kin
* any contact the Practice has had with you, including appointments (emergency or

scheduled), clinic visits etc.

* notes and reports about your health
* details about treatment and care received
* results of investigations, such as laboratory tests, x-rays, etc.
* relevant information from other health professionals, relatives or those who care for you
* administrative information such as complaints, letters explaining that you have moved out of our area etc.
* any recordings of phone calls we may make.

**Why do we store personal data?**

The Practice collects and holds data for the purpose of providing effective healthcare services to

our patients in a safe environment.

**Fair Processing**

The Practice manages patient information in accordance with existing laws and with guidance from

organisations that govern the provision of healthcare in England such as the Department of Health,

The British Medical Association and the General Medical Council. Fair Processing means that the

Practice has to be clear and open with people about how their information is used.

Every staff member who works for an NHS organisation has a legal obligation to maintain the

confidentiality of patient information. All of our staff and contractors receive appropriate and

regular training to ensure they are aware of their personal responsibilities and have legal and

contractual obligations to uphold confidentiality, enforceable through disciplinary procedures. Only

a limited number of authorised staff have access to personal information where it is appropriate to

their role and is strictly on a need-to-know basis. We maintain our duty of confidentiality to you at

all times. We will only ever use or pass on information about you if others 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), or where the law requires information to be

passed on.

Sometimes the Practice shares information with external organisations. These include:

* NHS trusts
* specialist trusts
* independent contractors such as dentists, opticians, pharmacists
* private sector providers including community services providers
* voluntary sector providers
* ambulance trusts
* clinical commissioning groups
* social care services and local authorities
* education services, police and fire and rescue services
* Other ‘data processors’ such as IT support, EMIS clinical management system provider.

We can disclose personal information if:

* it is required by law
* you provide consent – either implicitly or for the sake of their own care, or explicitly for

other purposes

* It is justified to be in the public interest

Some information will be shared centrally and used for statistical purposes (e.g. to review the

uptake and effectiveness of a screening program). We take strict and secure measures to ensure

that the minimal data is shared for the purpose. For example: the Practice shares your diabetes related data with the Diabetic Eye Screening Programme operated by Health Intelligence and commissioned by NHS England. This supports your invitation for eye screening where you are eligible and have been referred by the Practice for ongoing care by the screening programme. This data may be shared with any hospital eye services to support further treatment and with other healthcare professionals involved in your care.

If a patient has had NHS treatment, their personal information may be shared within a secure and

confidential online environment for invoicing purposes. This means sharing identifiable information such as name, address, date of treatment etc. to enable the billing process.

Our website uses cookies to optimise your experience and phone calls may be recorded for training and security purposes.

Risk stratification is a process used for identifying and managing patients who are at high risk of

requiring emergency or urgent care or who are very frail and more likely to need secondary care services. Typically this is because patients have a long term condition such as COPD, cancer or other medical condition at risk of sudden worsening. Information is collected to assess and derive a ‘risk score’ which may be shared with other care providers. If necessary your GP may be able to offer you additional services.

If you provide us with your mobile phone number we may use this to send you information relating to your health and the services we provide, reminders about your appointments or other health screening information. Please let us know if you do not wish to receive communications on your mobile by text

Information may be used for clinical audit purposes to monitor the quality of service provided. These processes enable your GP to focus on preventing ill health and not just the treatment of sickness.

The Practice is active for clinical research when called upon. Sometimes your information may be used for assessing your suitability for inviting you to be involved in clinical research studies. The Practice will always gain your consent before releasing your personal information.

**Keeping Data up to Date**

We have a duty to keep personal data as up to date as is possible. 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.

**Proactive Planning and Privacy Impact Assessments**

It is important that security of data and ensuring that we work in a safe and legal way is part of the

planning process in any new projects or developments. The Practice will carry out an Impact

Assessment when changing the way we work to ensure the safety of your personal data.

**Retaining Data**

Under GDPR data should not be stored for longer than is necessary. The Practice has a policy for the

retention period of the different types of data it stores.

**Access to Personal Information**

The GDPR gives patients the right to view any information held about them – the ‘Subject Access Right’ (SAR). This does not have to be in writing but we will need to check your identity to make

sure you are the person who is entitled to see the data. There is no longer a charge for straight forward SARs, however, there may be a charge to have repeated copies of the information held about you. Other than in exceptional circumstances, SARs should be completed within one month.

**Right to opt out of data sharing, to have inaccuracies corrected and to have data moved.**

You can object to your personal information being shared with other health care providers but if

this limits the treatment that you can receive then the doctor will explain this to you at the time.

Should you have any concerns about how your information is managed, or wish to opt out of any

data sharing at the Practice, please contact the Practice Manager, or your healthcare professional to

discuss how the disclosure of your personal information can be limited.

You have a choice on whether or not your confidential patient information can be used for purposes beyond your individual care, however, national data opt out is no longer recorded at the surgery. Please use the online service at https://www.nhs.uk/your-nhs-data-matters/manage-your-choice or call 0300 303 5678.

Patients have the right to change their minds and reverse a previous decision. Please contact the

Practice, if you change your mind regarding any previous choice.

When the Practice is about to participate in any new data-sharing scheme we will make patients

aware by displaying prominent notices in the surgery and on our website at least four weeks before

the scheme is due to start. We will also explain clearly what you have to do to ‘opt-out’ of each new

scheme.

Patients have a right to have any inaccuracies in their data deleted and corrected.

Patients have the right to move their data to another data controller (e.g another GP Practice)

**Right to complain and reporting of breaches**

Patients have a right to complain if they are not happy with the way their data is managed. Please

contact a member of the management team if you would like any more information or to make a

complaint. We have a duty to record any minor breaches of confidentiality and report any serious breaches to the ICO within 72 hours.

**Sending information outside of the EU**

There are strict regulations about what data can be sent outside of the EU. If you are planning to

emigrate outside of the EU you may want to consider making a request for a copy of your medical

records before you leave.

**Further information**

The Information Commissioner’s Office is the Regulator and offers independent advice and

guidance on the law and personal data, including your rights and how to access your personal information. For further information, please visit **www.ico.org.uk**