Confidentiality Notice

This document and the information contained therein is the property of St. Andrew's Medical Practice

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from St. Andrew's Medical Practice.

Document Details

Classification:	Standard Policy Document
Author and Role:	Tracey Martin (TM) - Practice Manager
Organisation:	St. Andrew's Medical Practice
Document Reference:	PATIENT GDPR POLICY
Current Version Number:	1.0
Current Document Approved By:	Dr Neil Middleton (NM)
Date Approved:	18/06/2018

Document Revision and Approval History

Version #	Date	Created by	Approved by	Comments
1.0	18/06/2018	TM	NM	Adopted Policy

PATIENT GDPR POLICY

INTRODUCTION

This policy sets out the data protection responsibilities of St. Andrew's Medical Practice under the EU General Data Protection Regulation (GDPR). It outlines our arrangements for the collection, storage and use of personal data under GDPR and the rights of patients to access their personal data.

Personal data refers to any information which relates to a natural person. Under GDPR a natural person is referred to as a data subject. As this policy relates to our patients we will refer to data subjects as patients throughout this document.

GDPR REQUIRMENTS

We hold data about our patients for a number of reasons connected with their health care. We must comply with GDPR in respect of this data in the following ways:

- Data must be fairly and lawfully processed.
- Data must be collected only for a legitimate purpose and processed only in a way that is compatible with that purpose.
- Data must be limited to what is required in relation to the purpose for which it is used.
- Data must be accurate and kept up to date.
- Data must not be kept for longer than is necessary.
- Data must be processed and stored in a safe and secure manner.
- The data collected and processed must be lawful, fair and transparent

The term 'processing' may include St. Andrew's Medical Practice obtaining, recording or holding the data or carrying out any set of operations on the data, including organising, altering, retrieving, consulting, using, disclosing, or destroying it.

We undertake to meet the above requirements and will put systems in place to ensure that patient personal data is used only for the purposes for which it was originally collected.

THE PERSONAL DATA WE COLLECT

Because you are a patient we need to collect and process certain information about you. This data is collected from the time you start receiving health and social care from St. Andrew's Medical Practice to the time that you are discharged or your health and social care need ends.

Examples of personal data that we will collect and process are:

- Name
- Address
- Age
- NHS Number
- Medical Conditions
- Medications

This is not a complete list but is indicative of the data we will need to collect and process in relation to your status as a patient with the Practice.

We will ask you to give your consent before we collect such data. We may refer you for treatment by other medical and/ or social care professionals who will need to access your medical records to provide their services to you. By giving your consent to your GP Practice you are also giving your consent for these other services to access your records and share your details with other professionals concerned with your care.

YOUR RIGHTS AS A PATIENT

GDPR gives you the following rights.

- The right to be informed about the data we collect and the reasons it is collected together with how we will use it and the way we store and destroy it.
- The right to access your data.
- The right to have any errors in your data rectified.
- The right to have your records erased in certain circumstances.
- The right to restrict processing.
- The right to data portability.
- The right to object to us processing certain data.

How we will enable these rights:

THE RIGHT TO BE INFORMED

This policy indicates the types of data that we hold about you. If we require additional information we will let you know. We will also explain why we need to collect the data and how it will be used.

We will allocate responsibility for Data Protection matters to a management person who will act as our Data Protection Officer. They will be responsible for all aspects of GDPR and for implementing this policy within St. Andrew's Medical Practice.

THE RIGHT TO ACCESS YOUR DATA

You may request access to your data by making a subject access request to the Data protection Officer. We will provide you with a form to make your request.

We will aim to reply to your request within one month.

We will not charge you for making a subject access request but may do so if a number of requests are made.

THE RIGHT TO HAVE ERRORS IN YOUR DATA RECTIFIED

If you find that any of the data we hold is inaccurate we have a responsibility to correct the error(s).

We aim to rectify any errors within one month of you notifying us.

THE RIGHT TO ERASE YOUR DATA UNDER CERTAIN CIRCUMSTANCES

You have the right to have personal data erased if:

- It is no longer necessary for the purpose for which it was originally collected
- You wish to withdraw your consent to us holding personal data and there is no reasonable, business, contractual or legal reason for us holding that data.

We will comply with your request to erase your personal data unless we have reasonable grounds to refuse. We will explain our reasons to you within one month of you making your request.

THE TIGHT TO RESTRICT PROCESSING

You may request that we cease processing of your personal data. We will retain and process only the data that we need to ensure that the business can operate its management systems and to allow us to comply with health care contracts or other legal requirements.

THE RIGHT TO DATA PORTABILITY

We may process your personal data using automated processes such as clinical systems software. You have a right to request a copy of such data and to use it for other purposes.

We will aim to comply with your request within one month of you making it.

THE RIGHT TO OBJECT TO THE PROCESSING OF YOUR DATA

You may object to us processing your personal data for certain purposes e.g. statistical purposes.

We will comply with your request immediately unless we can prove that we need to process the data for legitimate business reasons or for legal reasons e.g. to defend legal claims.

DATA RETENTION

We will only retain personal data for as long as is necessary in relation to the purpose for which it was originally collected.

When we no longer require the data we will archive it.

DATA SECURITY

We will ensure that all personal data will be kept secure.

We will adopt appropriate technical and organisational measures to prevent the unauthorised or unlawful processing or disclosure of data. Information of a personal nature will only be made available to personnel concerned with your care on a "need to know" basis.

We will keep records of the personal data we collect and process and the Data Protection Officer will be responsible for ensuring that we have measures in place to keep this data secure.

The following measures will be taken to keep personal data secure:

- Emails containing patient data will be encrypted
- Secure networks will be used to transmit patient data
- Patient data transferred in physical form will be marked “confidential”
- Electronic copies of patient data will be stored using passwords and encryption
- Paper copies or other physical copies will be stored in a locked cabinet
- All electronic copies will be backed up
- Data stored on laptops will be encrypted and password protected
- Passwords will be changed regularly
- Smartcards will be used to access clinical systems
- No software will be installed on Practice computers without permission
- Methods for securing personal data will be regularly reviewed
- Any third parties working as partners or in conjunction with the Practice who handle personal data will be required to demonstrate their compliance with this policy

IMPACT ASSESSMENTS

If we consider new uses for personal data which involves the use of technology to process and/or store it we will undertake a data protection risk (impact) assessment beforehand.

Such an assessment will cover the type and purpose of the data, the purpose for which it will be collected and used and the risks posed to patients.

The purpose of the assessment is to identify and minimise any such risks.

The Data Protection Officer will be responsible for conducting and overseeing all impact assessments.

TRANSFERRING PERSONAL DATA OUTSIDE THE EU

If we transfer personal data outside of the EU we will ensure that the receiving country has an EU approved level of data protection.

DATA BREACHES

All data breaches will be reported to our Data Protection Officer.

If the breach is likely to adversely affect the rights of a patient it will be reported to the Information Commissioner's Office. All affected patients will also be informed.

COMMITMENT

We will do our utmost to protect the personal data of our patients. It makes good business sense to set up systems to protect this data and it is essential that our patients have confidence that we will protect their data in accordance with the requirements of GDPR.

We will empower the Data Protection Officer to take such steps as are required to ensure that the Practice fully discharges its responsibilities under GDPR. We will also provide appropriate instruction and information for patients to ensure that they understand their rights and responsibilities under GDPR.

This policy will be reviewed annually to ensure it meets the needs of St. Andrew’s Medical Practice and its patients under GDPR.