General Data Protection Regulations

The Robins Surgery

First Practice Management

General Data Protection Regulations

- What is GDPR?
- What is changing?
- What does it mean to us?
- How do we make this happen?

First Practice Management

What is GDPR?

- The **General Data Protection Regulation** is the new EU legislation to protect the personal data of all EU citizens.
- It will apply even if we are no longer part of the EU.
- It will be a significant change in Data Protection for all UK , including the NHS and healthcare providers.
- Comes into force on **25th May 2018**

First Practice Management

GDPR terminology

- **Data Processing** – any actions taken with personal data (including storage);
  - Patient details
  - Job applicants
  - Storing and filing their details

- **Personal Data** – information about an individual that can identify them;
  - Name
  - Address
  - Patient ID / National Insurance No.

First Practice Management

GDPR terminology

- **Data Controller** – decides what the data is used for and how it is processed.
  - Legally Responsible for the use of data
  - Decide how to use the data (alone or with others)
  - Control the processing activities

- **Data Processor** – the person who processes the information for the Data Controller;
  - Recording
  - Changing
  - Updating
  - Organising

GDPR and Data Protection

- The current Data Protection Principles have been amended under the GDPR to make it easier for individuals to access information about them
  - Transparency & Lawfulness
  - Accountability

- Accuracy of the data held about Data Subjects

What is changing under GDPR?

- **Explicit consent** from data subject to process their data
- Patient has right to **withdraw consent**
- Data to be processed in compliance with **legal obligations**
- Practices should do a **risk assessment** to ensure data is secure
- **Data Subject Access Requests (DSAR)**
  - Respond within 1 month
  - No longer chargeable for most requests

What is changing under GDPR?

- Strengthens data subject rights to personal data;
  - Right to be Informed
  - Right of Access
  - Right to Rectification
  - Right to Erasure
  - Right to Restrict Processing
  - Right to Data Portability
  - Right to Object
  - Right to Automated decision-making and profiling.

What is changing under GDPR?

ACCOUNTABILITY

- We must be compliant and show that we are
- Know what data we hold and why we have it

PRIVACY NOTICE

- What information we hold, and what we do with it

CONSENT AND LAWFULNESS OF PROCESSING

- Provide proof of consent and lawful basis of processing.

First Practice Management

What is changing under GDPR?

DATA BREACHES

- Identify, record and report data breaches

MORE PATIENT'S "RIGHT TO…"

- Access to own data, no charge, and "right to forget" among others

DATA AWARENESS

- How & why we use/share data, any risks, reporting, is it lawful etc.

What does it mean to us?

- Change how we approach data protection
- Be more aware of how we process, access, view and record patient data
- Ask more questions about how secure our data is

This is not an option – it is essential.
GDPR will affect **all** organisations in the UK

First Practice Management

What does it mean to us?

- Fines will be imposed
  - Anything up to 20million Euros or 4% of global turnover (whichever is higher)

- Failure to follow rules could close down the practice.

What does it mean to us?

Processing Data must be done…

- Under instruction of Practice Data Controller
- Confidentially
- Securely

First Practice Management

Practice Contacts

Practice Data Controller : [Minhaz Bashar]

Caldicott Guardian : [Minhaz Bashar]

- Notify [Minhaz Bashar] of any Data Breaches (or potential).