Consentz

GDPR is almost here…

Consentz is at the forefront for developing its software and legals to be prepared fully for GDPR and we're here to help.

General Data Protection Regulation replaces the Data Protection Act 1998 on 25th May. So what does GDPR apply to:

Personal Data
Personal data means any information relating to an identified or identifiable person – so personal data on computers and paper files will be caught.

There are two types of personal data: *ordinary* personal data and *sensitive* personal data that demands higher standards – this includes health data.

First Steps to becoming Compliant
You need to audit what personal data your clinic collects and uses in all departments. This doesn't just catch medical records, but involves an analysis of marketing data, HR data, pensions data and supplier data.

In order to use personal data you need to show that its use falls within the defined lawful purposes.

For sensitive data, i.e. medical data, key gateways are:

- Explicit consent;
- Vital interests of data subject – this is say for reasons of their health; and
- Necessity to establish or defend a claim – i.e. records.

Transparency and Consent
Transparency over how data is used is a key GDPR theme. Using the personal data in accordance with the expectation of the individual is crucial.

In a nutshell the Information Commissioners Office wants businesses to be under an obligation to spell out what data they collect, what they do with it and stick with what they have told the consumer.

You therefore need to ensure that the following information is provided to individuals in your notices.

- Name and contact details of the controller (the clinic)
- Purposes for use of the data as well as the legal basis of the processing
- What your legitimate purposes are
- Categories of the recipients who the personal data will be disclosed

In addition to the above – the controller shall provide the data subject with further information in relation to:

- The period for which the personal data will be stored
- The right to access, rectify and erase the data (unless legally needed)
- The existence of the right to withdraw consent e.g. for direct marketing
- The right to lodge a complaint

Consents:

- Consent must be unambiguous and freely given
- Requires clear affirmative action
- For sensitive data, consent must be explicit
- Can be withdrawn at any time

GDPR Accountability and Governance

- You need to train your staff and make sure that those with access to personal data are aware what GDPR means and what they need to do.
- Personal data breaches, such as a lost medical record, must be reported within 72 hours
- You need to have a plan in place of how you would monitor and respond to a data breach.

Penalties

Up to €10 million or up to 2% of annual turnover whichever is higher. Also there is the added threat of potential individual claims by data subject.

For further information please go to the following link:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Embrace the Challenge!

A high quality digital platform will:

- Address fully the issues arising from GDPR regulation, as well as
- Transforming practice management and patient care

Consentz Terms and Conditions address the above points (prepared by Irwin Mitchell)

GDPR Features include:

- Time period for retention & report for files to be erased
- Patient access to their information
- Patient can change personal information remotely

Your Records are Secure with Consentz:

- Encryption
- Cyber security insurance
- Information Recovery Plans
- Data security monitoring
- Regular penetration testing by global data security company
- Hourly data back-ups
- Instantly revoke staff access