Surrey and Sussex Healthcare
NHS Trust

General Data Protection Regulation (GDPR) - Implementation

Dipa Bhella – Information Governance & Security Manager

Trust Board in Public

October 2017

Putting people first
Delivering excellent, accessible healthcare

An Associated University Hospital of Brighton and Sussex Medical School

What is GDPR?

- The GDPR is the General Data Protection Regulation. It's a new EU mandate designed to ensure data privacy and enhanced control of personal data for EU citizens.
- The GDPR replaces the EU's Data Protection Directive.
- The government has confirmed that the General Data Protection Regulation will form part of UK law following the country's withdrawal from the European Union.
- As at 25 May 2018, GDPR will need to be fully implemented within the organisation.

Key changes

- Increased penalties
  - Fines could be as high as 20 million euros or 4 per cent of annual global turnover
- More timely data breach reporting
  - Mandated to report breaches within 72 hours
- Subject access requests
  - No charge
  - One month to comply or up to 2 months extra (complex cases)

Key changes

- Right to data portability (new)
  - Enhanced form of subject access
  - Provide the data electronically and in a commonly used format

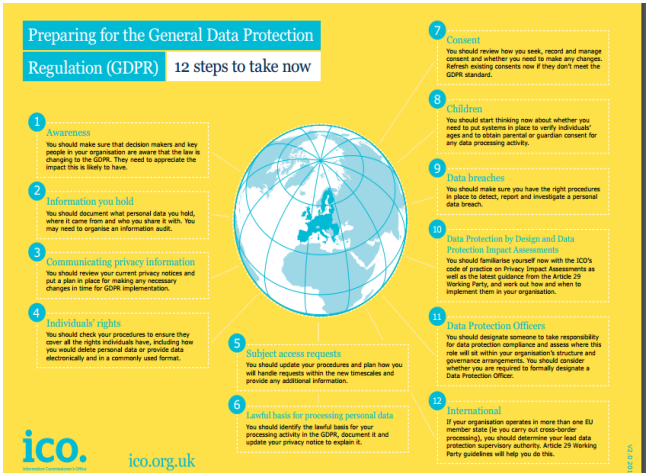
- Right to erasure (right to be forgotten)
  - Largely exempt in the H&SC sector
  - Keep data in line with current retentions schedules

Key changes

- Stronger data subject consent
  - GDPR states consent should be freely given, specific and unambiguous

- Appointment of a Data Protection Officer
  - Mandated DPO role to take responsibility for data protection compliance.

GDPR Implementation Action Plan



Action plan going forward covering the 12 steps

- Executive and Board briefing
- Update training materials
- Review data processor contracts
- Review Information asset register
- Review fair processing notice
- Document what personal data the organisation holds and where it came from (Data flow mapping)
- Data breaches - standard operating procedure
- Review consent procedures
- Implement the Data Protection privacy Impact Assessment

The GDPR implementation action plan will be monitored by the IGSG