



<b>Paper No. SET/56/17</b>	
	<b>Tick One ✓</b>
For discussion	
For approval	
For information/noting	✓

**Date of Trust Board Meeting:** 27 September 2017

**Confidential or Public Agenda:** Public

**Agenda item:** Implementation of General Data Protection Regulation  
– 25 May 2018

### 1.0 Introduction

This paper (and accompanying enclosure documents) brings to your attention the forthcoming European Union (EU) General Data Protection Regulation (GDPR) and its impact within Health & Social Care Trusts.

### 2.0 Background information

The implementation of GDPR on 25 May 2018 represents the biggest change in Data Protection law for 20 years. It replaces the Data Protection Act 1998, and it will continue to be enforced after the UK's exit from the EU. As a public body, the Trust has a statutory responsibility to know what personal data is held, how and why we process it, who has access to it, and with whom it is shared.

### 3.0 Brief summary of key points contained in the paper/s

#### 3.1 *GDPR Provisions*

GDPR retains the Data Protection Principles, as set out in the Data Protection Act however, they have been condensed into six as opposed to the eight principles. GDPR reinforces and extends citizens' rights, for example, requirements around obtaining "consent" are clearer and more demanding. New rights have been introduced, including:-

- The right to be forgotten (i.e. deletion of redundant personal data) and,
- Data portability (i.e., the transfer of personal data between bodies)

Other major provisions include:-

- Much higher fines for data breaches (up to €20 million or 4% of annual turnover, whichever is the highest);
- Statutory appointment of a Data Protection Officer;
- Mandatory personal data breach reporting to the Information Commissioner's Office (ICO) – any failure to report will be heavily penalised;
- 'Privacy by Design' approach to projects and IT systems involving personal data;
- Mandatory Privacy Impact Assessments (PIA) to identify and address risks

- to personal data;
- Creation and maintenance of an internal record of personal data you process, i.e. Information Asset Register;
- More detailed fair processing ('privacy') notices (to advise individuals how and why their personal data is used);
- Increased accountability of 'Data Processors' (those who process personal data on your behalf); and
- Report progress on GDPR preparations in your six monthly Assurance Statements.

### **3.2 Regional and Local Trust Preparations for GDPR**

A regional GDPR sub-committee has been commissioned by the Department of Health's (DoH) Information Governance Advisory Group (IGAG) with the aim of providing regional level HSC specific policy and guidance reflective of the needs of the new GDPR. The aim is to support the HSC to prepare for the requirements of the EU GDPR when it comes into force on 25 May 2018. A regional action plan is in place for all HSC Trusts. Local HSC Trust action plans have been developed as necessary. The Trust is represented on this group by Miss Lynda McAree, Head of Information Governance.

The HSC has a well-established Information Governance Framework and the majority of the requirements set out in the GDPR are already currently well developed. However the 12 steps to take now (ICO Guidance) to implementation of GDPR requires HSC to review its current policy & procedure as GDPR is very much about promoting the rights of the individual, our relationship with service users and the data we hold on them.

Within the Trust, the Information Governance Sub Committee (IGSC) is responsible for the implementation of the new GDPR Regulation. This is chaired by Mrs Weir and Ms Coulter, in their roles as Senior Information Risk Owner (SIRO) and Deputy SIRO. A Trust specific action plan has been developed (based on the regional action plan) and regular update reports are provided to the IGSC.

### **4.0 Recommendation/s for the Trust Board (please state if the paper/s is for information/noting or for approval by Board members)**

Trust Board is asked to note, for information, the preparation and plans in place in preparation for the implementation of the GDPR on 25 May 2018. In addition, a copy of the Trust's action plan (with status report as at 13 September 2017) together with the Information Commissioner's document – Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now is also attached.

**Lead Director:** Mrs Myra Weir  
**Designation:** Director Human Resources & Corporate Affairs (Senior Information Risk Owner)  
**Date:** 27 September 2017