General Data Protection Regulations (GDPR): Assurance Statement

The General Data Protection Regulation (GDPR), coming into force on the 25th May 2018, will be one of the strictest pieces of privacy legislation globally. Salisbury NHS Foundation Trust believes that privacy is a very important right for patients and employees and wishes to assure all the Trust's suppliers that we are working hard to ensure compliance in all areas of our business.

Within this statement we wanted to highlight the measures we have put in place to demonstrate our commitment to complying with GDPR.

Data Protection Officer

The Trust has designated a Data Protection Officer (DPO), who is advising the Trust on matters relating to data protection and GDPR compliance. The DPO will ensure that we are accountable and transparent to the public and the data protection regulator, the Information Commissioners Office (ICO), including the creation and maintenance of 'records of processing activities'.

Our DPO is: Ms Heidi Doubtfire-Lynn

IG/RA and Data Protection/Privacy Officer
C/O Informatics Department
Salisbury NHS Foundation Trust
SDH Central
Odstock Road
Odstock
Near Salisbury
SP2 8BJ

Email: Information.Governance@salisbury.nhs.uk
Tel: 01722 336262

Privacy by design

The Trust confirms that since 2018 all new or updated procedures or processes involving personal information must use of Privacy Impact Assessments (PIAs), now known as Data Privacy Impact Assessments (DPIAs) under GDPR help to identify and minimise the data protection risks.

Security

The Trust is committed to protecting and respecting the privacy of individuals, we take our obligations under data protection legislation seriously. We already manage personal data in accordance with the NHS Code of Practice: Confidentiality, Information Governance Toolkit which has been superseded by the NHS Digital Data Security and Protection Toolkit which is supported by the NHS Information Security Standards. We understand and welcome the

high standards that GDPR will promote and encourage across all organisations that process personal data on behalf of third party contractors and suppliers of service.

Data review

We are in the process of conducting an extensive review of all personal data we hold, and have prepared a detailed data roadmap which outlines where this data is held, why we hold it, and how long it must be kept for in line with the NHS Code of Practice: Records Management.

Contractual updates

Our Procurement Department is in the middle of conducting a full-scale due diligence exercise analysing third parties' GDPR compliance processing identifiable data on behalf of the Trust. If appropriate, supporting contractual clauses are being updated to comply with our statutory obligations under GDPR.

Processing updates

As GDPR guidance is issued we are updating our existing procedures to ensure we have the tools to maintain compliance with GDPR.

Improved Subject Access

We have updated our existing subject access request processes to ensure that it is easier and quicker for individuals to exercise their rights, and to respond efficiently to such requests within the statutory timescales.

Consent

Within the hospital environment we rarely rely on consent as the legal basis for collecting, using and sharing personal information. However, we continue to review our existing marketing practices, and associated consents/other lawful grounds for processing, to ensure that these are transparent, fair and GDPR compliant.

Pseudonymisation

The Trust routinely anonymises, pseudonymises and encrypts personal identifiable data. This may be used as one measure within a suite of measures designed to reduce risk where deemed appropriate and as part of an overall risk-based approach to the management of personal data.

Data Breaches

Under the GDPR, we must notify any data breach to the controller without undue delay. We have processes and procedures in place for identifying, reviewing and promptly reporting data breaches to the ICO.

Processing of personal information outside the UK

If personal information is transferred outside of the UK, we make sure that it is protected in line with the GDPR requirements.