Sandwell & West Birmingham Hospitals NHS Trust - GDPR Compliance Assurance Statement

General Data Protection Regulation (GDPR)- Information – How we've ensured compliance with data protection law, to make sure health and care data is always collected, stored, analysed and shared securely and legally.

Sandwell & West Birmingham Hospitals NHS Trust (the Trust) believes that the privacy and the rights of individuals is of the upmost importance and wishes to assure all of its patients, staff, partners and anybody else that it works with that it is working diligently on ensuring compliance with GDPR in all areas of its business.

Within this statement the Trust highlights the measures that have been put in place to ensure compliance with GDPR in relation to the processing of personal data.

Overview
Many of the GDPR's main concepts and principles are much the same as those in the current DPA, so most of the Trust's approach to compliance remains valid under the GDPR. However, there are new elements and enhancements, so the Trust will have to do some things for the first time and some things differently.

GDPR Implementation
The Trust has a GDPR Action Plan that has been formally endorsed by the most senior level of management, to ensure compliance with GDPR. The Plan covers the following areas:

1. Awareness – making sure that decision makers and key people are aware

2. Information – Establishing comprehensive records of processing activities (building on existing information asset registers and maps of information flows)documenting what personal data is held, how and where it is held, where it came from and with whom it is shared. This includes any contracts, information sharing or data processing agreements that the Trust has with its Data Processors, partner or third party organisations

3. Communicating privacy information – updating the Trust's current privacy and fair processing (transparency) notices to provide full disclosure of what personal data is used, for what purpose, who it is shared with and the legal basis for doing so and how long it will be retained

4. Individuals' rights – ensuring that Trust procedures cover all the rights individuals have, including how to cease processing personal data or provide data electronically and in a commonly used format

5. Subject access requests –updating Trust procedures and planning how to handle requests within the new timescales. The Trust will not be able to charge for requests and will have just a month to comply, rather than the current 40 days

6. Legal basis for processing – identifying the legal basis for processing information and documenting this in updated Trust Policies and Procedures

7. Consent – reviewing how to seek, obtain and record consent, when required. GDPR is clear that data controllers must be able to demonstrate that consent was given and that there is an effective audit trail

8. Legal Basis for processing – under GDPR our legal basis for processing the majority of data on a day-to-day basis will be as follows:
Article 6(1)(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
and
Article 9 (2)(h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9. Data breaches – ensuring procedures are in place to detect, report and investigate a personal data breach without undue delay

10. Data Protection by Design and Data Protection Impact Assessments (DPIA) – ensuring that data protection controls are considered at the design stage of new projects involving the processing of personal data

11. Data Protection Officer – the appointment of a Data Protection Officer to take responsibility for data protection compliance. They will have proven expert knowledge of data protection law and practices, and the ability to perform the tasks specified in the GDPR

Accountability

GDPR places greater emphasis on the documentation that the Trust must keep to demonstrate accountability. The Trust uses the annual Data Security and Protection Toolkit return that is made each March to NHS Digital (formerly known as the Information Governance Toolkit) to demonstrate our compliance with relevant legislation.

IT Security and Business Continuity Measures

The Trust continually seeks to ensure the confidentiality, integrity and availability of the personal data it stores or processes. The Trust maintains appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access

Further Information

If you wish to know more about how the Trust is meeting compliance with GDPR then please contact the Trust's Information Governance Manager, Email: IGovernance@nhs.net

March 2023