Imperial College Healthcare
NHS Trust

Guidance for all staff at Imperial College Healthcare NHS Trust: What does the General Data Protection Regulation mean for you?

The General Data Protection Regulation (GDPR) comes into force on 25th May 2018. It replaces the Data Protection Act 1998. By and large, the day to day activities of staff members within the Trust will not be substantially affected by the implementation of GDPR.

However, there are still **some changes** to the law that **will impact upon the work of Trust staff**, of which all staff need to be made aware.

The Data Protection Office (DPO) welcomes any enquiries or advice requests and is contactable at imperial.dpo@nhs.net.

1. **Incident Reporting:**

Under GDPR, the Trust will have an obligation to report breaches to the Information Commissioner's Office (ICO) if it presents a high risk to the rights and freedoms of individuals. This reporting must occur within 72 hours of that determination being made. Detailed records must still be kept of all data breaches within the Trust.

What this means for you: The DPO **already requires that all breaches are reported**. This policy will continue, but it is more crucial than ever that the proper reporting procedures are followed. You must report a breach to the DPO immediately. You will then be asked to complete an Incident Form detailing the incident and steps taken to investigate.

The DPO team will then assess the breach and make a determination as to whether it presents a high risk to individuals and whether it requires escalation to the ICO. You **must not** take it upon yourself to bypass the DPO to report breaches directly to the ICO.

2. Fair Processing of Data and the Trust Privacy Notice:

Under GDPR, there is an emphasis on **transparency** with regards to information processing. What this means is that patients, as data subjects, should be able to see how and why we are processing their data. This will be delivered through the revised **privacy notice to patients**. Given the complexity of the Trust's processing arrangements, this notice will be structured with different layers of detail.

What this means for you: Fair processing information must be provided at point of access, meaning that it must be accessible to patients. **You will need to know where the Trust Privacy Notice is published and how to direct patients to this information**. The 'top layer' of information will need to be readily available in clinical areas.

Fair processing equally applies to other data subjects, meaning the Trust's staff. As such, the **privacy notice for staff** will provide transparent information on how *your* data is handled and processed by the Trust.

3. Subject Access Requests:

It is important that **all staff** are aware of the rights of patients and staff to **access** the data that the Trust holds about them. Whilst this right existed previously, there are some significant changes under GDPR. The Trust can no longer require a £10 fee for such requests to be processed, and the window for responding to these requests has been shortened to a month.

What this means for you: The waiving of the fee for subject access requests may mean that we see an increase in these requests being made after GDPR goes live.

If you receive a request from a patient for their records, in whatever format, **it must be passed on to the Health Records department immediately: (imperial.accesstohealthrecords@nhs.net)**.

Subject access requests received by a former or current member of staff **must be passed on Human Resources immediately (imperial.hr.queries@nhs.net)**.

You must also be aware that any records and emails about a patient or colleague can form part of the data provided to the requestor, and must be written with the **proper professional conduct**.

4. **Changes to Consent:**

Under GDPR, the requirements surrounding consent become much stricter; consent is required to be freely given in a positive act ("opt-in" consent), and must be specific, fully informed, and unambiguous. It must also be recorded, with an option for the data subject to revoke this consent.

What this means for you:

Consent is not the legal basis for much of the Trust's processing of patient data. For the purposes of direct care the Trust is able to process patient data under the legal basis that processing is necessary for the exercise of the official authority of an NHS Trust.

The requirements around consent for processing data are very stringent under GDPR. You should only rely on consent if this is appropriate to the circumstances and no other legal base applies.

Where consent is required for the processing of data, the requirements for how consent must be captured should be carefully considered, so as not to breach the new regulation.

5. **Records of Processing and Data Protection Assurances:**

Managers need to note that maintaining up-to-date internal records of data processing arrangements and implementing appropriate technical and organisational measures to protect data and privacy are significant requirements under GDPR. This regulation goes further than existing data protection law in that organisations now

have **legal obligations** with regards to records of processing and appropriate data protection measures.

Managers across the Trust have the responsibility to ensure that all processing activities are properly documented and assured; this is called **privacy by default and design** under the GDPR. It will be **mandatory** under GDPR for a Data Privacy Impact Assessment (DPIA) to be undertaken for all high risk processing activities.

What this means for you: Any system which collects and processes personal data within your service **must be recorded** on the Information Asset Register in the first instance. Moreover, managers must ensure that the data protection assurances are in place to ensure that processing is being carried out in a secure and proper manner.

In practical terms, this means liaising with the DPO team to ensure that all the necessary assurances are in place, and with the ICT Applications team to ensure that processing activities are fully and properly recorded in the Trust's systems.

You can begin preparation by:

- Being aware of informational relationships;
- Ensuring that there is a Data Processing Agreement or Data Sharing Agreement in place;
- Being prepared for upcoming information audits to identify undeclared data processing activities;
- Assessing the internal procedures in your team for engaging new suppliers or technologies

The Data Protection Office (DPO) welcomes any further enquiries or advice requests and is contactable at imperial.dpo@nhs.net.