**GDPR preparation (General Data Protection Regulations)**

Page 2 of 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **1** | **Understanding GDPR and governance requirements from 25 May 2018** | | | |
| The General Data Protection Regulation applies to all EU businesses that process personal information, imposing the concept of ‘Data Protection by Design and Default’. It also makes organisations legally accountable for ensuring compliance with data protection law. The **Data Protection Act 2018** will apply the regulation in the UK and introduces UK-specific provisions in some areas such as processing of special category data (“sensitive data” by health professionals - GDPR Article 9(3)). All members that were registered with the ICO under the Data Protection Act 1998 should ensure that they update to comply. | | |  |
| Are decision makers aware of the changes to the law and to the increased level of obligation and risk including financial penalties? |  |  |
| Have you appointed a Data Protection Officer (DPO)? |  |  |
| Is the DPO fully aware of their responsibilities? |  |  |
| Does everyone working in the organisation know who the DPO is? |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **1** | Have you organised an information audit?  To do this, document the personal data that you currently process and maintain a register of data processing activity. You need to know:   * What personal data you hold * Where it came from * Who you share it with * What your lawful grounds are for processing it * How long you retain it for.   The audit should cover both patient and employee personal information. |  |  |  |
| Are the grounds for processing the above information still legitimate? |  |  |
| Is patient consent achieved and evidenced? (Remember, this is not consent to clinical treatment but how you process personal data – see guidance sheet below)  See our guidance sheet here – *Lawful processing including consent* |  |  |
| Do you have in place comprehensive policies to support confidentiality and security of personal information? |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **2** | **Demonstrating compliance with** **SARs** | | | |
| Have you revised your policy for dealing with subject access requests (SARs) which include the GDPR requirements? |  |  |  |
| Do staff have regular training and are they fully aware of their obligations and responsibilities in regard to the above policy? See our guidance sheet here – *Subject access rights* |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **3** | **Demonstrating compliance with data breaches** | | | |
| Do you have a policy in place for breach identification and reporting? |  |  |  |
| Do you have a written breach management plan? |  |  |
| Do you have a log of personal data breaches – including both reported and non-reported breaches to ICO? |  |  |
| Do you have evidence to show you have checked that third party contracts provide guarantees of GDPR compliance for processing your data and have clear responsibilities for data breach reporting? |  |  |
| Have you ensured that all staffare aware of and understand your breach policies? |  |  |
| Do you have evidence that all staff understand their individual responsibilities and liabilities in regard to the above policies? See our guidance sheet here – *Breaches* |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **4** | **Demonstrating compliance with privacy impact assessments** | | | |
| Do you understand the circumstances in which a privacy impact assessment (PIA) would be required? |  |  |  |
| Have you produced a privacy impact assessment template? |  |  |
| Do you know which areas of your practice will require a PIA? |  |  |
| Have you undertaken PIAs as required? |  |  |
| Have the relevant people in your practice been trained and understand when a PIA would be needed and how to use the PIA template? See our guidance sheet here – *Privacy impact assessments* |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Action Points** | **Yes** | **No** | **Action Required** |
| **5** | **Demonstrating compliance with privacy notices** | | | |
| Have you reviewed your current documentation relating to data protection and familiarised yourself with the requirements for privacy notices. |  |  |  |
| Do you have in place clear policies and processes for ensuringthatprivacy notices are up-to-date and accessible to patients and employees? |  |  |
| Can patients and employees access the privacy notices in formats appropriate to them See our guidance sheet here – *Privacy notices* |  |  |