

**IMPORTANT REMINDER – GDPR IS COMING! ALL STAFF MUST READ AND TAKE ACTION WHERE NECESSARY – MUST BE COMPLIANT BY 25TH May 2018**

This new legislation will replace the existing Data Protection Act 1998 and will sit alongside a new Data Protection Act 2018. The legislation covers everything that you do with personal data. It is important that you are aware of what this means to you and your area of work.

Fines for non-compliance are up to €20,000,000 or 4% of international turnover of the organisation

Data protection law covers both patients and staff information and everyone within the organisation will need to ensure compliance.

You need to take action now to ensure compliance in time for May 25TH 2018.

Key points to take account of are listed below, please read and determine which areas may be relevant to your work:

1. **Information you hold**
* Comprehensive records must be kept of all data processing activities – organisation must be *able to show accountability and prove compliance.*
* Organisations must implement appropriate security measures such as policies, staff training, compliance checks
* Data flow mapping and the Information Asset Register must be kept up to date
1. **Individual’s Rights**
* Individual’s rights will be extended:
* Rights of access to data
* To have inaccuracies corrected
* To have information erased where inaccurate
* To prevent direct marketing
* To prevent automated decision-making and profiling
* Data portability
1. **Subject Access Requests**
* Shorter time scale – only 1 month to provide information
* No charges can be made
* More information must be included in the response
1. **Legal Basis for processing personal data**
* Medical purposes condition has been expanded to expressly include health and social care. This applies to treatment and management of services.
* Review legal basis for all processing of staff or patient data – if you are relying on consent you will need to review this (see section 5 below) and ascertain if there is a more appropriate legal basis
1. **Consent – if using as a legal basis for processing data under GDPR**
* Review how you are seeking, obtaining and recording consent – must be recorded
* Must be freely given, specific, informed and unambiguous
* Must be a positive indication of agreement – cannot be inferred from silence, pre-ticked boxes or inactivity
* Must be able to demonstrate that consent was give – effective audit trail
* Individuals have a right to withdraw consent at any time
1. **Children**
* Need to be able to verify individuals’ ages and gather parental or guardian consent if under 13 if anything you do involves contacting children directly
* Gillick/Fraser competency still in place
1. **Data Breaches**
* Duty on all organisations to report certain types of data breach to the relevant authority and in some cases to the individuals affected where the breach is likely to result in a risk to the rights and freedoms of individuals. Important to recognise what is a breach.
* Must notify within 72 hours
* Failure to notify can result in an additional fine of up to €10m or 2% of global turnover
1. **Data Protection by Design**
* Must complete a Data Protection Impact Assessment (Privacy Impact Assessment) for **ALL** new processes, projects and systems that contain personal data
1. **Data Protection Officers**
* All public bodies and organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale must have a Data Protection Officer (DPO) who takes responsibility for data protection compliance
1. **New duties for data processors**
* GDPR places new specific legal obligations on data processors
* Must have contracts in place with all data processors and any organisation that is commissioned to carry out work on behalf of the CCG
* If you have any third parties carrying out work on your behalf you need to ensure there is a contract in place and that it is appropriate
1. **Fair Processing/Privacy Notices**
* Must be transparent and easily accessible and in a concise form
* Must have a separate privacy notice for children where relevant
1. **New ICO Powers**
* Additional fines
* Carry out audits
* Notify data subjects of a breach
* Restrict or erase data

If you are concerned that you may have actions to ensure compliance but need advice and help then please contact the helpdesk: Embed.infogov@nhs.net

The IG team are here to help – if there is anything you are not sure of contact your IG lead or the helpdesk.

**THE CCG MUST BE COMPLIANT WITH THE NEW LEGISLATION BY THE 25TH MAY 2018**