# Information Governance Bulletin

Autumn 2018

## Complying with GDPR

The months leading up to the launch of the new General Data Protection Regulation were extremely busy for CBC, with everyone working hard to ensure everything mandated by GDPR from 25 May 2018 was in place. Since then the Governance Team has continued to work alongside service managers to confirm new GDPR policies and publications have been successfully rolled out and embedded into normal ways of working.

## Data Security and Protection Toolkit (DSPT)

The IG Toolkit has been replaced in 2018/19 by the Data Security and Protection Toolkit (DSPT). The DSPT has been designed to be easier to use and with a simpler format, in response to feedback from a wide range of users. The toolkit also enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.

The new toolkit reflects current legislative and policy requirements for protecting patient data. CBC (and its practices separately) is required to publish an assessment using the new toolkit by 31 March 2019

## Data Protection Impact Assessments (DPIA)


A Data Protection Impact Assessment (DPIA) is a process used to help identify and analyse data processing to minimise data protection risks. DPIAs are a legal requirement under GDPR for any data processing which involves the use of personal identifiable information (PID), that is likely to be a high risk to individuals, or for any project involving the processing of personal data. This process is also a mandated requirement of the Data Security & Protection Toolkit.

A DPIA must be completed, as soon as identified, by the Information Asset Owner (IAO). A screening checklist is available to help decide when an impact assessment needs to be done. See the updated DPIA procedure - copy available from the governance team, cbchealth.governance@nhs.net.

### Submitting a DPIA

Completed assessments should be returned to cbchealth.governance@nhs.net and will be reviewed by the Quality and Governance Manager and SIRO.

**Note: Non-compliance with DPIA requirements can lead to fines imposed by the ICO.**

## Information Governance Mandatory Training

Please ensure you are up to date with all your statutory and mandatory training. This includes information governance and the relevant GDPR module. CBC (and its practices separately) is required to provide evidence of compliance for the Data Security and Protection Toolkit which will be submitted by the end of March 2019. In our efforts to avoid this being a last minute endeavour, we would appreciate it if all staff would check when their Information Governance and GDPR training is due, and would request that any training that is due during March 2019 is undertaken **as soon as practically possible**, **preferably by the end of February if this is feasible, or as early in March as you can.**

Thank you all in advance for your co-operation in this matter. This will allow us to gather certificates in a timely manner, to demonstrate compliance with this requirement.

# Data Security and Protection (IG) Incidents – GDPR implications

Under GDPR we are required to notify data security and protection incidents (personal data breaches) to the Information Commissioner's Office within *72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. There is also a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a Risk to individuals' rights and freedoms.

**All staff** (employed or sessional) are responsible for reporting incidents they are involved in or become aware of **without undue delay**, using the process set out in the Complaints & Incident Management procedure

## Whose responsibility is it to report data breaches to the ICO?

Responsibility has been assigned to key members of staff in each CBC service/practice who have access to report data breaches to the ICO through the DSP Toolkit. Where the 72 hour deadline is not met we must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

## *Practice staff only*

In the first instance please report data security and protection incidents to CBC's Quality & Governance Team without delay. These will be fielded to the relevant service manager for investigation and onward reporting to the ICO if relevant. The Practices Division service manager will inform you whether the incident needs to be reported locally via SIRMS.

* 72 hours starts when we **become aware** of the breach which may not necessarily be when it occurred.

# Case Studies: Consequences of data protection breaches

*In September a former nurse at Southport and Ormskirk Hospital NHS Trust was prosecuted for accessing patients' medical records without authorisation. She was fined £400 and was also ordered to pay costs of £364.08 and a victim surcharge of £40.*

Please be aware accessing medical records without a legal basis to do so is a crime.

*Bupa was fined £175,000 for failing to have effective security measures in place to protect customers' personal information.*

A failure to keep personal data secure is a breach of the GDPR & Data Protection Act 2018.

Fines issued by the Information Commissioner's Office can be severe for an organisation. CBC has measures in place to routinely monitor activity in order to detect and act upon anything unusual. An access control audit is also carried out on an annual basis.

Please ensure you keep your passwords safe and never share them with anyone under any circumstances.

# Key IG Contacts

**Kate Watson**
**Quality and Governance Facilitator**
**Data Protection officer**

Tel: 0191 497 7710
Email: kate.watson2@nhs.net

Cbchealth.governance@nhs.net (for sending and receiving information relating to complaints and incidents.

**Liz Orr, Quality & Governance Manager**
Tel: 0191 497 7718
Email: elizabethorr@nhs.net

October 2018