

**Agenda Item:19.0**

<h2 style="margin: 0;"><b>Governing Body</b></h2> <h3 style="margin: 0;"><i>held in public</i></h3>	<h2 style="margin: 0;"><b>Report</b></h2> <p style="margin: 0;">Date of Meeting: 25 January 2018</p>
-----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

<b>Report Title</b>	General Data Protection Regulations 2018		
<b>Report Author</b>	<b>Presented By</b>	<b>Responsible Director</b>	
<u>David McNeil</u>	<i>Jim Hayburn, Chief Finance Officer</i>	<i>Jim Hayburn, Chief Finance Officer</i>  <b>Signature:</b> <i>Approved by email</i>	
<b>Purpose for presenting report</b>	<i>This report outlines the proposals for the CCG's response to new data protection officer responsibilities</i>		
<b>Action Required:</b>	To give assurance		
<b>Approval Route:</b>	NA		
<b>Further Assurance:</b>	NA		
<b>Which Strategic Objectives does this report provide evidence for?</b>			<b>Please Tick</b> √
We will commission high quality, safe and sustainable models of care that deliver effective clinical outcomes and patient experience using evidence based decisions and best practice			
We will ensure that there is a financially sustainable and affordable healthcare system in Bedfordshire.			
We will lead, engage and operate as an effective place based and STP wide system partner to achieve greater integration of care delivery.			√
We will support local people and stakeholders to have an influence on services we commission to ensure our decisions are informed and shaped by local views and insights.			
We will operate and manage our Governing Body to the highest standards of accountability and transparency.			
<b>Implications/Assessments</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>
Have any financial implications been signed off by the Chief Finance Officer?	√		
Have any quality implications been signed off by the Director of Nursing & Quality?			NA
Have any privacy implications been signed off by the Head of Information Governance?			NA
Have any conflicts of interest implications been signed off by the Corporate Office?	√		
Have any public engagement implications been signed off by the Head of Communications & Engagement?			NA
Has an Equality Impact Assessment been carried out?		√	
<b>Key Risks</b>	<i>Risk of being not compliant with GDPR regulations</i>		
<b>Executive Summary</b>	The General Data Protection Regulations (GDPR) 2018 will replace the Data Protection Act 1998 in May 2018. The Regulations specify organisations should formally designate a		

Data Protection Officer (DPO). An organisation must designate a DPO if they are:

- A public authority (except for courts acting in their judicial capacity)
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- An organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

*GB are asked to note:*

- the requirement to review the contract with LCCG and NHSE
- that BCCG will need to recruit to this role in readiness for GDPR in May 2018

<b>Governing Body</b>	<b>25 January 2018</b>
<b>Presented by</b>	<b>Jim Hayburn, Chief Finance Officer</b>

**Agenda item: 19.0**

## **General Data Protection Regulations 2018**

### **Role of Data Protection Officer (DPO)**

#### **Introduction**

The General Data Protection Regulations (GDPR) 2018 will replace the Data Protection Act 1998 in May 2018. The Regulations specify organisations should formally designate a Data Protection Officer (DPO). An organisation must designate a DPO if they are:

- A public authority (except for courts acting in their judicial capacity)
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- An organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

#### **Position of the DPO**

The DPO will provide advice and support to the CCGs Executive Board in relation to data protection. Support the CCG's Caldicott Guardian and Senior Information Risk Owner (SIRO) to enable the Trust to adhere to all regulations and standards particularly in relation to the General Data Protection Regulations. This role is advisory and is not accountable. The Accountable Officer has overall accountability and responsibility for Information Governance and is required to provide assurance through the Statements on Internal Control that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

#### **Data Protection Officer Responsibilities**

At a high level, the key result area is to ensure that the organisation can demonstrate compliance with all the requirements of the GDPR. Key components of this include, but are not limited to:

- policies and procedures that comprehensively address the requirements of the GDPR, and that are available and current
- privacy notices are fit for purpose, up to date, and signpost to procedures that address subjects' rights under the GDPR
- a database that holds and can provide on request details of all processing activities with the data required by the GDPR
- evidence that privacy by default and design principles are incorporated in all processing
- evidence that data protection impact assessments are conducted in appropriate circumstances, and that their conclusions mitigate risk and are assured

- routine documented reports to the [highest management level] on the organisation’s state of compliance.

The Governing Body of the CCG has responsibility for the Information Governance agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, and IG Lead.

The CCG has specific responsibilities in relation to the DPO as mandated in the GDPR Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is “involved, properly and in a timely manner, in all issues which relate to the protection of personal data”.

It is crucial the DPO is involved from the earliest stage possible in all issues relating to data protection. In addition, it is important that the DPO be seen as a discussion partner within the organisation and that they are part of the relevant working groups dealing with data processing activities within the organisation.

Consequently, the organisation should ensure for example, that the DPO is invited to participate regularly in meetings of senior and middle management.

#### **Instructions and “performing their tasks in an independent manner”**

Article 38 (3) establishes some basic guarantees to help ensure that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organisation. This means that in fulfilling their tasks under Article 39, DPOs must not be instructed how to deal with a matter, for example, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain issue related to data protection law, for example a particular interpretation of the law.

#### **Dismissal or penalty for performing DPO tasks**

Article 38(3) requires that DPOs should “not be dismissed or penalised by the controller or the processor for performing their tasks”. This requirement strengthens the autonomy of DPOs and helps ensure that they act independently and enjoy sufficient protection in performing their data protection tasks.

#### **Monitoring compliance with the GDPR**

Article 39(1)(b) entrusts DPOs, among other duties, with the duty to monitor compliance with the GDPR.

#### **Other NHS organisations**

The role of DPO has been allocated to either:

- The current Head of Information Governance
- Director of Informatics (if one is in place)

#### **Current position at BCCG**

Currently BCCG provide this work under contract to LCCG and NHSE. The current post holder will retire in March. This means that the CCG will have to review current contract arrangements with LCCG and NHSE to supply this service and recruit a new member of staff to this role.

<b>Recommendation</b>
-----------------------

The CCG are asked to

- note the requirement to review the contract with LCCG and NHSE
- note that BCCG will need to recruit to this role in readiness for GDPR in May 2018.