Information Governance Bulletin

Spring 2018

Contracts and Liabilities

It's not long now until the introduction of the General Data Protection Regulation (GDPR) on 25 May 2018. The regulation introduces some new obligations in relation to legal agreements, which means we need to ensure that contracts and liabilities between controllers and processors are updated to ensure they are GDPR compliant. The main difference under GDPR is *data processor liability when acting outside a contract.*

Identifying and recording agreements

The Quality and Governance Team are in the process of identifying the agreements we have in place along with their date of review/how frequently they are reviewed and updated. Details will be held in a central log. Please check the attached spreadsheet and let us know the details of any not currently recorded.

Update guidance

Information Governance clauses will need to be reviewed and updated to include:

- The obligation to notify personal data breaches to the Information Commissioner's Office within 72 hours (in line with Article 33).
- Data processors' responsibility to notify any personal data breaches to the data controller 'without undue delay'.
- The obligation of processors to assist you to advise data subjects when there has been a personal data breach (in line with Article 34).

You must also check with data processors who their Data Protection Officer is – we need this info for the Information Asset Register.

See the attached information to help with your reviews. However please do not hesitate to contact Kate in her capacity as Data Protection Officer should you require any further advice. The information attached contains some useful checklists to ensure that all necessary information is included in your contract IG clauses.

Something to consider

Where other organisations produce and control the documentation – have you contacted them to ensure they are undergoing the same scrutiny and update to meet GDPR compliance?

Data Protection Impact Assessments (DPIA)

Under GDPR it is mandatory to carry out a DPIA for any new/changes in services, systems or processes which pertain to utilise personal identifiable information. It must be completed, as soon as identified, by the Information Asset Owner (IAO). This process is also a mandated requirement of the IGT to ensure that privacy and data protection concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

Guidance

The ICO are conducting a review of their DPIA guidance to ensure GDPR compliance, and this is expected to be available in April 2018. Our procedure will be updated in line with the new guidance, and will be issued ahead of GDPR coming into force. Until it is updated please use the attached version.

The Information Commissioner's Office (ICO)

In some instances where a high level of risk is identified and cannot be fully mitigated, the ICO will need to be notified for a decision to proceed. It is unlikely we would proceed with anything that poses such a high level of risk however we need to make you aware this is also a mandated requirement under new data protection law.

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.

Information Asset Register

CBC's Information Asset Register (IAR) allows us to understand what data we process, the legal basis for processing it, where the data comes from, where and how it is stored, who has access to it, who it is shared with and how, and what our legal basis is for sharing it, along with the security measures we have in place to protect it.

We'd like to take this opportunity to thank Information Asset Owners for their contribution to the development of the IAR. The register has been reviewed by the Governance Board and separately by the Senior Information Risk Owner who are happy that it demonstrates compliance with data protection law and it will be submitted with the annual Information Governance Toolkit.

Register Maintenance

Review of the register will take place annually, co-ordinated by the Quality and Governance Team, however, changes to assets or new assets should be updated/recorded as they happen.

Links to Information Asset Register and Corporate Risk Register

Any changes to existing assets or new assets should be recorded on the Information Asset Register. Any significant risks should be flagged to check whether they need to be recorded on the corporate risk register – those with a risk rating of 15 or above.

Door Entry System – Queens Park

The door entry system to Queens Park has changed. From 21 March 2018 staff will no longer be able to enter using their fingerprint. If you require a card or fob please contact Sue Hall: suzannehall@cbchealth.co.uk, 0191 497 7710.

We would like to assure you that your fingerprint will be permanently deleted with immediate effect.

Key IG Contacts

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

Kate Watson, Quality and Governance Facilitator
Tel: 0191 497 7710
Email: kate.watson2@nhs.net

Or cbchealth.governance@nhs.net