The Dudley Group
NHS Foundation Trust

Date: 18/06/2018

FREEDOM OF INFORMATION REQUEST FOI/014155 - GDPR

1.Have you invested in technology specifically to comply with GDPR?
No

2.Which information security framework(s) have you implemented?
ISO27001 and Cyber Essentials. The Trust is working towards Cyber Essentials Plus.

3. Have you signed contractual assurances from all the third-party organisations you work with requiring that they achieve GDPR compliance by 25 May 2018?
The Trust wrote to the third party organisations it works with requesting assurance that they achieve GDPR compliance by 25th May 2018.
The Trust is receiving the assurance from these organisations.

4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?
Yes

5. Do you use encryption to protect all PII repositories within your organisation?
FOI Exemption 43 Commercial Interest (release of the information could potentially damage The Trust's business reputation and/or the confidence that customers, suppliers or investors may have in it). Cyber-attacks against infrastructure have the potential to inflict significant, real-life disruption and prevent access to critical services that are vital to the functioning of Trust systems. It is imperative that the Trust is cyber resilient in the face of growing and sophisticated cyber threats. The certification the Trust publishes (ISO27001, Cyber Essentials) is more high level assurance that we work to a certain standard.

6. As part of this audit, did you clarify if PII data is being stored on, and/or accessed by:
a. Mobile devices
b. Cloud services
c. Third party contractors
Yes, under review of systems

7. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?
Yes

8. Does your organisation employ controls that detect the security posture of a device before granting access to network resources – i.e. valid certificates, patched, AV protected, etc.
FOI Exemption 43 Commercial Interest (release of the information could potentially damage The Trust's business reputation and/or the confidence that customers, suppliers or investors may have in it). Cyber-attacks against infrastructure have the potential to inflict significant, real-life disruption and prevent access to critical services that are vital to the functioning of Trust systems. It is imperative that the Trust is cyber resilient in the face of growing and sophisticated cyber threats. The certification the Trust publishes (ISO27001, Cyber Essentials) is more high level assurance that we work to a certain standard.

9. Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?
Yes

10. Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?
No