St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	032210518
From:	Commercial
Date:	21/05/18
Subject:	GDPR and Security

REQUEST & RESPONSE

If this request is too wide or unclear, I would be grateful if you could contact me as I understand that under the Act, you are required to advise and assist requesters. If any of this information is already in the public domain, please can you direct me to it, with page references and URLs if necessary?

I understand that you are required to respond to my request within the 20 working days after you receive this letter. Answers will be anonymised upon receipt.

1. Have you invested in technology specifically to comply with GDPR?

   No

2. Which information security framework(s) have you implemented?

   We have successfully implemented Cyber Essentials and are fully compliant with all the elements of the Information Governance Toolkit (now DSPT).

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?

   This programme of work has commenced in line with our General Data Protection Regulation action plan.

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

   This programme of work has commenced in line with our General Data Protection Regulation action plan.

5. Do you use encryption to protect all PII repositories within your organisation?

   Yes

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

   This programme of work has commenced in line with our General Data Protection Regulation action plan.

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.

   Yes

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

11. To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.

SIRO