Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI/LHCH/2018/134
From: Commercial

Date: 17 May 2018

Subject: GDPR implementation

Q1 Have you invested in technology specifically to comply with GDPR?

A1 No

Q2 Which information security framework(s) have you implemented?

A2 We have a local Information Security Management System in place; two employees who have CISSP qualifications and are working towards full compliance with Cyber Essentials requirements.

Q3 Have you signed contractual assurances from all the third-party organisations you work with requiring that they achieve GDPR compliance by 25 May 2018?

A3 No

Q4 Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?

A4 Yes

Q5 Do you use encryption to protect all PII repositories within your organisation?

A5 Yes

Q6 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

A6

a. Yes
b. Yes
c. Yes

All the above is sought via our Data Protection Impact Assessment process.

Q7 Does the organisation employ controls that will prevent an unknown device accessing PII repositories?

A7 Yes

Q8 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.

A8 Yes

Q9 Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?

A9 Yes

Q10 Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?

A10 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency; however the factors against release clearly outweigh this as release of the information would place the Trusts at risk of potential cyber-attack if released in to the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Q11 To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.

A11 The Trust Board