

Ref: FOI/GS/ID 4746

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ

Email: mtw-tr.foiadmin@nhs.net

06 July 2018

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to GDPR.

You asked:

- 1. Have you invested in technology specifically to comply with GDPR?*
 - ☐ Yes*
 - ☐ No*
- 2. Which information security framework(s) have you implemented?*
- 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?*
 - ☐ Yes*
 - ☐ No*
- 4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?*
 - ☐ Yes*
 - ☐ No*
- 5. Do you use encryption to protect all PII repositories within your organisation?*
 - ☐ Yes*
 - ☐ No*
- 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*
- 7. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?*
 - ☐ Yes*
 - ☐ No*
- 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*

o No

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

o Yes

o No

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

o Yes

o No

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

Trust response:

1. No

2. Not applicable.

3. Yes

4. Yes

5. 6. 7 & 8.

The information which has been withheld is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (<https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf>) run as follows:

31.—(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.

9. Yes

10. No

11. Chief Executive