The Tavistock and Portman NHS
NHS Foundation Trust

Freedom of Information Act 2000 disclosure log entry

Reference

18-19067

Date sent

19/06/2018

Subject

GDPR Preparations

Details of enquiry

1. Have you invested in technology specifically to comply with GDPR?
    - Yes
    - No
2. 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
3. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?
    - Yes
    - No
4. Do you use encryption to protect all PII repositories within your organisation?
    - Yes
    - No
5. 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
6. Does the organisation employ controls that will prevent an unknown device accessing PII repositories?
    - Yes
    - No
7. 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
    - No
8. Should PII data be compromised, have you defined a process so you can notify the relevant supervisory authority within 72 hours?
    - Yes
    - No
9. Have you ever paid a ransom demand to have data returned / malware (aka ransomware) removed from systems?
    - Yes
    - No
10. To which positions/level does your data protection officer report? i.e. CISO, CEO, etc.

Response Sent

1. Have you invested in technology specifically to comply with GDPR?
    - Yes, on incidents management only
2. Which information security framework(s) have you implemented?
    - NHS Information Security Management Code of Practice
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
    -
4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?
    - Yes, (GDPR Contract Variation)
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:
    - Cloud services only
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.
    - Trust Board