South East Coast Ambulance Service NHS
NHS Foundation Trust

South East Coast Ambulance Service NHS
Foundation Trust
Nexus House
Gatwick Road
Crawley
RH10 9BG

Email:foi@secamb.nhs.uk

Date 13th June 2018

Email:

Dear,

I am writing in response to your enquiry under the Freedom of Information Act 2000 (FOIA) reference FOI/18/05/25.

You requested the following information, please also see our response below:

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

2. Which information security framework(s) have you implemented
The Trust has a robust information security framework in place, which is underpinned by an Information Security Policy. The Trust has a variety of software tools in place to protect its network such as anti-virus, ransom wear protection and undertakes security patching. We also undertake penetration testing on an annual basis to ensure the security of our systems. There is also a team in place, which reviews, and if necessary acts on CareCert alerts.

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?
We are currently in the process of doing this at the moment.

4. Have you completed an audit to identify all files or databases that include personally identifiable information (PII) within your organisation?
Yes - The Trust has a functioning Information Asset Register, which records the information assets in place. It is also currently undergoing an organisation wide records review which will be completed during 2018

5. Do you use encryption to protect all PII repositories within your organisation?
No

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

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 – All IG breaches are reported to the Information Governance Lead who will review, grade and report the incident to the regulatory authority within statutory timeframes if relevant.

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.
The Information Governance Lead is the nominated Data Protection Officer for the Trust. They report directly to the Head of Compliance / Executive Director of Nursing and Quality

I hope you find this information of some assistance.

If for any reason you are dissatisfied with our response, kindly in the first instance contact Caroline Smart, Information Governance Manager via the following email address:

FOI@secamb.nhs.uk

Yours sincerely

Freedom of Information Coordinator
South East Coast Ambulance Service NHS Foundation Trust