East London
NHS Foundation Trust

Information Governance
The Green
1 Roger Dowley Court
Russia Lane
London
E2 9NJ

Email elft.foi@nhs.net
Website: https://www.elft.nhs.uk

26 October 2021

Our reference: FOI DA3932

I am responding to your request for information received 31 August 2021. I am sorry for the delay in responding to your request. This has been treated as a request under the Freedom of Information Act 2000.

I am now enclosing a response which is attached to the end of this letter. Please do not hesitate to contact me on the contact details above if you have any further queries.

Yours sincerely,

K Harvey

Keshia Harvey
Information Governance Manager

If you are dissatisfied with the Trust's response to your FOIA request then you should contact us and we will arrange for an internal review of this decision.

If you remain dissatisfied with the decision following our response to your complaint, you may write to the Information Commissioner for a decision under Section 50 of the Freedom of Information Act 2000. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113
Web: www.ico.org.uk

Please note that the data supplied is not allowed to be re-used and/or published without the explicit consent of East London NHS Foundation Trust. Please contact the signatory to request permission if this is your intention

Request:

I am writing to you under the Freedom of Information Act 2000 to request the following information from East London NHS Foundation Trust. Please can you answer the following questions:

Question 1. In the past three years has your organisation:

a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)

i. If yes, how many?

b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

c. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)

d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?

i. If yes was the decryption successful, with all files recovered?

e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?

i. If yes was the decryption successful, with all files recovered?

f. Had a formal policy on ransomware payment?

i. If yes please provide, or link, to all versions relevant to the 3 year period.

g. Held meetings where policy on paying ransomware was discussed?

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation

i. If yes at what cost in each year?

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

j. Requested central government support for malware, ransomware, or system intrusion investigation?

k. Paid for data recovery services?

i. If yes at what cost in each year?

l. Used existing contracts for data recovery services?

m. Replaced IT infrastructure such as servers that have been compromised by malware?

i. If yes at what cost in each year?

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?

i. If yes at what cost in each year?

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?

i. If yes how many incidents in each year?

Answer: The Trust has reviewed question 1 of your request for information, Section 1(1) of the Freedom of Information Act 2000 states:

Any person making a request for information to a public authority is entitled—
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
(b) if that is the case, to have that information communicated to him.

East London NHS Foundation Trust has not had any ransomware incidents and does not hold the information requested and it is therefore not disclosable.

Question 2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?

a. If yes is this system's data independently backed up, separately from that platform's own tools?

Answer: The Trust uses Office 365 as part of the nhs.net shared tenancy which does not use independent backups.

Question 3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

a. Mobile devices such as phones and tablet computers

Answer: Yes

b. Desktop and laptop computers

Answer: No

c. Virtual desktops

Answer: No

d. Servers on premise

Answer: Yes

e. Co-located or hosted servers

Answer: Yes

f. Cloud hosted servers

Answer: Yes

g. Virtual machines

Answer: Yes

h. Data in SaaS applications

Answer: Yes

i. ERP / finance system

Answer: Not applicable.

j. We do not use any offsite back-up systems

Answer: No

Question 4. Are the services in question 3 backed up by a single system or are multiple systems used?

Answer: Multiple.

Question 5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

Answer: Yes.

Question 6. How many Software as a Services (SaaS) applications are in place within your organisation?

a. How many have been adopted since January 2020?

Answer: Approximately 20-30.