Essex Partnership University
NHS Foundation Trust

Freedom of Information Request

Reference Number: EPUT.FOI.23.2798
Date Received: 16th of January 2023

Information Requested:
1. What was the total number of cyber-attack incidents that have been recorded in your trust in the past 24 months?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

2. What is the classification of your policy regarding breach response?
The breach response policy is classified as a Corporate Policy. Incidents are classified during the breach response process.

3. Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, and Windows XP?
This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

4. What are the top 20 cyber security risks in your Trust, and how are they managed?
This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still Identified/managed.

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows, Windows XP)?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

7. What is your current status on unpatched Operating Systems?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

8. Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, and Windows 2022?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?

Yes we utilise secure boundaries however we believe further details is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

10. Does your Trust hold a cyber-insurance policy? If so:
a. What is the name of the provider?
b. How much does the service cost?
c. By how much has the price of the service increased year-to-year over the last three years?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

11. When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?

The Executive Team and NEDs are provided with regular updates via reporting channels and scheduled committee meetings. Training is provided on an annual basis with cyber-certified professionals via face to face sessions and the Trust's mandatory training requirements. Regular staff communications are also provided via the weekly staff communication channels.

12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?

Yes

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

There have been zero staff members let go specifically as a result of cyber security governance.

14. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

None

15. Are there mandatory minimum training requirements for those transferred internally to work in cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

All Cyber security staff are expected to gain a relevant qualification that relates to their role, ranging from CompTIA through to CISSP. Those with the more advanced qualifications keep updated by means of gaining CPE credits to keep abreast of Cyber and ensure certifications can be renewed.

16. How much money is spent by your Trust per year on public relations related to cyber-attacks? What percentage of your overall budget does this amount to?

£0.
The Trust's communications team raises awareness of cyber security to staff via internal communication activities.
The Trust does not carry out external communications related to cyber-attacks.
Occasionally the trust includes awareness raising messaging in internal news and all staff bulletin (Wednesday Weekly) on the back of national campaigns from NHS Digital and the National Cyber Security Centre.

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?

We do not have a Chief Information Risk Officer, however in place we do have a Senior Information Risk Officer (SIRO) as a requirement laid out by the DSPT. Supporting our SIRO we have a Chief Information Officer (CIO) who reports to the SIRO and a Deputy Chief Information Officer who reports to the CIO.

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?

Last Audit completed in Aug 22 – Audits undertaken annually.

19. What is your strategy to ensure security in cloud computing?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust

services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

20. Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System /Application, and the total spend for enhanced support?

This information is exempt under Section 31 (1a) of the Freedom of Information Act as disclosure would, or would be likely to, prejudice the prevention or detection of crime.

Essex Partnership NHS Foundation Trust believe that releasing this information would enable cyber criminals to identify and take advantage of any weaknesses within the security of trust services. This would put patient & trust information at risk, including clinical, financial, and sensitive personal data. We therefore apply section 31(1)(a). Section 31 is a qualified exemption, so we have considered the public interest, but we believe that on this occasion the risk to data outweighs the public interest in cyber security concerns.

Section 31

31 Law enforcement.

(1)Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a)the prevention or detection of crime,

(b)the apprehension or prosecution of offenders,

(c)the administration of justice,

(d)the assessment or collection of any tax or duty or of any imposition of a similar nature,

(e)the operation of the immigration controls,

(f)the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained,

(g)the exercise by any public authority of its functions for any of the purposes specified in subsection (2),

(h)any civil proceedings which are brought by or on behalf of a public authority and arise out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment, or

(i)any inquiry held under the **[F1**Inquiries into Fatal Accidents and Sudden Deaths etc. (Scotland) Act 2016**]** to the extent that the inquiry arises out of an investigation conducted, for any of the purposes specified in subsection (2), by or on behalf of the authority by virtue of Her Majesty's prerogative or by virtue of powers conferred by or under an enactment.

(2)The purposes referred to in subsection (1)(g) to (i) are—

(a)the purpose of ascertaining whether any person has failed to comply with the law,

(b)the purpose of ascertaining whether any person is responsible for any conduct which is improper,

(c)the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise,

(d)the purpose of ascertaining a person's fitness or competence in relation to the management of bodies corporate or in relation to any profession or other activity which he is, or seeks to become, authorised to carry on,

(e)the purpose of ascertaining the cause of an accident,

(f)the purpose of protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

(g)the purpose of protecting the property of charities from loss or misapplication,

(h)the purpose of recovering the property of charities,

(i)the purpose of securing the health, safety and welfare of persons at work, and

(j)the purpose of protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3)The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Publication Scheme:

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT's Publication Scheme is located on its Website at the following link https://eput.nhs.uk