Essex Partnership University
NHS Foundation Trust

Freedom of Information Request

Reference Number: EPUT.FOI.21.2009
Date Received: Legal Team

Information Requested:

1. How many cyber-attacks (incidents) did your organisation experience in the last 3 years?

2. If these statistics are available within the cost limit, how many of those incidents involved a) Malware b) Ransomware c) Hacking d) Phishing emails

3. How many incidents over the last 3 years were reported to the Department of Health and Social Care, whether under the Security of Network and Information Systems Regulations 2018, or otherwise?

4. How many incidents over the last 3 years resulted in a notification to the Information Commissioner's Office?

5. How many incidents over the last 3 years were reported to both DHSC and the ICO?

Response:

The NHS Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA.

S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

Factors in favour of confirming or denying the information is held
The NHS Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the NHS Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The NHS Trust recognises that answering the request would promote openness and transparency with regards to the NHS Trust's ICT security.

Factors in favour of neither confirming nor denying the information is held
Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The NHS Trust, like any organisation, may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the NHS Trust considers that confirming or denying whether the requested information is held would provide information about the NHS Trust's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the NHS Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.
If the NHS Trust were ether to confirm or deny the existence of the requested information, the disclosure would be likely to prejudice, the effective conduct of public affairs for the Trust, the NHS or any other government department(s) and as such conflicts with Section 36(2c) of the FOIA. The full wording of section 36 can be found here: https://www.legislation.gov.uk/ukpga/2000/36/section/36

Balancing the public interest factors
The NHS Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extend the NHS Trust is able to detect and deal with ICT security attacks. The NHS Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the NHS Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the NHS Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the NHS Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the NHS Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the NHS Trust's ICT systems

---

Applied Exemption:

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