Freedom of Information Request: Our Reference CTMUHB_437_23

You asked:

I would like to submit the below FOI request to your NHS board:

1. **In 2023, what annual cybersecurity budget has been allocated to your NHS Trust?**

   No central budget allocated.

2. **Can you also provide your Trust's annual cybersecurity budget for the years:**

   a. **2022**
   b. **2021**
   c. **2020**
   d. **2019**
   e. **2018**
   f. **2017**

   Cyber security is funded from the ICT budget, and we do not hold this information in the format requested or that can be easily extracted.

3. **In 2023, how is your annual cybersecurity budget spent:**
   a. **What percentage goes towards cybersecurity training for employees?**
   b. **What percentage goes towards technology investments?**
   c. **What percentage goes towards employee resources for your cybersecurity team?**

   In accordance with the Freedom of Information Act 2000, this acts as a Refusal Notice under section 17 of the Act.

   Cwm Taf Morgannwg University Health Board has deemed that the information requested is exempt from disclosure under Section 31(1)(a) and Section 38(1)(a)&(b) of the Freedom of Information Act 2000 (the Act).

   The University Health Board (UHB) recognises its duty to protect the public and individuals, and we will not jeopardise this duty by providing this information. In our opinion, this would weaken our ability to protect our patients, staff and other service users. We have also considered the harm which will or will be likely to arise from the release of this information along with information already in the public domain.

   Section 31(1)(a) of the Act provides that information which is not exempt by virtue of Section 30 (criminal investigations and proceedings) is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime. In guidance, the Information Commissioner's Office has advised that Section 31 amongst other things, prevents information being disclosed that would increase the risk of the law being broken. In addition, it can be claimed by any public authority.

Revealing cybersecurity details into the public domain would make this information accessible to criminals and cyber terrorists and subsequently compromise public and individual safety.

Section 38(1)(b) – endanger the safety of any individual. Providing this information could enable cyber criminals to gain knowledge about the Health Boards capabilities and IT security measures, and this could enable them to plan attacks where they perceive a lower level of security resource exists. This exposes our IT systems to greater risk and therefore, constitutes a risk to both public and staff, as our systems are used to provide patient care.

The UHB is relying upon these exemptions as it considers that releasing this information about our IT systems, would in the present climate, make it more vulnerable to crime.

Section 31 – Law Enforcement of the Act states that:

31(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

Section 38 – Health and Safety of the Act – states that:

38(1) Information is exempt information if its disclosure under this Act would, or would be likely to –
(a) endanger the physical or mental health of any individual, or
(b) endanger the safety of any individual.
(2) 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, have either of the effects mentioned in subsection (1).

Therefore, the UHB considers that the public interest in withholding the information outweighs any arguments for disclosure, therefore protecting the Health Board from potential criminal activity.

4. How many employees work in your NHS Trust?

c14,000 staff.

5. How many employed, full-time members of staff make up your NHS Trust's cyber/infosecurity team?
6. How many hours of cybersecurity training are employees of your NHS Trust required to undertake every year?
7. Has your NHS Trust paid any ransom demands to cybercriminals in the last five years?
   a. If yes, how much did you pay in total?
8. Has your NHS Trust had any patient records compromised / stolen by cybercriminals in the last five years?
   a. If yes, how many records were compromised / stolen?

5 – 8. Please see response to question 3.