File reference	W17FoI434
Key words	Cybersecurity
Date of release	07/09/2017
Attachments	No

Freedom of Information Act Disclosure log - Reply Extract

You asked

I am interested in the cybersecurity arrangements at NHS Trusts and wish to request the following information under the Freedom of Information Act 2000.

The following questions relate to information technology systems operating within your Trust. The term 'clinical systems' used below includes for example those that permit access to viewing patient images and scans, patient notes, patient laboratory reports etc. and also those that permit access to the Trust's network and computer terminals for clinical purposes. Please answer the questions for the situation on the date of receipt of this request for information.

It would be appreciated if responses could begin with the one- or two-word options given in square brackets at the end of each question, followed by any explanatory text that may be felt appropriate.

1. Do the Trust's clinical systems share username and password combinations? [Yes, all/Yes, some/No]
2. For clinical systems, are users required to change their passwords at pre-defined regular intervals? [Yes, all/Yes, some/No]
3. For clinical systems, are minimum requirements set regarding users' passwords' composition e.g. mandating that they containing 'special' characters, contain upper and lowercase letters or contain numbers and letters (please do not include rules regarding password length in this answer)? [Yes, all/Yes, some/No]
4. For clinical systems, are minimum length requirements set regarding users' passwords e.g. that they must be more than a pre-specified number of characters? [Yes, all/Yes, some/No]
5. For clinical systems, are maximum length requirements set regarding users' passwords e.g. that they must be less than a pre-specified number of characters? [Yes, all/Yes, some/No]
6. Are users provided with an indicator of password strength when they are choosing passwords for clinical systems? [Yes, all/Yes, some/No]
7. For clinical systems, are passwords checked against published databases of known compromised passwords e.g. those available at haveibeenpwned.com? [Yes, all/Yes, some/No]
8. For clinical systems, are passwords stored as plain text? [Yes, all/Yes, some/No]
9. For clinical systems where passwords are stored hashed, are password hashes salted? [Yes, all/Yes, some/No/Not applicable]
10. For clinical systems, when incorrect passwords are entered, do further attempts eventually result in either throttling of further access attempts or account lock-out? [Yes, all/Yes, some/No]

11. For clinical systems, when users log in successfully, are they shown details of recent logins to that account? [Yes, all/Yes, some/No]
12. For clinical systems with web browser based interfaces, is login compatible with password management software (for example 1Password or Last Pass)? [Yes, all/Yes, some/No]
13. For clinical systems, does the Trust employ two-factor authentication? [Yes, all/Yes, some/No]
14. Does the Trust provide access to clinical systems from outside Trust premises e.g. using virtual private network technology? [Yes/No]
15. Is access to clinical systems from outside the Trust premises restricted to Trust-owned devices? [Yes/No/Not applicable]
16. Does access to the Trust's network from outside Trust premises require two-factor authentication? [Yes, all/Yes, some/No/Not applicable]
17. For devices with access to the Trust's network, are manufacturers' passwords changed from default on installation? [Yes, all/Yes, some/No]
18. Do users of the Trust's clinical systems receive specific training on cybersecurity in general? [Yes, all/Yes, some/No]
19. Do users of the Trust's clinical systems receive specific training in choosing and maintaining appropriate passwords? [Yes, all/Yes, some/No]
20. Do users of the Trust's clinical systems receive specific advice not to share passwords between clinical systems and other accounts? [Yes, all/Yes, some/No]

Our response

Beyond the information published on the Trust's website, we are not able to provide further information. Please refer to our legal statement as exemptions apply to the questions you have asked.

Our legal statement relating to the use of exemptions

Introduction

Section 31 and 38 apply to all of the questions you have asked. We are sorry that we cannot be more helpful, but trust that you will understand our approach in light of the risks associated with responding, particularly in light of recent national news events about cybercrime.

We have for some time adopted a similar approach to all requests about our integrated network security and believe this is necessary in maintaining the highest levels of security.

Exemptions applied

Section 31.-(1) (a) the prevention or detection of crime applies, as does 31.-(3) neither confirming nor denying we hold the information requested.

Section 38-(1) (a) and (b) the Health and Safety exemption applies. Additionally section 38.-(2) applies in that we are neither confirming nor denying we hold the information requested.

Exemptions use rationale

This disclosure would prejudice the prevention and detection of crime and any information, albeit confirming what we hold or do not hold could assist criminals and place our patients and staff at harm. The Trust has provided a more detailed rationale below for each exemption used and applied them following the careful consideration of submissions made to a Public Interest Test in deciding the outcome of our response to you.

Section 31 – Law enforcement- prevention of crime

We consider this exemption applies because disclosing details of our security arrangements could prejudice the security and integrity of the Trust's network and increase the risk of unauthorised access to information held by the Trust, much of which is confidential and sensitive. The level of detail that would be released would enable external parties, who are not privy to the confidential aspects of Trust's IT systems, knowledge of our security equipment and by association its integrated network security. The Trust employs a range of security tools to mitigate the risk from different types of security threats. Firewalls, Intruder Detection Devices Antivirus and other products form a mesh of security that protects the Plymouth NHS Network and data, the more of these vectors that are known, the weaker the security of the network protection. There is a real risk that this knowledge could assist external parties in attempting a cyber-attack/hack into the Plymouth NHS Network. The anticipated harm from this is a breach of data protection (failure to protect information resulting in an unauthorised disclosure), data loss, and disruption to patient care through a loss of IT services. The severity of harm is extensive with millions of patient records put at risk of unauthorised disclosure.

Section 38 Health and Safety

Such disclosures also endanger the physical or mental health and safety of patients and staff. The dangers have become self-evident from recent events reported in the news, including delays to treatment and diagnostics to name but a few. Any failure of our infrastructure endangers both the physical and mental health of our patients and exposes them to danger.