Ref: FOI/CAD/ID 4201

Please reply to:
FOI Administrator
Trust Management
Service Centre
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

18 August 2017

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Cybersecurity.

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]

The information requested is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (https://ico.org.uk/media/for-organisations/documents/1207/law-enforcement-foi-section-31.pdf) run as follows:

31.—(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.