Reference:	FOI.16165.24
Subject:	Security practices and patient data
Date of Request:	27 November 2024

Requested:

1. What cryptographic primitives, algorithms, and protocols are used in the securing of patient data.

2. What security procedures and hardening is used to reduce the attack surface of software used to store and transport patient data.

3. What physical security measures are in place to ensure that there is no physical access by unauthorised persons to machines, safes, buildings, and other places where patient data is stored, both digital and analogue.

4. How are the humans in the loop required to behave with regard to this data (my mother, who works with Powys country council, tells me that government jobs are generally pretty good with that kind of thing, but I want to be sure).

5. What are the penalties for leaking such data, either accidentally or on purpose (see note about mother above).

Response:

Hywel Dda University Health Board (UHB) is unable to provide the information requested for questions 1, 2 and 3, as it has deemed that the information requested is exempt from disclosure under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA). The UHB has also considered the "mosaic effect"; 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 FoIA 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 (ICO) 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. The UHB is relying upon this exemption as it considers that releasing this information about its IT systems and physical security measures would make it more vulnerable to crime.

Section 31(3) of the FoIA provides that the duty to confirm or deny does not arise in relation to this information.

Section 31 of the FoIA is subject to the public interest test.

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, which will help to maintain public trust in the UHB.

In favour of non-disclosure: By releasing the information, the UHB would be vulnerable to this being used for crime, which potentially could compromise the security of both patient and staff information, whilst causing disruption to the flow of information through UHB systems, impacting on

patient care and safety. There is a clear public interest in protecting society and the UHB from the impact of crime. The UHB has also given consideration to previous cyber-attacks within the NHS, which is already in the public domain.

Decision: The UHB considers that the public interest in withholding the information is greater than the interest in disclosing, therefore protecting the UHB from potential criminal activity.

4. The UHB has applied a section 21 exemption of the FoIA to this part of your request, as the requested information is already reasonably accessible within the public domain. Provided overleaf are hyperlinks to a number of pages on the UHB's website, where you can read about why the UHB collects information about you, how this information may be used, as well as explaining what information we collect; you can also find out more detail about your right to see your health record and how to gain access to it.

   We have also included a link to the UHB's privacy notice. As described within the provisions of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), we take appropriate measures to maintain the security of your data. Information collected is governed by this privacy statement and use of the UHB's website signifies your agreement.

   Your information, your rights - Hywel Dda University Health Board

   How to make a request for my personal information? - Hywel Dda University Health Board

   Website privacy policy - Hywel Dda University Health Board

   The UHB also provides a list of policies that relate to your request:

   - 837 - All Wales Information Security Policy
   - 836 - All Wales Information Governance Policy
   - 275 - Secure Transfer of Personal Information Policy
   - 282 - Network Security Policy
   - 1138 - Security Management Policy
   - 201 - All Wales Disciplinary Policy and Procedure

5. Anyone found to have accessed information incorrectly will be managed in accordance with the policies detailed above. The UHB has a statutory duty to operate in accordance with UK GDPR and DPA. These laws and the UHB's practices are regulated by the ICO, and any data breaches must be handled in accordance with ICO procedures, which may on occasion result in further action being taken by the ICO. Further information can be found via the ICO website: Report a breach | ICO

The UHB takes its data processing obligations seriously. Should you have any concerns relating to the processing of your personal data, these can be directed to the Information Governance team directly on information.governance3@wales.nhs.uk.