Freedom of Information Request: Our Reference CTMUHB_458_21

Clarification provided on the 4 November:
Thank you and I am sorry for the confusion relating to my questions. I am particularly interested in insider threat/fraud linked to IT systems as a whole. However, I am also aware that sometimes organisations are set up in such a way that there may a specific person responsible for overarching auditing/monitoring of fraud which includes IT.

In terms of question 4, I am interested in how much was lost as a result of insider fraud/corruption in the last 5 years 'in general' as I am aware that it is probably not possible to break that down in terms of linking it to IT systems. NHS Counter Fraud Authority estimate that the NHS is vulnerable to £1.21 billion worth of fraud each year and I would like to understand how that relates to Cwm Taf Morgannwg University Health Board.

You asked:

1. **Does anyone in Cwm Taf Morgannwg University Health Board have responsibility for auditing/monitoring insider threats – counter fraud?**

   The Health Board's Counter Fraud Team have responsibility to investigate allegations of economic crime committed against the Organisation. Referrals are received under the Counter Fraud Policy and Response Plan.

2. **How is Cwm Taf Morgannwg University Health Board able to check that your systems are being used in the way that they should**?

   The Health Board has auditing software, which enables them to check use of systems. This can be done via routine reports, auditing and investigation. Routine reports are presented to the Health Board's Audit Committee and can be found via:
   Audit and Risk Committee - Cwm Taf Morgannwg University Health Board (nhs.wales)

3. **How many employees have misused their authority and used your IT systems inappropriately, (e.g.: to identify vulnerable people, falsify records etc) in the last 5 years?**

   We can confirm that the Health Board does not centrally record this information in a way that is easily retrievable. There are various audit capabilities dependent on the system used (such as clinical/ non-clinical / staff records). Whilst we have an auditing tool (NIIAS) for potential inappropriate use of clinical systems, this would not capture the detailed information you have requested, as this would be held in the investigation stage if appropriate.

4. **How much money has Cwm Taf Morgannwg University Health Board lost as a result of insider fraud/corruption in the last 5 years?**

   This information is not held. The Health Board would keep a record of funds written off, but not losses, as we would be actively in motion to recover those funds lost. Further information regarding counter fraud services within NHS Wales can be found via the link below:

About Counter Fraud Service Wales - NHS Wales Shared Services Partnership

5. **How often do you have to audit your IT systems to make sure employees are using them appropriately?**

   How frequently an audit is undertaken would depend on the system.

6. **When and how would Cwm Taf Morgannwg University Health Board be alerted to the fact that someone has used the IT system inappropriately?**

   The auditing software would raise an alert which can be viewed when logged into.

7. **Who has overall responsibility for ensuring that your IT systems are secure from internal threats?**

   The ICT department is responsible for Cyber Security.

8. **Do you currently have a budget allowance for auditing and monitoring your IT systems within Cwm Taf Morgannwg University Health Board? If so, how much?**

   There is no specific budget for auditing and monitoring.

9. **How many computers are there in Cwm Taf Morgannwg University Health Board?**

   Approximately 10,000 end points.

10. **What operating systems do your computers use?**

    The Health Board holds the information you have requested. However, we are unable to provide you with that information as we consider that the following exemption/s apply to it:

    Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

    - To protect the work of one that does.
    - To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

    The crime in question here would be a malicious attack on the health boards computer systems.

    The 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.

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

The exemption is subject to the public interest test. There is an overwhelming public interest in keeping health board systems secure and protecting the UHB from potential criminal activity, which would be served by non-disclosure. This outweighs the public interest in accountability and transparent which would be served by disclosure.