Freedom of Information Act 2000 - Request Reference FoI/21/393
IT Security

1. **In the past three years has your organisation:**

   a. **Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)**
      i. **If yes, how many?**

None

   b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**

Not applicable

   c. **Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)**

Not applicable

   d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?**
      i. **If yes was the decryption successful, with all files recovered?**

Not applicable

   e. **Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?**
      i. **If yes was the decryption successful, with all files recovered?**

Not applicable

   f. **Had a formal policy on ransomware payment?**
      i. **If yes please provide, or link, to all versions relevant to the 3 year period.**

Cardiff and Vale University Health Board (the UHB) is withholding this information, relying on Section 31 (1) (a) of the Freedom of Information Act 2000 (prevention and detection of crime). Specifically, the UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention of crime, particularly cyber-crime. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

Public Interest Test:

In favour of disclosure: The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

Against disclosure: There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cyber Security and the associated Cyber-Risk / Cyber-Attacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

Decision: The UHB considers that the public interest in withholding the information is significantly greater than any interest there may be in disclosing it and potentially exposing sensitive personal data to an increased level of risk. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public. Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself. The UHB considers its responsibility to protect the personal data of patients and staff to be of the highest importance. It was therefore decided that it was not in the public's interest to disclose this information.

g. Held meetings where policy on paying ransomware was discussed?

Please see above.

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
   i. **If yes at what cost in each year?**

No

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

No

j. Requested central government support for malware, ransomware, or system intrusion investigation?

No

k. Paid for data recovery services?
   i. If yes at what cost in each year?

No

l. Used existing contracts for data recovery services?

No

m. Replaced IT infrastructure such as servers that have been compromised by malware?
   i. If yes at what cost in each year?

No

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
   i. If yes at what cost in each year?

No, if any PC has malware it is wiped clean and reinstalled rather than replacing it.

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
   i. If yes how many incidents in each year?

The UHB is withholding this information, relying on Section 31 (1) (a) of the Freedom of Information Act 2000 (prevention and detection of crime). Specifically, the UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention of crime, particularly cyber-crime. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

Public Interest Test:

In favour of disclosure: The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

Against disclosure: There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cyber Security and the associated Cyber-Risk / Cyber-Attacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

Decision: The UHB considers that the public interest in withholding the information is significantly greater than any interest there may be in disclosing it and potentially exposing sensitive personal data to an increased level of risk. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public. Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself. The UHB considers its responsibility to protect the personal data of patients

and staff to be of the highest importance. It was therefore decided that it was not in the public's interest to disclose this information.

2. **Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?**
   a. **If yes is this system's data independently backed up, separately from that platform's own tools?**

Please see above.

3. **Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)**
   a. **Mobile devices such as phones and tablet computers**
   b. **Desktop and laptop computers**
   c. **Virtual desktops**
   d. **Servers on premise**
   e. **Co-located or hosted servers**
   f. **Cloud hosted servers**
   g. **Virtual machines**
   h. **Data in SaaS applications**
   i. **ERP / finance system**
   j. **We do not use any offsite back-up systems**

Please see above.

4. **Are the services in question 3 backed up by a single system or are multiple systems used?**

Please see above.

5. **Do you have a cloud migration strategy? If so is there specific budget allocated to this?**

Please see above.

6. **How many Software as a Services (SaaS) applications are in place within your organisation?**

   a. **How many have been adopted since January 2020?**

Please see above.