Information Governance Team
Monnow Ward
Bronllys Hospital
Bronllys
Brecon
Powys LD3 0LY
Email: Powys.FOI@wales.nhs.uk
Tel: 01686 252170 / 01874 442071

Our ref: IG/FOI/FOI.064.26 16 March 2026

Sent via email to: [redacted]

Dear [redacted]

Request under the Freedom of Information Act 2000

I write further to your request for information, which was received on 13 February 2026, to confirm, in accordance with S.1(1)(a) of the Freedom of Information Act 2000, that Powys Teaching Health Board (PTHB) does hold the information that you require, but have applied an exemption to this request. For ease of reference your request is set out below and the Health Board's response follows.

Your Freedom of Information (FOI) Request:
I am writing to you under the Freedom of Information Act to request the following information:

1. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for the Endpoint Detection and Response (EDR) solution
Include Supplier,
Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: The practice of securing organisational assets such as laptops, desktops, mobile phones, and servers against malicious activity. It encompasses tools and strategies designed to detect, prevent, and respond to threats directly on the device itself.

2. Please provide the following information for the current maintenance and licensing agreement for the primary Perimeter Firewall/ Intrusion Prevention System (IPS) solution
Include Supplier,

Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: The processes and technologies used to protect the boundaries (the perimeter) of an organisation's internal network from unauthorised external access. It involves monitoring and controlling incoming and outgoing network traffic.

3. Please provide the following information for the service agreement covering the Cloud Security Posture Management (CSPM) platform or equivalent third-party cloud security monitoring too
Include Supplier,
Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: The set of security measures designed to protect data, applications, and infrastructure running in cloud environments (e.g., AWS, Azure, GCP). It also includes securing internally and externally facing applications themselves (application security).

4. Please provide the following information for the service agreement covering your Identity & Access Management (IAM) software
Include Supplier,
Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: A framework of policies and technologies that ensures the right users have the appropriate access to the right resources at the right time. It involves managing digital identities, authentication (verifying identity), and authorisation (granting access).

5. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for your current Managed Security / SOC Services
Include Supplier,
Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: The outsourcing of security monitoring and management to a third-party expert. A Security Operations Center (SOC) is a centralised function (internal or outsourced) responsible for continuous monitoring, threat analysis, and managing security incidents.

6. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for your current Vulnerability & Compliance Management service
Include Supplier,
Product Name,
Start Date,
Expiry Date,
Annual spend 2025/2026 [£],
Additional notes [including any framework used]

DEFINITION: The continuous, cyclical practice of identifying, classifying, prioritising, remediating, and mitigating software weaknesses (vulnerabilities). Compliance Management ensures that security practices adhere to specific internal policies, regulatory requirements (like GDPR), and industry standards.

Powys Response:
Q1 – Q6. Powys Teaching Health Board is withholding this information from disclosure under section 31(1)(a) of the Freedom of Information Act 2000 ('the prevention or detection of crime'). This section states:

"Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a) " the prevention or detection of crime"

Section 30 of the Freedom of Information Act 2000 does not apply to this request.

This information is exempt from disclosure under Section 31(1a) of the Freedom of Information Act 2000 (FoIA). PTHB has considered that if the data you have requested were to be combined with other information which may be available in the public domain, there would likely to be an increased risk of a cyber-security attack upon the Health Board. As part of the Critical National Infrastructure for the NHS, the Health Board has a duty to protect the integrity of our systems, and the Health Board is of the opinion that disclosure of the withheld information would be likely to prejudice the prevention of these criminal acts in relation to the NHS Wales computer systems leading to the disruption of the operations of NHS Wales. It is our belief the disclosure of the information requested could expose weaknesses in our systems and lead to breaches, making the UK or its citizens, in this case our patients, more vulnerable to security threat.

Section 31 is a prejudice-based exemption and therefore subject to a public interest test.

Public Interest Test
In favour of disclosure, we recognise the need for transparency and we appreciate that it is in the public interest to know where data concerning their health is kept. It is reassuring to the public that we have services in place which protect information, as well as ensuring that the NHS infrastructure remains in working order and are not, for example, subject to a malicious attack.

In favour of non-disclosure, we would argue that if the information got into the wrong hands this information could be used to target our networks and buildings in knowing exactly where the information is held and disclosing this detail could determine when the health Board is at our most vulnerable. There is therefore a strong public interest in keeping the details of where this information is held securely and confidential at all times in order to protect data security, and in doing so, to protect the integrity of our systems.

In conclusion we have therefore concluded there is a strong public interest in protecting the confidentiality of patient data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access. For these reasons, the Health Board has concluded that the public interest in maintaining the exemption far outweighs the public interest in disclosure and therefore apply this exemption in relation to this information.

If you have queries or any concerns, contact details are given at the top of the letter. Please remember to quote the reference number above in any future communications. If you are dissatisfied with the handling or response to your request and wish to ask for a review of this, please contact us and we will arrange for this to be done.

Further information is available from the Information Commissioner's Office who can be contacted at:
Address: Information Commissioner's Office (Wales), 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH.
Telephone: 0330 414 6421
Complaints Portal: www.ico.org.uk/foicomplaints
Web site: https://ico.org.uk/

Re-use of Public Sector Information
All information supplied by the Health Board in answering a request for information (RFI) under the Freedom of Information Act 2000 will be subject to the terms of the Re-use of Public Sector Information Regulations 2015.

Under the terms of the Regulations, the Health Board will licence the re-use of any or all information supplied if being used in a form and for the purpose other than which it was originally supplied. This license for re-use will be in line with the requirements of the Regulations and the licensing terms and fees as laid down by the Office of Public Sector Information (OPSI). Most licenses will be free; however, the Health Board reserves the right, in certain circumstances to charge a fee for the re-use of some information which it deems to be of commercial value.

Further information including a sample license terms and fees can be found at Open Government Licence.

Yours sincerely

Vicki Cooper
Chief Digital Data Officer

Rydym yn croesawu derbyn gohebiaeth yng Nghymraeg. Byddwn yn ateb y fath ohebiaeth yng Nghymraeg ac ni fydd hyn yn arwain at oedi.

We welcome receiving correspondence in Welsh. We will reply to such correspondence in Welsh and this will not lead to a delay.