Reference:	FOI.20196.26
Subject:	IT Infrastructure, Digital Maturity and Technology Contracts
Date of Request:	14 April 2026

Requested:

I am requesting information relating to your organisation's IT infrastructure, digital maturity, staffing, contracts and technology spend.

Section 1 - IT Budget and Spend

1. What is your organisation's total annual IT / digital technology budget for the current financial year (or most recently completed financial year)? Please break this down into:
   a. Capital expenditure (CapEx)
   b. Operational expenditure (OpEx)

2. What proportion of your total organisational budget does IT / digital technology represent (as a percentage)?

3. Is there a separate cyber security budget? If so, what is its value?

4. Please provide the name(s) of any Commissioning Support Units (CSUs) or managed service partners that manage IT expenditure on your behalf, if applicable.

Section 2 - IT Staffing

5. How many whole-time equivalent (WTE) staff are directly employed in IT, digital or technology roles within your organisation?

6. Please provide a breakdown of IT staff by job role or band (e.g. Agenda for Change band or equivalent). Specific names are not required.

7. Does your organisation have the following named roles in post?
   (Please answer Yes / No / Vacant for each):
   a. Chief Information Officer (CIO) or equivalent
   b. Chief Digital Officer (CDO) or equivalent
   c. Chief Technology Officer (CTO) or equivalent
   d. Chief Information Security Officer (CISO) or equivalent
   e. IT Director / Head of IT
   f. Digital Transformation Lead or equivalent

8. How many IT staff are employed via third-party contractors or agency arrangements? What is the approximate annual spend on these arrangements?

Section 3 - Server and Compute Infrastructure

9. Does your organisation operate on-premise server infrastructure? If yes:
   a. What is the approximate number of physical servers in operation?
   b. What server vendors / manufacturers does your organisation use (e.g. Dell, HPE, Lenovo, Cisco UCS)?

c. What is the approximate age profile of your server estate (e.g. percentage under 3 years, 3–5 years, over 5 years old)?

10. Does your organisation use virtualisation technologies? If yes, which platform(s) (e.g. VMware, Microsoft Hyper-V, Nutanix)?

11. Does your organisation use hyperconverged infrastructure (HCI)?
    If yes, which vendor(s)?

12. Does your organisation use cloud computing services (not including office 365)?
    If yes:
    a. Which cloud provider(s) do you use (e.g. AWS, Microsoft Azure, Google Cloud, other)?
    b. Approximately what proportion of your workloads are cloud-hosted vs on-premise?
    c. What is the approximate annual cloud spend?

Section 4 - Storage Infrastructure

13. What storage platform(s) does your organisation use (e.g. NetApp, Dell EMC, Pure Storage, HPE, IBM)?

14. What is the approximate total usable storage capacity across your estate (in TB or PB)?

15. What is the approximate age of your primary storage estate?

Section 5 - Backup, Disaster Recovery and Business Continuity

16. What backup software solution(s) does your organisation currently use (e.g. Veeam, Commvault, Veritas NetBackup, Cohesity, Rubrik, Zerto)?

17. What is your backup target infrastructure (e.g. on-premise disk, tape, cloud)?

18. Does your organisation have a documented Disaster Recovery (DR) plan? When was it last tested?

19. What is the current Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for your critical clinical systems?

20. Does your organisation use an offsite or cloud-based backup solution? If yes, which provider?

Section 6 - Networking and End-User Computing

21. Who provides your Wide Area Network (WAN) and/or internet connectivity services?

22. What network equipment vendors does your organisation use (e.g. Cisco, Juniper, Aruba, Palo Alto)?

23. What is the approximate number of end-user devices (laptops, desktops, tablets) in your organisation?

Section 7 - Software, Licensing and Key Clinical Systems

24. What is your current Electronic Patient Record (EPR) / Electronic Health Record (EHR) system? Please provide the vendor name and product.

25. What Patient Administration System (PAS) does your organisation use?

26. Does your organisation use a Picture Archiving and Communication System (PACS) / radiology imaging system? If yes, which vendor and product?

27. Does your organisation have a Microsoft Enterprise Agreement (or equivalent) in place? When is this due for renewal?

28. What is the approximate annual spend on software licences across the organisation?

29. Please list any other significant enterprise IT contracts (by contract type / system category — e.g. HR, finance, workforce management) with approximate annual values where held.

Section 8 - Warranties, Contracts and Procurement

30. For your primary server, storage and network infrastructure, are vendor warranties and/or third-party maintenance contracts in place?

    Please provide:
    a. The type of coverage (vendor warranty, third-party maintenance, or both)
    b. The name of the maintenance provider(s), if applicable
    c. Approximate contract expiry dates where held

31. What procurement frameworks does your organisation use for IT hardware and services (e.g. Crown Commercial Service, NHS Shared Business Services, G-Cloud, Tech Products 4)?

32. Are any significant IT contracts due for renewal within the next 24 months? Please provide contract category (not necessarily full commercial detail).

Section 9 - Digital Maturity and Strategy

33. Has your organisation completed a Digital Maturity Assessment (DMA) or equivalent framework in the last two years?
    If so:
    a. Which assessment framework was used (e.g. NHS England DMA, HIMSS EMRAM, Other)?
    b. What overall maturity score or rating was achieved?

34. Does your organisation have a current Digital / IT Strategy? If so, what is the publication or approval date?

35. Has your organisation achieved or is actively working towards any recognised digital accreditations (e.g. HIMSS Level, NHS Digital aspirant status, Cyber Essentials Plus)?

36. What are the top three stated digital priorities for your organisation in the current or next financial year?

Response:

Hywel Dda University Health Board (UHB) has applied an exemption under Section 31(1)(a) of the Freedom of Information Act 2000 (FoIA) to part of question 29 as it has deemed that some of the information requested is exempt from disclosure as it would be likely to prejudice the prevention or detection of crime and potentially increase the risk of cyber-crime. The UHB has also considered the "mosaic effect"; the harm which will or will be likely to arise from the release of this information, when utilised alongside information already in the public domain.

Section 31 of FoIA is a qualified exemption requiring public authorities to apply the public interest test set out in Section 2(2)(b).

The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

The UHB has therefore considered the following:

In favour of disclosure: The UHB has a duty to maintain openness and transparency in all its activities, including decision making, which will help to maintain public trust in the UHB. Disclosing cyber security product information could provide assurance to the public that the UHB has a robust IT infrastructure in place, which in turn would reassure the public that their information is safe, and that public money has been well spent to ensure this.

Against Disclosure: A disclosure made under the FoIA, is a disclosure to the world at large and by releasing the details of its cyber security products, the UHB would be vulnerable to it being used for crime. Such action could compromise the security of UHB systems and both patient and staff information, whilst causing disruption to the flow of information through UHB systems, impacting on patient care and safety.

The UHB takes its Data Protection and Information Governance responsibilities very seriously and has robust arrangements in place to protect its IT systems and infrastructure. Disclosure of this information would reveal how to undermine systems, with the potential need to implement disproportionate steps resulting in additional expense to the public purse, to counter an increased risk that is currently managed.

Decision: Disclosing the information regarding the UHB's cyber security products will likely provide attackers with valuable information regarding the capability of the UHB's cyber security. Such a disclosure would enable targeted research that would compromise the integrity and confidentiality of its systems which contain sensitive information. The UHB has also taken into account the wider context of significant and growing cyber threats and attacks which continue to present a substantial risk to the world at large.

There is a clear public interest in protecting society and the UHB from the impact of crime. Therefore, the UHB has concluded that the public interest in withholding the cyber security products is greater than the interest in disclosing, consequently protecting the UHB from potential criminal activity.

The UHB has also applied an exemption under Section 43 of the FoIA to the annual values requested for question 29, as they relate to third parties and disclosure would be prejudicial to their commercial interests. Section 43(2) exempts information, where disclosure would or would be likely to prejudice the commercial interests of any company.

Commercial interests may be prejudiced where disclosure would, or would be likely to:

- Weaken a company's position in a competitive environment by revealing market sensitive information or information of potential usefulness to its competitors
- Damage a company's business reputation or the confidence that customers/users, suppliers or investors may have in it.

This exemption is qualified; therefore, even if information falls within Section 43, public authorities must then apply the public interest test set out in Section 2(2)(b). The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

The UHB has therefore considered the following:

In **favour of disclosure**: There is a public interest in transparency and in the accountability of public funds. Furthermore, it is in the public's interest that public funds be used effectively and that public sector bodies obtain the best value for money when contracting for the provision of services. Private sector bodies engaging in commercial activities with the public sector must expect some information about those activities to be disclosed.

Against Disclosure: Disclosure of this information would have a direct impact and cause substantial harm to the suppliers, as it would disclose their pricing and products/services provided to the UHB, and it would be likely that this would damage their ability to work within a highly competitive sector. The information being requested is likely to be used by their competitors to gain a competitive advantage.

Decision: The UHB has considered that releasing the information under the FoIA, to which the UHB is subject, will give an unfair advantage to the suppliers' competitors. The UHB believes that there is wider established public interest in companies not being prejudiced merely because they have contracted with or are bidding to contract with a public sector body, and that there is a public interest in ensuring that there is competition for public sector contracts.

Therefore, the public interest in withholding the annual values is greater than the interests in disclosing it and thereby giving unfair commercial advantage to competitors of the company to which this information concerns.

Additionally, the UHB is unable to provide you with the information requested for question 19 of your request, as it is estimated that the cost of answering your request would exceed the "appropriate limit" as stated in the Freedom of Information Act 2000 and the Data Protection (Appropriate Limit and Fees) Regulations 2004. The "appropriate limit" represents the estimated cost of one person spending 18 hours (or 2½ working days) in determining whether the UHB holds the information, and locating, retrieving and extracting the information.

In order to provide you with the current Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) for its outsourced critical clinical systems, the UHB would need to undertake a manual trawl of each contract to identify any information that would fulfil this part of your request, as this is not recorded centrally.

The UHB has identified that it currently has one hundred and twenty-three (123) active contracts. It is estimated that a manual search of these records would exceed the 18 hours stipulated within

the FoIA. Based on the number of records identified, conducting a search, taking a minimum of ten (10) minutes per record, would exceed the 'appropriate limit', costing the UHB the following:

123 @ 10 minutes per record = 20 hours and 32 minutes
20 hours and 32 minutes @ £25 per hour = £513.33

The UHB is therefore applying an exemption under Section 12 of the FoIA, which provides an exemption from a public authority's obligation to comply with a request for information where the cost of compliance is estimated to exceed the appropriate limit.

However, under Section 16 of the FoIA, we are required as a public authority, to provide advice and assistance so far as it is reasonable to individuals who have made a request under the FoIA, this can include assisting a requestor to further refine their request.

Unfortunately, the UHB is unable to provide advice on how you can refine your request further. This is due to the UHB still requiring a manual trawl of all outsourced critical clinical care contracts to be undertaken to identify information that may fulfil this part of your request.

1. The UHB provides the IT capital and operational expenditure budget for the 2025/26 financial year.

Question	Answer
a. Capital expenditure	£7,394,000.00
b. Operational expenditure	Pay - £14,654,721.00 Non-pay - £15,864,960.00

2. The IT budget allocation is 2.4% of the UHB's total budget.

3. The UHB does not have a separate budget for cyber security, it is incorporated into the overall IT budget.

4. Not applicable.

5. & 6. The UHB provides within the table below, the Whole Time Equivalent (WTE) of staff employed within its Digital and IT services, by job role and Agenda for Change (A4C) pay band, as at 1 May 2026.

Job role	Pay band	WTE	Job role	Pay band	WTE
Clinical Coding Clerk	2	8.40	Senior Information Manager	6	1.00
Information Officer	3	2.00	Data Standards Manager	6	1.00
Information Officer	2	2.00	Senior Information Developer	6	4.00
ICT Service Desk Analyst	3	10.00	Data Quality Improvement Manager	6	0.8
Clinical Coder	3	7.06	Digital Inclusion Manager	7	1.00
Data Quality Officer	3	0.60	Lead Specialist Senior Analyst	7	5.00
ICT Service Delivery Officer	4	2.00	Data Scientists	7	2.00
Clinical Coder	4	4.00	Principal Data Engineer	7	1.00
Senior Clinical Coder	4	10.47	Benefits Realisation Manager	7	1.00
Information Analyst	4	1.00	Corporate Information Manager	7	1.00
Data Quality Analyst	4	1.40	Senior Project Manager	7	9.00

Digital Senior Support Technician	5	14.00	End User Computing Technical Lead	7	1.00
ICT Infrastructure Engineer	5	1.00	ICT Senior Infrastructure Engineer	7	4.00
Junior Cyber Security Specialist	5	2.00	Lead Software Developer	7	1.00
Software Developer	5	1.00	Senior Cyber Security Specialist	7	1.00
Clinical Coding Supervisor	5	2.00	Data Assurance Lead	8a	1.00
Application Support Specialist	5	10.00	Head of Data Development	8a	1.00
Information Manager	5	0.85	Senior Digital Project Manager	7	2.00
Senior Information Analyst	5	1.00	Technical Implementation Lead	7	1.00
Digital Product Specialist	6	1.00	Telecoms Operations Manager	7	1.00
WPAS Supervisor	5	1.00	Programme Manager	8a	3.00
Information Developer	5	2.00	Client Services Operations Manager	8a	1.00
Project Manager	6	1.00	Cyber Security Operations Manager	8a	1.00
Business Change & Benefits Advisor	6	2.00	Data Centre Operations Manager	8a	1.00
Digital Inclusion Adviser	6	2.00	Network Operations Manager	8a	1.00
Cyber Security Specialist	6	2.00	Data Assurance Lead	8a	1.00
ICT Desktop Team Leader	6	4.00	Head of Data Development	8a	1.00
ICT Infrastructure Technician	6	3.00	Head of Information Services	8b	1.00
ICT Infrastructure Engineer	6	3.00	ICT Infrastructure Operations Manager	8b	1.00
Telecoms Support	6	1.00	Head of Division	8b	1.00
Service Desk Team Leader	6	1.00	Head of Data Science	8b	1.00
Software Developer	6	2.00	Head of Digital Operations	8c	1.00
Total					**159.58**

7. The UHB provides the requested information within the table overleaf.

Question	Answer - Yes/No
a. Chief Information Officer (CIO) or equivalent	No
b. Chief Digital Officer (CDO) or equivalent	No
c. Chief Technology Officer (CTO) or equivalent	Yes - Head of Digital Operations
d. Chief Information Security Officer (CISO) or equivalent	Yes - Cyber Security Manager
e. IT Director / Head of IT	Yes - Digital Director
f. Digital Transformation Lead or equivalent	Yes - Head of Digital Innovation and Transformation

8. Not applicable. The UHB does not employ third-party contractors or agency staff in its IT department.

9. The UHB does operate on-premise server infrastructure.

   a. The UHB has approximately eighty (80) physical servers in operation.

   b. The UHB uses Dell, HPE, Nutanix(SUN) and CISCO UCS.

   c. The UHBs server estate is under three (3) years old.

10. The UHB does use virtualisation technology. The platforms are VMWare and Nutanix.

11. The UHB does use Hyperconverged Infrastructure (HCI). The vendor is Nutanix.

12. The UHB does use cloud computing services, excluding Microsoft office 365.

    a. The UHB uses the cloud provider Azure.

    b. The UHB does not hold this information.

    c. The approximate annual cloud spend was £144,000.00, during the 2025/26 financial year.

13. The UHB uses the storage platforms Hewlett Packard Enterprise (HPE) and Pure Storage.

14. The UHB's approximate useable storage capacity is three hundred and fifty (350) terabytes (TB).

15. The approximate age of its primary storage estate is two (2) to four (4) years old.

16. The UHB uses the backup software solution Rubrik.

17. The UHB's backup target infrastructure is on-premise with archive to Cloud.

18. The UHB does have a documented Disaster Recovery (DR) plan. However, the UHB does not have a specific date as the system restore process is periodically tested throughout the year.

19. An exemption under Section 12 of the FoIA has been applied. However, under Section 16, the UHB can confirm that for its outsourced clinical critical systems the contracted RPO is twenty-four (24) hours, and the RTO is two (2) hours. In house systems do not have a set RPO or RTO.

20. The UHB does not use an offsite or cloud-based backup solution.

21. The UHB's Wide Area Network (WAN) is provided by the Public Sector Broadband Aggregation (PSBA).

22. The UHB uses the network equipment vendors Cisco, Aruba and Fortigate.

23. The number of end user devices is approximately thirteen thousand (13,000).

24. The UHB does not have an Electronic Patient Record (EPR)/Electronic Health Record (EHR) system. The UHB uses the Welsh Clinical Portal (WCP) for clinical records, however, this system is not defined as an EPR/EHR system.

25. The UHB uses the Welsh Patient Administration System (WPAS).

26. The UHB does use a Picture Archiving and Communication System (PACS). The vendor is Phillips and the product is PACS.

27. The UHB does have a Microsoft Enterprise Agreement (EA) in place. The renewal date is July 2026 and is managed by Digital Health and Care Wales (DHCW).

28. The annual spend on software licenses across the UHB is approximately £9,537,000.00 excluding VAT; this includes DHCW services and Microsoft EA via DHCW which is £5.082,000.00.

29. Under the FoIA, an exemption under Section 31 has been applied to cyber security products and an exemption under Section 43 has been applied to the annual values requested. However, the UHB provides the IT contracts over £5,000.00, by contract type and system category, excluding cyber security products, at Attachment 1.

30. The UHB does have vendor warranties and maintenance contracts in place for its primary server, storage and network infrastructure.

    a. - c. Please see Attachment 1.

31. The procurement frameworks used for IT products and services are provided below:
    - Welsh Government Commercial Delivery (WGCD), formerly the National Procurement Service (NPS) framework
    - NHS Shared Business Services (SBS)
    - Crown Commercial Services (CCS).

32. Please see Attachment 1.

33. The UHB has completed a Digital Maturity Assessment (DMA) during the period 1 May 2024 and 30 April 2026.

    a. The UHB used the Healthcare Information and Management Systems Society (HIMSS) Infrastructure Adoption Model (INFRAM) assessment framework.

    b. The overall maturity score achieved was four (4).

34. The UHB provides a copy of its digital strategy 'Our Digital Response 2020-2025', at Attachment 2. The strategy is currently being renewed.

35. The UHB has not and is not actively working towards any recognised digital accreditations.

36. The UHB provides below its top three (3) digital priorities for the 206/27 financial year:
    - Electronic Medicines Prescribing Administration
    - Open Eyes – Ophthalmology HER
    - Emergency Department system upgrade