Digital Health & Intelligence Committee

Tue 20 February 2024, 09:00 - 12:00

MS Teams

Agenda

09:00 - 09:10
10 min

1. Standing Items

1.1. Welcome & Introductions

David Edwards

1.2. Apologies for Absence

David Edwards

1.3. Declarations of Interest

David Edwards

1.4. Minutes of the Committee Meeting held on 3rd October 2023

David Edwards

📄 DHIC Public Minutes 03.10.23.pdf (7 pages)

1.5. Action Log following the Committee Meeting held on 3rd October 2023

David Edwards

📄 DHIC Public Action Log - Oct.pdf (1 pages)

1.6. Committee's Chairs Actions

David Edwards

09:10 - 10:15
65 min

2. Items for Review and Assurance

2.1. Digital Transformation and Digital Strategy Progress Report

25 mins   David Thomas

📄 2.1 - Digital Strategy.pdf (6 pages)

2.2. Joint IMT & IG Corporate Risk Register

10 mins   David Thomas

📄 2.2a - Joint IMT IG Risk Register Cover.pdf (3 pages)
📄 2.2b - DHI Combined Risk Register - Appendix 1.pdf (4 pages)

2.3. IG Data & Compliance (SIs, Data Protection, GDPR, FOI, SARs, Staffing & Mandatory Training)

10 mins   James Webb

📄 2.3 - IG Compliance.pdf (6 pages)

2.4. Digital Services Key Performance Indicators

10 mins   *David Thomas*

📄 2.4a - Digital Services Key Performance Indicators Cover (2).pdf (2 pages)
📄 2.4b - Appendix 1 - Key Performance Indicators.pdf (12 pages)

2.5. Framework Policies, Procedures & Controls Update

10 mins   *David Thomas*

📄 2.5a - Framework Policies Procedures and Controls Cover.pdf (2 pages)
📄 2.5b - Controlled Documents Schedule Oct '23 DA Appendix 1.pdf (1 pages)

10:15 - 10:15
0 min

3. Items for Approval / Ratification

3.1. Information Governance Policy

10 mins   *James Webb*

📄 3.1a - Information Governance Policy Cover.pdf (3 pages)
📄 3.1b - CV IG policy v0.8 (2023 review) 1.pdf (33 pages)

10:15 - 10:15
0 min

4. Items for Noting and Information

4.1. Digital Directors Peer Group

5 mins   *David Thomas*

📄 4.1a Digital Directors Peer Group Cover.pdf (2 pages)
📄 4.1 - Appendix 1 - Directors of Digital Peer Group Meeting Oct23.pdf (4 pages)
📄 4.1 - Appendix 2 - Directors of Digital Peer Group Meeting Nov23.pdf (5 pages)
📄 4.1 - Appendix 3 - Directors of Digital Peer Group Meeting Dec23.pdf (3 pages)
📄 4.1 - Appendix 4 - Directors of Digital Peer Group Meeting Jan24.pdf (4 pages)

10:15 - 10:20
5 min

5. Agenda for Private Digital & Health Intelligence Meeting

David Edwards

i) Minutes and Action Log from the Private DHIC Committee held on 03.10.2023

ii) Digital Budget and Investment and Strategy Case for Investment

iii) Caldicott Guardian Report

iv) Cyber Update

10:20 - 10:25
5 min

6. Any Other Business

David Edwards

10:25 - 10:25
0 min

7. Items to bring to the attention of the Board / Committee

David Edwards

10:25 - 10:25
0 min

8. Review of the Meeting

David Edwards

10:25 - 10:25
0 min

9. Date & Time of next Meeting:

David Edwards

28th May 2024 at 9am via MS Teams

Unconfirmed Minutes of the Public Digital & Health Intelligence Committee Meeting Held On 3 October 2023 Via MS Teams

Chair:		
David Edwards	DE	Independent Member – Information Communication & Technology (IM-ICT)
Present:		
Akmal Hanuk	AH	Independent Member – Local Community (IM-LC)
In Attendance:		
Fiona Jenkins	FJ	Executive Director of Therapies & Health Sciences (EDTHS)
Bruce Johnson	BJ	Digital Service Delivery Architect (DSDA)
Angela Parratt	AP	Director of Digital Transformation (DDT)
Matt Phillips	MP	Director of Corporate Governance (DCG)
David Thomas	DT	Director of Digital and Health Intelligence (DDHI)
Francesca Thomas	FT	Head of Corporate Governance (HCG)
Mark Wardle	MW	Consultant Neurologist
James Webb	JW	Head of Information Governance and Cyber Security (HIGCS)
Observers:		
Secretariat		
Rachel Chilcott	RC	Corporate Governance Officer
Apologies:		
Keith Harding	KH	Independent Member – University (IM-U)
Meriel Jenney	MJ	Executive Medical Director (EMD)
Suzanne Rankin	SR	Chief Executive Officer (CEO)

Item No	Agenda Item	Action
DHIC 23/10/001	**Welcome & Introduction** The Committee Chair (CC) welcomed everyone to the Public meeting and confirmed the meeting was quorate.	
DHIC 23/10/002	**Apologies for Absence** Apologies for absences were noted. **The Committee resolved that:** a) The apologies were noted.	
DHIC 23/10/003	**Declarations of Interest** **The Committee resolved that:** a) No Declaration of Interest were noted.	
DHIC 23/10/004	**Minutes of the Meeting Held 15 August 2023** **The Committee Resolved that:** a) The Minutes of the Meeting held on the 15 August 2023 were confirmed as a true and accurate record.	

1

DHIC 23/10/005	**Action Log – Following the Meeting held on 15 August 2023**	
	The Action Log was received.	
	The Committee Resolved that: a) The Action Log was discussed and noted.	
DHIC 23/10/006	**Chair's Action taken since the last Committee Meeting**	
	The Committee Resolved that: a) There were no Chair's Actions taken since the last meeting.	
	Items for Review and Assurance	
DHIC 23/10/007	**Digital Transformation Progress Report**	
	It was noted that progress had not been significant due to a recent meeting in August.	
	The DDT presented and summarised the Digital Transformation Progress Report. The report is available to view in detail alongside the papers received for the Public DHIC Committee on the 03/10/2023 for Agenda item 2.1.	
	The DDHI added that the vacancy scrutiny had been applied across the organisation, and digital should not be any different, and this involved reshaping their services to achieve savings in the long-term.	
	The IM-LC asked whether enough money had been put into digital throughout the current financial year, or whether the money had not been forthcoming.	
	The DDHI responded that the digital budget was small, but that there was an opportunity to inform the organisation's long-term financial modelling.	
	The EDTHS asked if the recent regulations in place around scrutinising vacancies had impeded on the team's ability to deliver digital schemes.	
	The DDHI stated that he hoped to explain to the scrutiny panel that digital would not be able to move forward with a large number of vacancies, as they were fundamental to deliver their digital roadmap. He added that part of the problem was that they did not have interim staff to fill posts.	
	The DDHI commented further that needed to get the message across that the more investment there was in digital, the more efficient the organisation could become – which would only have a positive impact on finances.	
	The DDT noted that regarding recruitment, there were national pressures and competition for certain skillsets. In	

2

		addition, if they were unable to offer fully remote posts, they had been unable to fill a vacancy. The IM-ICT asked what England were doing differently to be able to invest in digital, and if there had been a deeper dive into the benchmark figures. The DDHI added that many Trusts in England had better infrastructure which made a big difference on spend. He stated that they had undertaken some benchmarking with other Health Boards in Wales, however some organisations had procured more services from Digital Health Care Wales (DHCW) than others. Their overall digital maturity was not comparable to England currently. **The Committee Resolved that:** a) The Committee reviewed the progress report and noted the planned investment case being developed.	

DHIC 23/10/008		**Joint IMT & IG Corporate Risk Register**
		
		The Joint IMT and IG Corporate Risk Register Paper was presented and the following was highlighted:
		    - The top risks remained unchanged since the August meeting – their top risk remained as cyber security;
		    - Effective Resource Utilisation was at a lower risk due to the Health Board having found a better way forward on how they utilised existing resources;
		    - They had removed the NWIS Governance Arrangements from the Risk Register since the August meeting.
		
		The DCG stated that the DDHI had briefed the September Board on the Board Assurance Framework for Digital.
		
		The Committee Resolved that:
		    a) The Committee noted the progress and updates to the Risk Register report.	

DHIC 23/10/009		**IG Data & Compliance (Sis, Data Protection, GDPR, FOI, SARs, Staffing & Mandatory Training)** The HIGCS presented and summarised the IG Data & Compliance Report which considered key information governance issues. The report is available to view in detail alongside the papers received for the Public DHIC Committee on the 03.10.2023 for Agenda item 2.3. The IM-ICT asked why the requests for medical records had increased. The HIGCS responded that he was unsure. The IM-ICT asked that if the number of requests sustained at this level, if there would be a challenge to meet compliance. The HIGCS responded that it would have to be raised with the operational management team responsible for that department to be resourced. However, he noted that the	

Chilcott Rachel
13/02/2024 10:28:00

3

3/7

3/98

		single front door would improve compliance and make the process swifter. **The Committee Resolved that:** a) The Committee received and noted a series of updates relating to significant Information Governance issues.	
DHIC 23/10/010		**Digital Services Key Performance Indicators** The Digital Services Key Performance Indicators Report was presented. The slides provided stationary screenshots of the data being captured from Ivanti and displayed in Power BI for the reporting of Lag Key Performance Indicators within DH&I. The DSDA highlighted that: - The numbers had increased since the previous year due to more digital teams coming on board. This would continue to increase; - The time taken to complete requests had reduced, which allowed staff more time to focus on further project related work; - The number of First Call Resolutions had increased, and less time was taken to close incidents; - There was some concern over incidents that had remained open for around a year – one of their biggest challenges was getting hold of users who were frontline workers. The DDT asked how far along were they in being able to automate some of the high-volume low complexity requests. The DSDA responded that the most significant was the new starters, which was a fully automated process. They hoped to have further automation processes implemented within the following few weeks. The DSDA continued: - Understanding of 'requests' had improved as the team had received fewer general requests – this was potentially due to the deployment of the new source service portal which enabled a search functionality, and the updated FAQ area for users to find self-help to software resolutions; - Change requests were heavily dominated by PARIS changes; - Change Management had gone live the previous week, which would soon be rolled out - this would allow other digital teams to be aware of changes; - The following week, The DSDA would set up a Problem Management Board to start logging problems. The IM-LC queried if there was a way to understand where people were struggling. He suggested that the requests received related to the hardware and software systems within the Health Board, and asked for the team's general take on the system.	

4

	The DSDA responded that the team were working on a Configuration Management Database (CMDB) which tracked all of their devices and incidents logged against particular items. The DDHI added that: - Teams were undertaking an analysis piece to understand the implications of not adequately investing in modern devices; - They only had a small team of 3 or 4 people that undertook training, which was inadequate when looking at an organisation of this size; - He wished to reach out to the Executive Director of People & Culture to understand levels of competence amongst staff; - They should consider publishing some of their performance outside of this Committee; - They would set some SLAs around what users could expect in terms of response times to their calls, so that they could monitor whether they were performing against the agreed internal standards. The IM-LC asked whether there would be merit in undertaking a digital survey to understand people's competence levels. The DDT responded that a survey would be undertaken for Electronic Prescribing Medicines Administration (EPMA), and that HR and HEIW colleagues had pulled together information on digital competence. He added that an all-encompassing digital strategy was needed for the whole organisation, which would be complex in an organisation with multiple domains and differing competence levels. The IM-ICT asked whether the team had looked into online learning (e.g. LinkedIn learning) for staff. The DDT responded that their online learning was not all-encompassing. <u>Actions:</u> 1. To liaise with the Executive Director of People & Culture (EDPC) to get an idea of the digital competence levels across staff in the organisation and potential options regarding training (DH). **The Committee Resolved that:** a) The Committee reviewed and noted the progress since the last update on the Ivanti service desk tool in relation to KPIs.	
DHIC 23/10/011	**Framework Policies, Procedures & Controls Update** The DDHI highlighted that: - The IG Policy – the proposal was to bring this back to DHIC for review and approval as a substantive policy; - The IG Corporate Training Policy – this was being finalised and would be brought back to the following DHIC committee meeting;	

5

		- The IT Security Incidents Breach Guidance had been replaced by a Standard Operating Procedure (SOP) and would be deployed across the organisation. **The Committee Resolved that:** a) The Committee noted progress.	
		Items for Noting and Information	
DHIC 23/10/012		**Minutes: Digital Directors Peer Group** The DDHI highlighted that: - There had been further discussions on the RISP programme across Wales in terms of the go-live dates for individual organisations, due to the reliance on the expiry of the existing Fuji contract for some Health Boards. This had now been resolved; - The next meeting of the Digital Directors was that afternoon; and - They held a Regional Digital Summit around 3-4 weeks previously, which was well attended with ABUHB and CTUHB colleagues. They identified common areas of opportunity which they were keen to explore. Action: 1. For a substantive piece of work to be brought back to DHIC which summarised how the regional work with ABUHB and CTMUHB was progressing, following discussions held at the recent Regional Digital Summit around common areas of opportunity (DH) **The Committee Resolved that:** a) The Committee noted the minutes of the 08.08.2023 and 05.09.2023 Digital Directors Peer Group meetings.	
		Agenda for Private Digital & Health Intelligence Meeting	
		(i) Minutes from the Private DHIC Meeting held on 15 August 2023 *(ii)* Digital Budget and Investment and Digital Strategy Case for Investment (confidential paper) *(iii) Caldicott Guardian Requirements (Confidential paper – contains personal data)* *(iv) Cyber Report including: Performance Measures (confidential paper)*	
DHIC 23/10/013		**Any Other Business** No Other Business was discussed.	
DHIC 23/10/014		**Items to bring to the attention of the Board / Committee** No Items were brought to the attention of the Board / Committee.	
		Date & Time of next Meeting:	

6

	Tuesday 20th February 2024 at 9am via MS Teams	

7

Action Log
Following the Digital Health & Intelligence Committee
Held on 3rd October 2023
(For the 13th February 2024 meeting)

Minute Ref	Subject	Agreed Action	Lead	Date	Status
Complete Actions					
DHIC 15/08/010	**Digital Services Key Performance Indicators**	To explain how the Key Performance Indicators (KPIs) statistics are starting to make a difference to the Health Board.	Russell Kent	03.10.2023	**COMPLETED Committee updated on 03 October 2023**
Actions in Progress					
DHIC 23/10/011	**Digital Services Key Performance Indicators**	To liaise with the Executive Director of People & Culture (EDPC) to get an idea of the digital competence levels across staff in the organisation and potential options regarding training.	David Thomas	13.02.2024	**Update in February 2024**
DHIC 23/10/012	**Minutes: Digital Directors Peer Group**	For a substantive piece of work to be brought back to the Committee which summarises how the regional work with ABUHB and CTMUHB is progressing, following discussions held at the recent Regional Digital Summit around common areas of opportunity.	David Thomas	13.02.2024	**Update in February 2024**
Actions referred from another Committee					
Actions referred to the Board / Committees of the Board					

Chilcott,Rachel
13/02/2024 10:28:00

**CARING FOR PEOPLE
KEEPING PEOPLE WELL**

Bwrdd Iechyd Prifysgol
Caerdydd a'r Fro
Cardiff and Vale
University Health Board

Report Title:	**Digital Transformation Progress Report**			Agenda Item no.	2.1
Meeting:	**Digital and Health Intelligence Committee**	Public	x	Meeting Date:	20 February 2024
		Private			
Status *(please tick one only):*	Assurance	x	Approval		Information	
Lead Executive:	**Director of Digital and Health Intelligence**				
Report Author (Title):	**Director of Digital Transformation**				

Main Report
Background and current situation:

Demand for D&HI project support continues and the directorate's run rate of activity is fairly consistent.

Project activity summary January 2024

The graphics at Figure 1 shows a summary of project works in train as reported to the Digital Advisory Board in January.

Project activity typically represents some form of additionality to the IT estate e.g. software, hardware and so on, in essence something new that will subsequently require some on-going maintenance and support.

Project works are resourced in one of two ways; from within existing capacity or, sometimes, with additional resource support during implementation. These temporary additional resources don't provide for the need to pull on teams across the department in order to complete a project. The effect of this is typically evidenced as implementation delays.

Once projects complete any additional resource falls away whilst maintenance falls to existing capacity for support, inevitably building a cycle of increased support needs as the current IT estate expands.

This is discussed further in Item 3.1 of the private meeting of DHIC

Activity summary
- Active projects have been ranked against criteria and are in progress
- Pipeline means we are at the very early stages of understanding a requirement, or, the requirement is understood and we are waiting the resource to start work or, we have parked the initiative pending investment
- LBAU (large business as usual) – these are work requests that will take more than 10 days to complete but can be managed within a single team with limited interdependency with other teams in the department
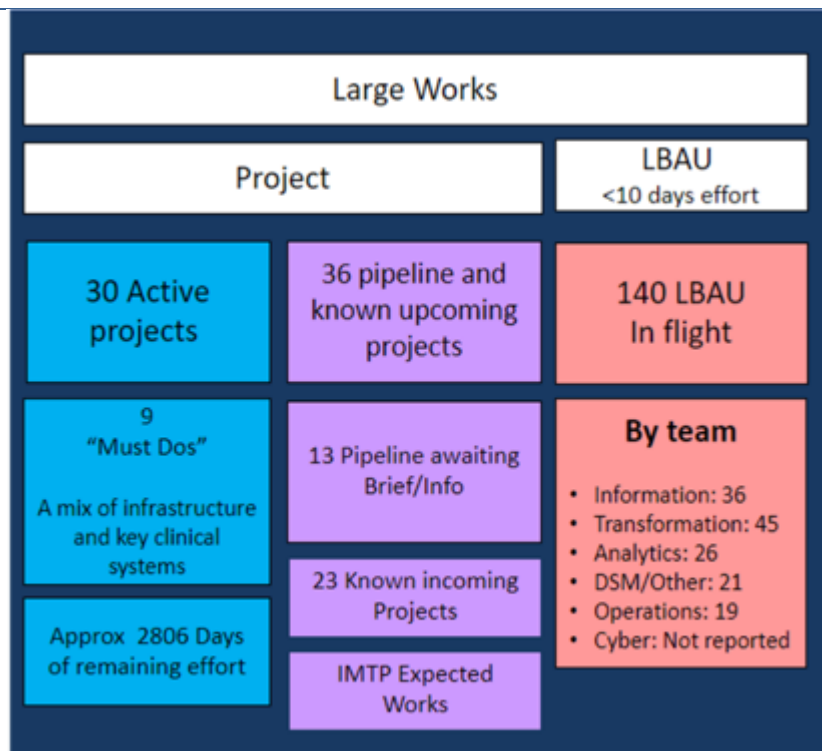
Chilcott Rachel
13/02/2024 10:28:00

Figure 1

IMTP 24/25

Progress continues to be made on delivery of IMTP priorities, most of which are Welsh Government funded national programmes, including WNCR, EPMA and LIMS.

The 24/25 IMTP process is nearing conclusion and major initiatives that will form part of the D&HI 24/25 workplan are shown at Figure 2.

- Pipeline items in Figure 2 are initiatives we expect to be implementing in 24/25 but this needs to be confirmed
- 23/24 initiatives are already started and will continue throughout 24/25
- 24/25 shows the major programmes that will start in that year
- 25/26 shows major initiatives we believe will start in that year

Figure 2

Shaping our Future Digital Services

Figure 2 describes some major digital initiatives that we expect will contribute significantly to improving aspects of our digital maturity including for example electronic prescribing and medicines administration (EPMA), fully implementing Welsh Nurse Care record and a new, more modern laboratory information system.

The interoperability challenge remains as these applications continue to be data silos.

In October it was reported to the Committee that in order to improve our digital maturity and put in place the capabilities we need for interoperability as well as to improve our HIMSS level of digital maturity, an investment case for the next 3 to 5 years was prepared for submission in quarter 4 2023/4.

It became apparent through the highly collaborative IMTP planning process that our digital ambitions are not affordable given the challenges of our physical estate and calls on discretionary capital.

A new plan to source the necessary investment has been formulated and this is discussed further at item 3.1 of the private meeting of DHIC

Tactical Activity Update on work programme since October 2023

Key Updates from across the D&HI services:

Digital Service Management (DSM)

Project Accelerator has moved to first delivery and Project and large works management control is being moved to project accelerator over the coming months, controls and features to expand allowing management of risk, benefit, and project milestones.

- The team has undertaken two skills building sessions (benefits and risk management) with a third (Business Requirements) planned for the 13th of February: with good feedback from attendees so far. These sessions produce a product @risk log etc..) that is then built into the M.S Project Accelerator.
- Peer/learning visit to ABuHB whom established a Digital PMO in 2019. AB are significantly ahead of CaV on PM methodology and processes, which will now be shared with CaV. CaV arguably ahead on the development of MS Project Accelerator as the 'container' for Digital Projects
- Recruitment to the two vacancies within the team (retiring senior managers for WCP and Training) have been delayed in scrutiny. There is risk of not filling these roles in 23/24, as advert can only go out to internal candidates

Digital Operations

- A multi site comprehensive Wi-Fi audit is currently under way. This started in Dec 23/Jan 24 with a review of the existing Wi-Fi infrastructure and more recently actual floor walking throughout our main sites.
- Our networking security has been further improved with the updating of Cisco ISE hardware and software, which controls how devices are able to access the CAV network.
- The Telecoms team have completed an organisational wide move from Analogue to Digital telephony ahead of the national 2024 deadline. All of this with minimal disruption and seamlessly in the background.
- The Support teams continue to develop the Service Desk with enhancements in ticket handing and trialling functions such as CHAT and improved user creation automations.
- The Server team have consolidated the entire 600+ virtual server estate on standardised hardware and software. This has included procuring some new HPE servers and VMware licences. As well as gaining enhanced functionality from existing Microsoft investments.
- Backups and Recovery times have been improved by the Server team. This has been achieved by consolidating on a single backup product ensuring better RPO and RTO times for the organisation.

Digital Transformation

- PMS Migration – PMS Live, PMS Test, PMS Train, Data Warehouse; PMS Live migration is in progress – phase 1 is complete and phase 2 is on hold until we can path the 11g database (preparation for this is in progress). PMS Test, Train and Data Warehouse migration will follow PMS live migration
- PMS Forms 6 Migration to Forms 12c Migration – Oracle WebLogic has been implemented and the PMS Forms have been migration. Currently in Testing. PMS Migration cannot complete until PMS Forms 12c is ready.
- E-Triage – Messaging specification agreed, awaiting delivery from supplier; preparatory work underway with sample messages – agreeing delivery timescales with supplier and EU department.
- Regional Shared Care Record – supported proof of concept with integrations of data from Cardiff Vale Health Board, Cardiff Council and Vale of Glamorgan Council.
- WRAPPER – Phase 1 (other Health Board's booking into Cardiff's MDTs, including functionality to view Outpatient Appointments in Cardiff) in final UAT, expected delivery in early March; Phase 2 – Cardiff booking into other Health Board's MDTs.
- Scan4Safety – demographic update integration completed; further requirements in evaluation
- Welsh Nursing Care Record – admissions, discharges and demographics data products – delivered and used in nursing dashboard; further evaluation of data products on-going.
- CTM – MDT booking functionality, real-time updates of cancer tracking data and SCP submissions to DHCW/Welsh Gov.
- PROMS – PSOM standards work is ongoing with CAV, Value in Health and Firely, moving towards the end of its final phase. Implementing standards in messaging flow. CAV and MCO working together and planning testing. A requirement for delivery is the completion of the AIMES solution.
- AWTTC – designing replacement system for All Wales Toxicology and Therapeutics Centre for tracking and managing trial medications.
- ePOAC – stability and user experience enhancement delivered. Document integration with CAV Clinical Portal and WCP currently in UAT. Further Integration with PMS (Inpatient TCI's and Waiting Lists) is planned for 24/25; design is in progress.
- ePMA – pre-contract discussions with supplier underway. Staffing levels for implementation and BAU identified. Welsh Government funding for implementation approved. Multidisciplinary discussions underway, with plans being developed, for a number of foundational digital capabilities, including Common Demographics Store, API Management (APIM), and Identity and Access Management (IAMS) including Single Sign-On (SSO).

PARIS Mental Health and Community system & Power Apps

- Paris was audited by Internal Audit with a "Reasonable" assurance
- New Paris application and database servers on line. Non live environments migrated. Live migration due in Q2/Q3 2024.
- New CRT referral form live using a new Kafka data feed
- Physiotherapy Referrals Kafka feed from D&T into Paris live
- CAMHS and Primary Mental Health merged into new service – Emotional Wellbeing & Mental Health Care Group
- Safe@Home live on Paris with WCP document upload functionality coming very soon
- Paris demographics API live and being used in DCR Shared Care Portal, HPV Power App and Flu Power App
- Flu and HPV Power Apps updated and live ahead of the 2023/24 winter campaign

Architecture and Analytics

- UHW2 planning – the planning team along with analytics team and Cardiff Uni shared our 1st modelling output with women and children that forecast the "do nothing option" for 10 years. It was well received and next steps are to bring in additional and tweak the output in a format for greater understanding.
- The Cardiff Uni team have finished writing up the frequent attenders at A&E research paper and are sharing this for peer review prior to submitting this to a journal.
- The monthly Integrated performance report is currently being produced for this month and additional significant changes (recommended by the Wales Audit office report) are required for future publications.

- Final steps to complete the 1st iteration of a project to develop a predictive tool to determine if a patient will deteriorate while in hospital.
- The capacity and demand modelling for the COO office for many uses including IMTP and service reviews which feed into the UHW2 modelling work. We are currently developing a dimensional model for Annual IMTP, UHW2 Future Hospitals Programme, Clinical Services Programme and continuous monitoring of services capacity and demand

Business Intelligence Service

- Stage 2 Operational Cancer dashboard was released and well received.
- Mortality dashboard development completed now awaiting demo, feedback and release.
- Flow dashboard developed for OPAT using data from STAMP/WCWS – data refreshes every 10 minutes and provides secure drill down to patient details.
- New accredited Power BI visualisation called Easy SPC has been installed – enables the creation of fully interactive SPC charts with step change and annotation to be included in Power BI.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

The Digital & Health Intelligence team continue to deliver a wide range of initiatives to support CAVUHB strategic ambitions and current organisational pressures. Demand continues to outstrip capacity and we have changed our governance to support us to manage this in the context of CAVUHB priorities.

The Committee is asked to note that D&HI remains challenged in terms of human resources and investment to transform digitally. The Committee is also asked to recognize that Digitalisation is a major opportunity and key requirement to support the organisation as it strives to improve safety, quality and operational efficiency.

We remain committed to developing plans and securing investment to achieve our digital objectives in support of the UHB aims to transform clinical service delivery.

Recommendation:

The Board / Committee are requested to:

1. REVIEW the progress report and note the planned investment case being developed.

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1.	Reduce health inequalities		6.	Have a planned care system where demand and capacity are in balance	
2.	Deliver outcomes that matter to people	x	7.	Be a great place to work and learn	x
3.	All take responsibility for improving our health and wellbeing		8.	Work better together with partners to deliver care and support across care sectors, making best use of our people and technology	x
4.	Offer services that deliver the population health our citizens are entitled to expect	x	9.	Reduce harm, waste and variation sustainably making best use of the resources available to us	x
5.	Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10.	Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives	

Five Ways of Working (Sustainable Development Principles) considered
Please tick as relevant

Prevention		Long term		Integration		Collaboration	x	Involvement	x

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: No

Safety: No

Financial: Yes
Benefits realisation from smarter working practices using digital solutions

Workforce: Yes
Supports our contribution for our digitally enabled workforce

Legal: Yes/No

Reputational: Yes

Supports our ability to manage our resources and data effectively

Socio Economic: No

Equality and Health: No

Decarbonisation: Yes
Improved use of digital solutions – this reduces travel by staff and patients (home working and virtual appointments)

Approval/Scrutiny Route:

Committee/Group/Exec	Date:

Chilcott Rachel
13/02/2024 10:28:00

Report Title:	Joint IMT & IG Corporate Risk Register			Agenda Item no.	2.2	
Meeting:	Digital and Health Intelligence Committee	Public	x	Meeting Date:	20th February 2024	
		Private				
Status *(please tick one only):*	Assurance		Approval		Information	x
Lead Executive:	Director of Digital and Health Intelligence					
Report Author (Title):	Director of Digital and Health Intelligence					

Main Report
Background and current situation:

The joint IMT Risk register is a combined register consisting of digital / Information Governance and Information / Performance risks.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

There are currently 13 joint IMT/IG risks identified on the report:

1 x Risk remains in red status with a score of 20 which is:

- Cyber Security

1 x Risk has moved from yellow status with a score of 8 and has now moved to amber with a score of 12.

- WCCIS Local team not resourced

3 x Risks have moved from amber status into yellow status with a score between 8 and 9 which are:

- Server Infrastructure
- Outcome Measures
- WLIMS

7 x Risks remain in yellow status with scores between 8 and 9 and these are:

- Data Quality
- Data availability (Accessibility of Data)
- Clinical Records Incomplete
- Insufficient Resource – Capital & Revenue
- UHB Standard Data Processing
- Governance framework (IG policies and procedures)
- Non-Compliance with data protection legislation

1 x Risk remains in yellow status with a score of 4

- Effective resource utilisation

Recommendation:
The Board / Committee are requested to: NOTE progress and updates to the Risk Register report.

Link to Strategic Objectives of Shaping our Future Wellbeing: *Please tick as relevant*				
1. Reduce health inequalities		6. Have a planned care system where demand and capacity are in balance		
2. Deliver outcomes that matter to people	x	7. Be a great place to work and learn		x
3. All take responsibility for improving our health and wellbeing	x	8. Work better together with partners to deliver care and support across care sectors, making best use of our people and technology		x
4. Offer services that deliver the population health our citizens are entitled to expect	x	9. Reduce harm, waste and variation sustainably making best use of the resources available to us		x
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives		x

Five Ways of Working (Sustainable Development Principles) considered *Please tick as relevant*									
Prevention	x	Long term		Integration		Collaboration	x	Involvement	

Impact Assessment: *Please state yes or no for each category. If yes please provide further details.*
Risk: Yes/
As outlined in the risk register
Safety: Yes
Financial: Yes
Non-compliance and less efficient ways of working
Workforce: Yes
Impacts on ways of working
Legal: Yes
Compliance with regulatory requirements
Reputational: Yes
Trust of staff and patients/service users
Socio Economic: Yes/No
Equality and Health: Yes/No
Decarbonisation: Yes
Green IT and digital solutions that support greater virtual working

Approval/Scrutiny Route:		
Committee/Group/Exec	Date:	

RISK REGISTER TEMPLATE

CLINICAL BOARD/CORPORATE DIRECTORATE: | **CORPORATE**

SPECIALITY/DEPARTMENT: | **Digital & Health Intelligence**

Risk Ref.	Strategic Objective	Date risk added dd/mm/yyyy	Risk	Exec Lead	Initial Risk Rating			Controls	Assurances	Current Risk rating			Gaps in Control	Gaps in assurance	Actions	Who	When	Target Risk rating			Date of next review	Assurance Committee
					Consequence	Likelihood	Total			Consequence	Likelihood	Total						Consequence	Likelihood	Total		
A4/0023	8	06/08/2011	**Cyber Security** - Due to prevailing national and international Cyber Security threats there is a risk that the Health Board's IT infrastructure could be compromised resulting in prolonged service interuption and potential impacts on the safety of patients due to an inability to access electronically stored data.	Director of Digital and Health Intelligence	5	4	20	The UHB has in place a number of Cyber security precautions. These include the following: - The implementation of additional VLAN's and/or firewalls/ACL's - Segmenting and an increased level of device patching. - The use of Monitoring and Vulnerability Softare - Health Board wide Mandatory Cyber Security Training and Phishing Campaigns.	Regular Cyber Security updates that review the Health Board's preparedness for a cyber attack and the controls in place are undertaken in the following forums: - at fortnightly Operational Cyber Group Meetings - at monthly Cyber Security Meetings - at each private and public Digital Health and Intelligence Committee An Assessment of the Health Board's Cyber Assessment Framework was undertaken in January 2022 with 4 Critical Priority Areas and 6 Significant/Moderate Priority Areas recommended.	5	4	20	Additional resources is required to fully implement recommended areas of best practice. Completion of mandatory Cyber Security training is below the required level.		The requirements to address the resourcing of Cyber Security Management have been acknowledged in an approved but unfunded UHB Business Case. (May 2022: Successful business case bid made to BCAG to ensure appointment of dedicated Cyber resources. Roles are currently being advertised and recruited to. Global cyber threat increase in response to events in Ukraine. Implementation of NIS Regulations provides powers to WG to penalise organisations who are non-compliant with fines up to £17m or 4% of turnover. Continued efforts need to be made to improve compliance with the Health Board's Cyber Security Mandatory Training and to increase awareness of and engagement with the Health Board's Phishing Campaigns. Compliance with/completion of Cyber Resilience Unit Recommendations. September 2022 : Two of the 4 roles have been appointed to. The remaining posts are in the recruitment process. Jan 2023 - We have successfully appointed a Cyber Security Manager and we anticipate a start date mid February. One of their main priorities will be to implement the improvement action plan May 2023 update - Cyber Security Manager post to be re-advertised. Second phishing simulation email sent to all staff in March 2023. New malware incident SOP developed. July 2023 update: IT Security Officer appointed and due to commence in post August 2023. This post will support the UHB with its NIS compliance and allow the cyber analysts to prioritise security monitoring. Further work is being done to the Cyber Security Manager role to achieve a higher banding before re-advertising September 2023 update: IT Security Officer in post. This allows the Cyber Security Analysts to concentrate on proactive monitoring. A number of Cyber Security awareness sessions delivered by the IT Security Manager have been presented to a number of platforms, including HIF and Digital Coordinators groups. **January 2024 update: Cyber Security Manager now re-banded and currently being advertised. This new post will operational lead the Cyber team strengthen the UHB's cyber security posture. A further phishing simulation was launched in October to continue raising cyber security awareness. In February, we also promoted 'vishing' training to all staff.**	Head of IG & Cyber Security	August 2022 Ongoing	5	3	15	01/07/2022	Digital Health Intelligence Committee
A4/0025	8	10/07/1905	**WCCIS2:** The National procurement appears intent to procure a basic/limited product for Mental Health services. Drivers for this include BCU asking for 'limited/out of the box' products to move them off paper and 20yr old solutions. An immaturity of awareness of a full M.H service requirement is also at play within DHCW/National Programme Team. The implications of an immatured M.H solution being annointed by Wales (in a procurement that seeks the cheapest option against a suite of immatured requirements) is that CaV will have no upgrade/migration path for PARIS (which can only exist in current model until c2030). If CaV fall out of the National procurement, then no W.G supportive funds will be available to support the uHB in a replacement for PARIS.	DT			0	The uHB have led on the establishment of a Regional Digital Board, which has remit over WCCIS2. A WCCIS2 Regional Programme Lead is employed (Tim Evans) to maintain contact in and out of the National programme, however, huge concern exists due to the fact that DHCW manage the funding of WCCIS2, leading to a situation that if CaV do not take the option served up, no funding or onwards integration resource will be available for a local/regional procurement.	No assurance exists. The uHB Executive team are required to support an escalation letter to DHCW asking for assurances to be given to CaV that at least one matured product will exist on the National framework.	4	3	12		uHB level involvement to bring assurance to CaV concerns is required.	**January 2024 - A uHB letter outlining this concern is with David Thomas, Angela Parratt and Cath Doman (Dir, Integrated Health and Care) to escalate to Execs to drive assurance at DHCW and W.G**	Head of Digital Services Management				0		

ID	Score	Date	Risk Description		Controls/Mitigation		Score columns				Update/Progress	Owner					
A3/0110	8	13/12/201	**Server Infrastructure** The IM&T Department is actively implementing a vFarm infrastructure that significantly reduces costs whilst dramatically increasing resilience of Server Systems. However, the cost savings are to the Health Board as a whole and Service Departments in particular and come at an increased cost to IM&T specifically. This infrastructure requires core investment to complete and revenue based support to maintain. There is a requirement to also retain a minimal number of physical servers for those systems not capable of virtualisation.	DT	The UHB continues to address priority areas in relation to its infrastructure management and strategic programme.	0	4	2	8		Jan 2023: Servers, racking and UPS devices have all been purchased. We are waiting for electrical work to be completed in Woodland House and UHL to implement. This action is currently sat with CAV CEF. May '23: Installation of the new additional Disaster Recovery locations is pending. This is due to Capital, Estates and Facilities electrical work still being outstanding. This work is planned for June and July 2023. When complete there will be DR Infrastructure located at UHL and Woodland House. July 2023: Electrical work has been completed within CRI and Woodland with UPS devices and new racks comissioned. UHL is planned for mid Aug due to complexity. The first DR and secondary production equipment is planned to be installed in Woodland House in late Aug 23. Sept 2023: Woodland House electrical work completed, planned network connectivity upgrades in Oct will allow the DR/Backup site to be used. UHL electrical work and UPS installation delayed by CEF due to other comitments. Planned for completion by the end of Sept 2023. **Jan 2024: Electrical work has been completed and A/C units installed. Servers and Services will be moved in a phased approach to UHL and Woodland House Q2/3 2024/25.**	Head of Digital Operations				0	
	8	28/09/2015	**Outcome Measures:** Risk: Unavailability of full, consistent care delivery information results in an inability to ascertain outcomes of care we provide, and commission, plan and improve services accordingly. Consequence - Low assurance on safety, quality and effectiveness of services and satisfaction with services, sub optimal decision making, inability to execute policy and strategy, reputational damage.	DT	Analysis and wider engagement and communication of outcome and audit data, triangulated with efficiencies and effectiveness data as part of Medical Director led programme established. UHB and national investment in data repositories and clinical forms will support programme	0	3	3	9		Acceleration of programme. This will be addressed via the Digital Strategy enablers programme and clinician and analyst channels programme boards (Oct 2020). Jan 2021: both channel programme boards established and will drive the programme. September 2022: Digital Strategy seen as a key enabler to support the UHB's wider strategic programmes. Raodmap and investment plan shared withg Execs, SLB and Board. Jan '23 - Data Improvement Group established by Director of Digital and Health Intelligence Director and Director of Finance; initially baselining of patient data that is captured across the UHB - will then focus on completeness and quality of the data. May '23: It's been agreed to focus on 4 specialities to do a deep dive into their use of systems to collect and report/analyse data - a model that can be applied to other areas. Jul '23. Interviews have been arranged with Endoscopy, Physio, Orthopaedics, General Surgery and PCIC between 19-Jul-23 and 31-Jul-23. Interview responses will be analysed and brought back to the next data improvement meeting on the 08-Aug-23 for discussion and agreeing next steps. Sept '23: Following the data improvement interviews a common theme is that many services are validating their waiting lists. There is an opportunity to develop a tool to reduce this admin burden. Several additional data improvement interviews have been arranged to ensure we are capturing the requirements of the services. **Jan 2024: This work is being absorbed into the Data Insights development mechnisim looking at current and future data insights provision with work to prduce a data strategic plan strategy by Qtr 2 24/25.**	Head of Architecture and Analytics and Head of Business Intelligence				0	
A4/0024	8	29/01/2021	**The Welsh Pathology Information management system (WLIMS)** implementation has taken longer than envisaed. As a result of this all Health Boards will not have migrated off their legacy pathology systems (Telepath) by end of March 2018, which is when their current telepath contracts will expire (contract currently in extension).	DT	The UHB engaged with NWIS and other Health Boards to evaluate options available to mitigate this risk.	0	4	2	8		May 2022 update: HW and SW contract extended to end of 2025 Sept 2022: Risks associated with the LINC programme ability to deliver have been raised at national CEO level. May '23: LINC programme changes agreed with new plan and timescales being worked up (Sept '23) **Jul '23: CAV Digital Operations are actively working with AWMGS to move the current LIMS environment out of its isolated DMZ and onto the Cymru domain. In parallel to this the Server operating systems and LIMS application are being upgraded. This work is planned to be completed mid-August 2023.** Sept 2023: An agreed solution has been found. The SCC Servers have been moved onto the NHS Wales Domain after AV, Patching and Security checks. This work is due to be completed by Mid/late Sept 2023. **Jan 2024: SCC servers have been added to the domain as per Sept update. NEW Hardware has been commissioned in late 2023 and will be moved to the CICG site Q1 2024/25.**	Head of Operations				0	
	8	19/02/2018	**Data Quality** High level risk - core business activities potentially compromised as a result of weaknesses in assurance framework in areas listed below: Absence of Standard Operating Procedures to administer patient activity, Low take up of staff training in Standard Operating Procedures to administer patient activity, Incorrect/incomplete/late recording of activity Absence of ISO 27001 certification. Consequences: Potential for poorer patient outcomes and experience, analysis and benchmarking flawed resulting in poor decision making, under recovery of income, inability to maximise potential of R&D	DT	Further re-invigoration of the role out of COM2 will increase clinically validated data. Updates and training programme scheduled for mental health and our partners in order to address issues identified in recording and reporting compliance with parts 2 and 3 of the mental health measures. New dashboard release will expose greater amount of data to users, in a more user friendly way, enabling validation by relevant clinicians. Data quality group has established a work plan to improve quality and completeness of data and how it is presented.	0	3	3	9		Data Quality Group needs to be refocussed. It is currently not meeting due to IG staffing pressures. Sept 20 Data Quality will be addressed via the new governance arrangements - specifically the Analyst Channel Programme Board; plans to establish this board in October 2020. Jan 2021: the Analyst Channel Programme board is holding its inaugural meeting in February, chaired by a clinician. May 2022: Working with the CCIO and service leads, a data strategy is being developed to support the digital strategy roadmap plans, which will be produced by Q3 2022/23. September 2022: Data Quality as part of the Data Strategy is being addressed at UHB level comprising baseline position of info/data by November 2022 and a complete audit by March 2023. Jan '23 - CAV UHB position made clear in a written response to the Senedd's sub committees relating to the adoption of the WCCIS' system May '23: Little progress with data strategy writing however, data quality should begin (and can be done in parallel) at the point of collection e.g. systems need to have checks in place when recording data (system enhancements) July '23: Data Improvement Group has wide representation across the Clinical Boards and is focussing on completion of full baseline to identify all data sources Sept '23: The Data Improvement Group have setup interviews with people who can help document known data quality issues and potential improvements. This will form part of the data improvement roadmap **Jan 2024: This work is being absorbed into the Data Insights development work looking at current and future data insights provision with work to prduce a data strategy by Qtr 2 24/25.**	Head of Architecture and Analytics				0	

ID	Score	Date	Risk	Mitigating actions				Score			Progress updates	Owner	
	8	28/09/2015	**Risk: Accessibility of data**: UHB does not have an ability to access and use the data it requires to carry out its full range of statutory obligations and enable delivery of our strategy and IMTP. . Specific risks - lack of access to GP data and the UHB's data residing in NWIS supplied applications (e.g. WCRS, WRRS) Consequence - Inability to deliver strategic UHBs, namely - Supporting people in choosing healthy behaviours, - Encouraging self management of conditions, - Enabling people to maintain or recover their health in or as close to home as possible, - Creating value by enabling the achievement of outcomes and experience that matter to people at appropriate cost, - Enable and accelerate the adoption of evidence based practice, standardising as appropriate	DT	0		Approach identified to work with C&V GPs to share data across care sectors to inform improvement and to gain a better understanding of need, demand and the capacity available to meet it. National data repository programme will provide access to tools and expertise	3	3	9	National Architectural design group and interoperability group being set up in line with Once for Wales agreement and WG Informatics statement of intent should provide medium term solution. HB taking forward data acquisition programme in line with the development of the electronic care record. May 2021: in support of information sharing outside of direct care purposes, agreement has been reached with WAST and Cardiff Council (Social Services) for data to be shared; a similar request to include GP data is currently being considered by the Wales GPC/DHCW. May 2022: Data sharing between CAV UHB, WAST and Cardiff Council's social services being piloted following successfyl test. GP data remains out of scope pending WG review of governance for cross-setting information sharing. September 2022: Information sharing between CAV UHB, Cardiff Council and WAST established. Additionally, the Digital Care Record Group has been established reporting to the RPB Board. Jan '23 - Digital Care Record Group scoped out a work plan for delivering the sharing of information - initially for the "Looked After Children" utilising the LDR May '23: Digital Care Region has scoped out a work plan to create a patient identity management service to enable the safe sharing of patient records between health and social care. A proof of concept was recently developed and is now in the testing phase. Jul '23. DHCW have released in beta 2x APIs (for testing) to access their national documents repository and consumption of their reference data service. The Regional Partnership Board (Digital Care Region) have approached a company called Blackpear who can facilitate the accessing of GP data. Prehab to rehab team and Local Data Resource team are in talks with ViPC to facilitate the accessing of GP data. Sept '23: To date DHCW have released a total of four national beta APIs 1) reference data 2) demographics 3) documents 4) diagnostic results for review and testing by HBs. The Regional Partnership Board Digital Care Region Shared Cared Record continues to make progress with testing to be complete end of September. There will also be several months effort to work through the IG considerations of sharing the data. **Jan 2024: We have started work with DHCW API management team to understand the WRRS API so that we can help Richard Davies (Cardiff and Vale UHB - Anaesthetics) with yearly lab bloods data and Robert McLeod (Cardiff and Vale UHB - ENT) to check if MRI skull scans have been carried out.**	Head of Architecture and Analytics	0
	8	28/09/2015	**Clinical Records Risk**: Clinical records are not joined up across disciplines, care settings or geographical boundaries resulting in incomplete and out of date patient information. Summary information is not routinely shared across systems. Differing local service models which are also going through a period of significant change mean access to appropriate data is an increasing need. Consequence is unsupported clinical decision-making, introducing patient harm and/or disadvantage and failure to meet NHS Wales digital strategy	DT	0		UHB architectural design to be reviewed to consider local data repository for bringing together in a usable way clinical information held in numerous clinical systems. UHB working through a programme to implement once for Wales requirements for data and technical interoperability standards.	3	3	9	National prioritisation for NWIS to open up the national data repositories. Jan 2020: NDR & CDR workshops to understand the technical roadmap this will be picked up via the national IT infrastructure review being undertaken in Feb / March 2020 . The new governance model supporting the Digital strategy delivery will address via the clinician channel programme board, which is being established in October 2020. Jan 2021: The clinician channel programme board has been established and will drive direction and priorities for the NDR/LDR in CAV. May 2021: All Digital strategy channel programme boards established and led by a senior clinician, overseeing the delivery of the CAV Digital Strategy roadmap plans. Jan 2022: NDR Programme Board re-established with a smaller focussed group. CAV represented via Director of Digital & Health Intelligence. September 2022: CAV LDR plan being formalised. Jan ' 23: CAV LDR now live, data started to be ingested, albeit to support mostly operational reporting. Low head count in LDR stifling pace of delivery, in particular the development of a summary record shared across multiple domains. May '23: The LDR workload has been steadily increasing overtime to a point where customers are unhappy with the support and pace of delivery. Currently there are 28 projects WIP (1,620 days of effort to complete), 4 projects on-hold (120 days of effort to complete) and 41 projects on the backlog (1,980 days of effort to complete). The resource to carry out these projects are 2 x WTE and 2 x 0,5 WTE, which is impeding the pace of delivery and support Jul '23. A consultancy company that provides enterprise architecture services is helping to document and design the future UHB landscape. The data improvement group will be interviewing 5x services to determine how they use systems (or paper) in their daily workflows.Their responses will be analysed to determine the wider architectural work. Sept '23: The data improvement working group is supporting the mapping out of all patient data captured across the UHB in all formats. The output of this work will inform the enterprise actitechture plans for supporting the timely sharing of data across different systems, services and organisations at a system wide level **Jan 2024: The data quality working group have conducted several interviews with various parts of the organisation to determine how they use data and in what systems. The group will meet on 12-feb-2024 to review these findings and set the next objectives. The Digital Care Region demonstrated at the 1st regional board meeting, a proof of concept website combining health and social care data into a single record, which was well received, next steps are to introduce more data, this time for looked after children.**	Head of Architecture and Analytics	0
A2/0004	8	13/12/2013	**Insufficient Resource:** The delivery of the IM&T Strategic Work plan is based on the UHB being able to ensure that the IM&T Department is appropriately resourced to manage infrastructure and deliver projects. All bench marking information indicates that the UHB is significantly under resourced in this area. Consequence: Inability to support operational and strategic delivery at pace required, reliance on outsourcing at enhanced cost, non compliance with legislation (FOI / GDPR)	DT	0		The UHB continues to address priority areas in relation to its infrastructure management and strategic programme.	3	3	9	Jan 2021: Discretionary capital allocation for Digital has been restored to £500K for 20/21. The UHB is also actively engaged with Welsh Government in undertaking a review of National Infrastructure requirements as part of the plans to increase Digital investment in Wales. In addition the Digital infrastructure 5 year sustainability plan has been updated to ensure that highest priority risks are addressed first with any available funding. The D&HI directorate has also been successful in gaining in excess of £1m additional revenue funding from the UHB for 20/21 and there are bids being considered for recurring additional revenue. May 21 Update: Year end funding of in excess of £2m plus earlier allocations in support of COVID has allowed to HealTh Board to plan to enahnce its Digital Device infrastructure. There is however a great deficit going forwards between the anount of Discretionary capital allocated to Digital and the requirements to sustain our infrastructure. This has been highlighted to Capital Management Group and included in the Digital services Case for Investment plan submitted to management executive in December 2020. Sept 21 - A staff gap analysis has been carried out in DH&I. Significant shortfalls has been identified and formalised within the report being presented to CAV UHB Exec Board by the Director of DH & I Jan 2022 update: A submission on resourcing was submitted to management Exec in November but was only funded on a non recurring basis to end of March. Further submissions are being prepared for consideration by the Business Case Assessment Group (BCAG) May 2022: D&HI and Finance teams have reviewed current structures and cost base and developed a plan to resource priority areas already idetnfiied as critical ; these are under consideration by the DoF and likely to require business cases for submission to BCAG. Sept 2022: succesful bids to BCAG have resulted in additional investment in the Digital Operational team, 365 team and WiFi team. Unfunded cases comprise of information and project/service delivery requirement resources. These will be reviewed and built into the longterm financial model work being led by the Director of Finance. Jan '23: Implementation of the Digital Stragies work plan (Road map) continues to be dependant on addequate resources; a process of prioritising organisational programmes of work is currently undertaken May '23: Digital investment challenges to be discussed in private session of DHIC on 30.05.23. Governance changes proposed to manage the process of sequencing to be in place by July 2023. July '23: Digital roadmap and Digital Information Programme proposals presented and discussed at Board on 27.07.23. Agreement that investment cases should feed into the long term financial plan (DDHI & EDOF to action) Sept '23: outlined investment cases developed which will be presented to the UHB Investment Group in November 2023. **Jan'24: Proposal developed and presented to CMG in December 2023. 'Case for Investment' setting out the request for capital monies in 2024/25 to develop the business case for longer term investment. Being reviewed at February 2024 CMG meeting.**	Director of D&HI	0

Risk	Date	Owner		Controls/Assurance		Score			Progress/Updates	Lead
8	16/02/2018	**UHB Standard Data Processing** Risk: obligations and accountabilities relating to the way data is handled are not formalised Consequence: the UHB could suffer detriment and/or have difficulties applying remedies against a third party if data is not handled appropriately	DT	0	Library of outline documents for sharing data available, with completion of these supported by corporate information governance department. Requirements to use and refer to are being emphasised within the training.	4	2	8	Procurement are greatly assisting process by referring all issues involving data sharing to the corporate IG department. September 2022: Procedures improved via the IG Working Group whereby new data requests for data sharing are reviewed and actioned in a consistent manner. January 2023 update: IG Dept due to provide a presentation to the Procurement Dept January 2023 on requirements to ensure IG and cyber security are satisfied when third parties are enlisted. May 2023: No further update Jul '23: Digital Care Region has scoped out a work plan to create a patient identity management service to enable the safe sharing of patient records between health and social care. A proof of concept was recently developed and is now in the testing phase. Sept '23: No further update **Jan '24: work progressing in developing a data strategy to support the Data Insights plan to address completeness and quality of data in our clinical systems.**	Director of D&HI 0
8	16/02/2018	Risk: **IG policies and procedures** are not up to date/do not cover all relevant areas. Procedures are not aligned to relevant national policies. Consequence: Lack of clarity in terms of how the UHB expects its staff to work to in order for relevant accountabilities to be discharged.	DT	0	Update: Controlled document framework requirements delayed due to resource constraints - Integrated IG policy is live and covers a number of existing policies.	4	2	8	Restructuring of IG department will increase amount of expert resource. Investment in training will also increase available expertise to support the review of policies. A formal review of policies and procedures is underway as per risk #7. May 2022: Controlled documents are reviewed and action plans for refresh or updates are routinely captured and reported on at each DHIC meeting. September 2022 update: A third party has been enlisted to update existing policies and implement new SOPs were we are have identified gaps in our processes. This work is progressing with updates reported to DHIC. January 2023 update: A number of existing procedures have been updated and two new ones created. These will be presented to DHIC in February 2023. May 2023 update: 10 policies/procedures/guidelines updated and presented to Feb 2023 DHIC. A further two documents currently in the process of being reviewed/updated. July 2023 update: The Records Management Policy has been updated and is being brought to DHIC in August 2023. Additionally, the Records Management Procedure and Transportation of Casenotes and PII Procedure have been updated. September 2023 update: Records Management Policy ratified by DHIC in August 2023. Also approved were the Records Management Procedure and Transportation of Casenotes and PII Procedure. **January 2024 update: Overarching Informatiion Governance Policy being presented to DHIC (February 2024) with proposed changes.**	Head of IG & Cyber Security 0
8	28/09/2015	Risk:- **Non compliance with Data Protection & Confidentiality Legislation** - the UHB's progress in taking forward the action plan to reduce the risk of non compliance following the ICO's assessment of our 'reasonable assurance' with the GDPR/ DPA is not sufficient to mitigate the risk of non compliance with Data Protection Legislation. Consequence: Mistrust of our population and other stakeholders resulting in their unwillingness to share / divulge essential information, Significantly financial penalties - and increasing post BA case	DT	0	Clinical Board assurance and co-ordinated mitigation of risk being developed via quality and safety meetings. Ownership and community of practice anticipated to develop across IAOs/IAAs from this. GDPR awareness being used to ensure Leaders and asset owners are reminded of existing requirements and mandatory nature of the asset register. Options for enabling messaging in compliance with legislation has been considered by clinical and executives on a number of occasions, and UHB close to agreement.	4	2	8	Restructuring of IG department will increase amount of expert resource. Resolution of long term absence will also increase available expertise and resource to support GDPR plan, and manage the operational requirements on the corporate department. Ongoing implementation of GDPR/ICO action plan. The Information Governance team have developed a work plan to review and update all outstanding policy and procedure documents in the CDF and these are scheduled to be complete by December 2020. Implementing the action plan will reduce the risk, May 2021: policies are being reviewed and an update will be reported to DHIC in June 2021. Sept 2021: Business case being presented to appoint further IG support to support with CB engagement. Jan 2022: Additional non-recurring funding made available until 31.03.22. Recurrent funding bids are being prepared for consideration by the Business Case Assessment Group (BCAG) May 2022: Review of all mandaorty training being done in June to ensure that IG and cyber training are prioritised. September 2022 update: Following a 6 month program of work, staff accessing their own records and family records has fallen by 76% and 65%, respectively. The UHB is required to ensure that it has appropriate security controls in place to protect patient data. January 2023 update: There continues to be a decrease following targetted comm in the number of staff accessing own and family records (80% & 75% respectively) May 2023 update: Ongoing work tackling inappropriate access to clinical systems with access to own and family records reduced by 76% and 85%. July '23: IG Mandatory training for Cardiff and Vale staff continues to increase. NIAS compliance has improved as a result of awarness raising September 2023 update: IG Mandatory training now at 76% across the workforce. NIIAS monitoring continues with over >750 letters sent to staff on behalf of the Caldicott Guardian regarding inappropriate access. **January 2024 update: The Information Governance Dept is focusing on a number of proactive tasks that are outstanding. Once in place, the risk of GDPR non-compliance will reduce. These will be completed by Qtr 22 24/25.**	Head of IG & Cyber Security 0
8	01/10/2018	**Effective Resource utilisation** :With an increasingly restricted resource, the UHB requires assurance that digital effort is expended in the most benefits laden workload. Benefits based prioritisation requires robust and matured benefits tracking and a matured reprioritisation mechanism. This requires some changes of technique within the Digital department.	DT	0	Establishment of a formalised corporate prioritisation mechanism based on benefits and corporate drivers for change.	4	1	4	Jan 2023: A PM for the DFD project has been employed until Mar 23. The project has come to a partial completion awaiting recruitment of a dedicated staff member to assist with request triaging. May 2023: A new Head of Digital Services Management post has been created and new PMO team and function as well as process has been agreed by the CAVUHB Senior Digital Management team. July '23: Digital Advisory Board established as group representing all Clinical Boards focussed on prioritisation of work requests. Sept 2023: Change Management is currently being piloted by the Digital Operations teams (Starting with the Server Team) Sept 2023. Depolyment to the rest of Digital Operations is expected by Oct/Nov 2023. **Jan 2024: After a successful pilot and test within the Server Team, other Digital Operations teams are using the new Change Management Process with a view to deploy to the wider Digital teams Q2/3 2024.**	Head of Digital Operations 0

Report Title:	IG Data & Compliance (SIs, Data Protection, GDPR, FOI, SARs, staffing and mandatory training)			Agenda Item no.		2.3
Meeting:	Digital & Health Intelligence Committee	Public	X	Meeting Date:		20th February 2024
		Private				
Status *(please tick one only):*	Assurance	X	Approval		Information	
Lead Executive:	Director of Digital & Health Intelligence					
Report Author (Title):	Head of Information Governance and Cyber Security					

Main Report Background and current situation:

This report considers key information governance issues considered by the responsible Executive Director, Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO). Specifically, it provides information on the following areas of Information Governance within Cardiff and Vale University Health Board (the UHB).

- Information Governance (IG) Staffing levels and capacity
- Data Protection Act - Serious Incident Summary and Report
- Freedom of Information Act - Activity and Compliance
- Data Protection Act (DPA) - Subject access requests (SAR)
- Compliance monitoring/National Integrated Intelligent Auditing Solution (NIIAS)

Each individual report contains specific details relevant to the subject area, and includes updated information since the previous report to the Digital Health Intelligence Committee (DHIC) on how the UHB has complied with the obligations of each piece of legislation that satisfy the information governance requirements.

The UHB is required to ensure that it complies with all the legislative requirements placed upon it. In respect of Information Governance, the relevant legislation which largely impacts on this work are the Data Protection Act 2018 (DPA), UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000 (FOIA).

Quarterly reports are produced for the DHIC to receive assurance that the UHB continues to monitor and action breaches of the UK GDPR/DPA 2018, FOI requests and that subject access requests (SAR) are actively processed within the legislative time frame that applies and, that any areas causing concern or issues are identified and addressed.

ASSESSMENT

1. **Information Governance Staffing Levels and Capacity**

Information Governance staffing levels remain stable but continue to be challenged with the current workload.

The staffing structure is as follows:

- David Thomas, Director of Digital and Health Intelligence is the Senior Information Risk Owner
- Professor Meriel Jenney, Medical Director, is the Caldicott Guardian
- James Webb is the Data Protection Officer
- The Information Governance Department is currently resourced at 5 WTE.

2. Data Protection Act – Serious Incident Report

Date reported: September 2023 to January 2024

Between September 2023 and January 2024, the Information Governance Department have reviewed a total of 279 information governance related incidents reported via Datix. On average, for the last 12 months, the Information Governance Department reviews approximately 51 incidents per month. Of these breaches reviewed during this recent period, 4 of these breaches met the threshold to be reported to the Information Commissioner's Office (ICO). Additionally, the UHB has received two complaints from the ICO concerning the way the UHB has handled two subject access requests. The details of these breaches are outlined in the private setting of this committee.

3. Freedom of Information Act

FOI compliance percentage for the last rolling 12 months against the 20-working day deadline is demonstrated as follows:

Freedom of Information Requests

Legend: Compliance % — Requests
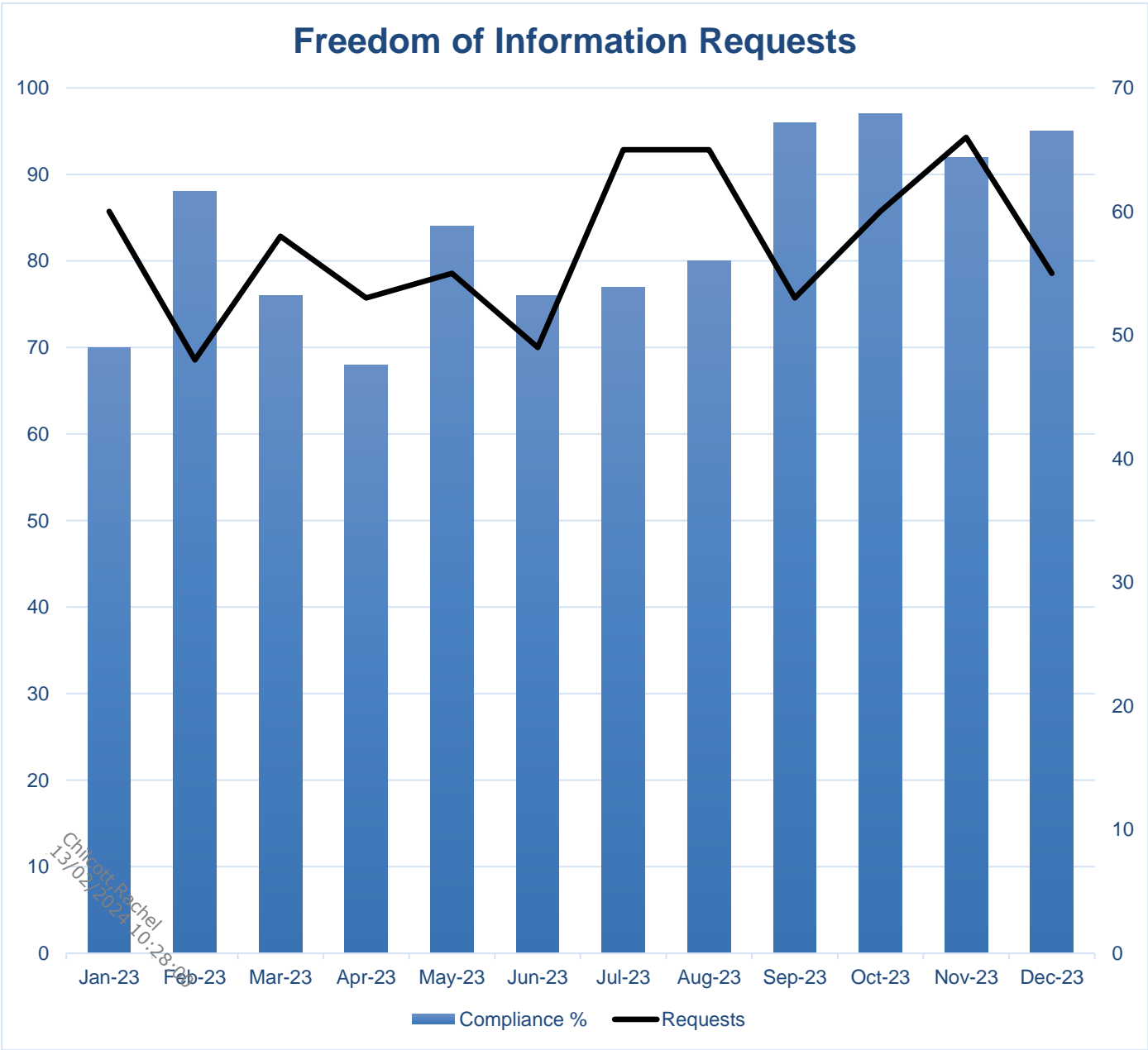
The average number of FOIs received during the last 12 months has slightly increased to 57 requests per month (from 55) and average compliance has slightly increased to 83% from (82%). FOI compliance for August to December 2023 was 80%, 96%, 97%, 92% & 95%, respectively.

A link to the UHBs FOI disclosure log can be found below. This provides a link to every FOI the UHB publishes online. In the event that requests are made for the same information, the UHB is able to signpost requestors to this log.

https://cavuhb.nhs.wales/about-us/governance-and-assurance/freedom-of-information/disclosure-log/

4. Subject Access Requests Processed

4.1 Health Records requests

Medical Records SAR compliance percentage for the last rolling 12 months against the one-month deadline is demonstrated as follows:

Subject Access Requests for Medical Records
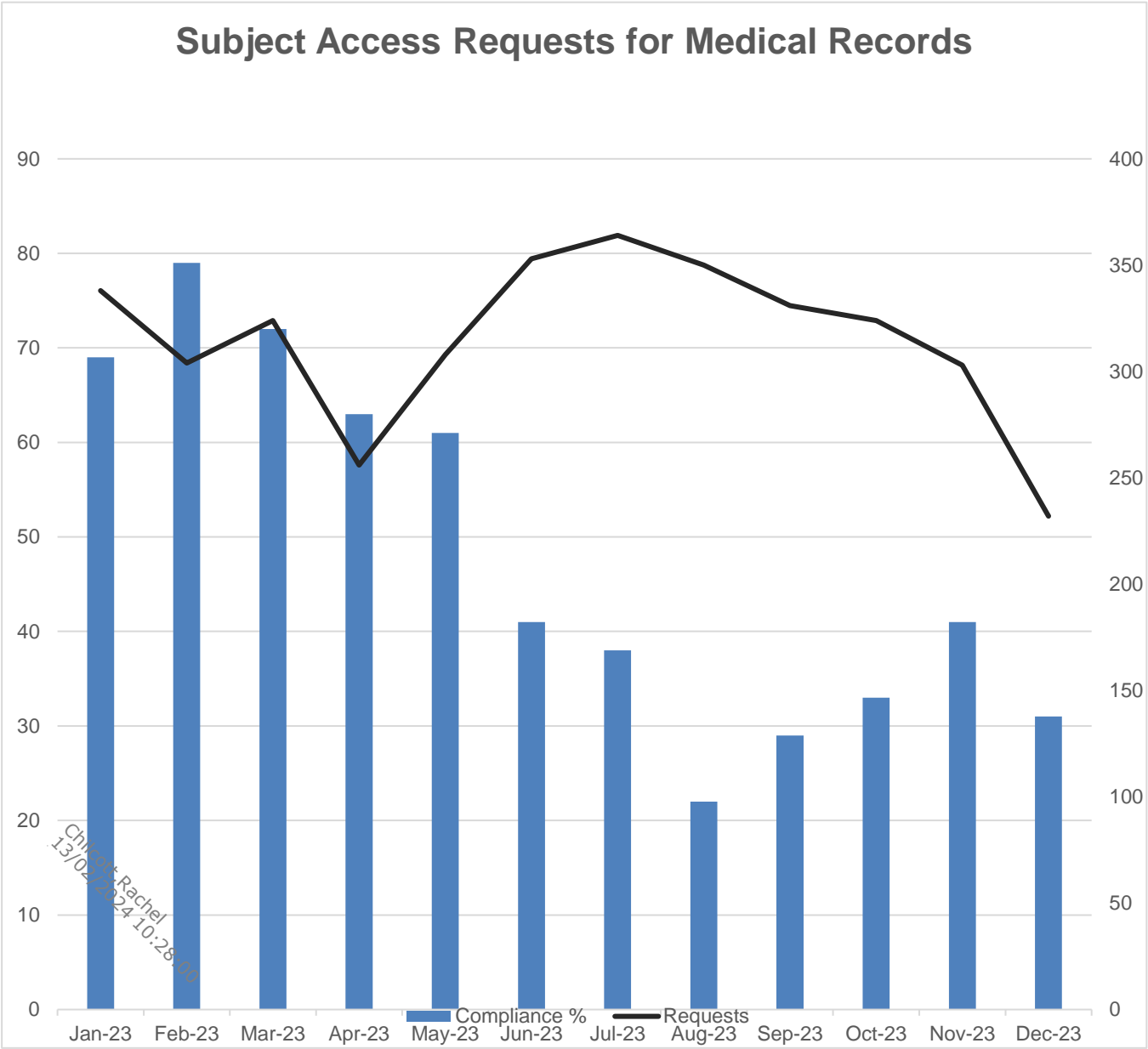
The number of requests has steadily dropped since July 2023. Compliance remains a cause of concern averaging 48% (a drop from 60%) over the last rolling 12 months. During this time an average of 316 requests have been submitted each month (an increase from 302).

The team continue to manage a number of absences caused by sickness and recruitment vacancies.

The Access to Records team have commenced a local improvement program with an agreed action plan which is beginning to demonstrate an improvement since. In addition to this, the Subject Access Request Digital Front Door is remains in alpha testing. There will be a phased roll out following a successful pilot.

4 .2 Non-Health Records

A total of 63 subject access requests submitted for non-health records were received from August 2023 to December 2023. 61 requests (97%) were complied with, within the legislated timeframe.

5. Compliance Monitoring/NIIAS

Since January 2022, the UHB has sent out a total of 886 letters to staff who have been identified by the UHB's instance of the National Intelligent Integrated Audit Solution (NIIAS), based on a process approved by Management Executive.

These letters form part of an approach which also includes a wide-reaching and targeted comms program of work. Further detail will be provided in the private committee agenda.

6. Information Governance Mandatory Training

Overall UHB Information Governance training compliance is currently 76% and is broken down by Clinical Boards as follows.

Org L4	Assignment Count	Achieved	Compliance %
001 All Wales Genomics Service	331	282	85%
001 Capital, Estates & Facilities	1450	1249	86%
001 Children & Women Clinical Board	2414	1884	78%
001 Clinical Diagnostics & Therapeutics Clinical Board	2617	2098	80%
001 Corporate Executives	1100	877	80%
001 Medicine Clinical Board	1999	1384	69%
001 Mental Health Clinical Board	1549	1039	67%
001 Primary, Community Intermediate Care Clinical Board	1167	927	79%
001 Specialist Services Clinical Board	2228	1655	74%
001 Surgical Services Clinical Board	2408	1652	69%
UHB	**17263**	**13047**	**76%**

The overall figure does not represent a change in overall completeness since figures were last provided to the last two Committees.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

- Information Governance resource remains unchanged since the last committee meeting.
- 279 information governance related incidents reviewed from September 2023 to January 2024.
- 4 data breaches since the last committee have been reported to the Information Commissioner's Office.
- Freedom of Information compliance marginally increased to 83% for last 12 rolling months.
- Requests for access to medical records has fallen since July 2023 but compliance has dropped to 48%.
- The Information Governance Department continues to send letters to staff who breach data access policy.
- Information Governance mandatory training remains at 76%.

Recommendation:

The Board / Committee are requested to:

- RECEIVE and NOTE a series of updates relating to significant Information Governance issues

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1. Reduce health inequalities	X	6. Have a planned care system where demand and capacity are in balance	
2. Deliver outcomes that matter to people	X	7. Be a great place to work and learn	x
3. All take responsibility for improving our health and wellbeing	X	8. Work better together with partners to deliver care and support across care sectors, making best use of our people and technology	x
4. Offer services that deliver the population health our citizens are entitled to expect	x	9. Reduce harm, waste and variation sustainably making best use of the resources available to us	x
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives	

Five Ways of Working (Sustainable Development Principles) considered
Please tick as relevant

Prevention	x	Long term		Integration	x	Collaboration	x	Involvement	x

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: Yes
Compliance with legal and mandatory requirements
Safety: Yes
Supports patient and staff safety
Financial: Yes
Non-compliance

Workforce: Yes	
Applies to entire workforce	
Legal: Yes	
compliance	
Reputational: Yes	
Confidence in managing assets/supporting services	
Socio Economic: Yes/No	
Equality and Health: Yes/No	
Decarbonisation: Yes/No	

Approval/Scrutiny Route:	
Committee/Group/Exec	Date:

Chilcott Rachel
13/02/2024 10:28:00

Report Title:	**Digital Services Key Performance Indicators**			Agenda Item no.	**2.4**	
Meeting:	**Digital and Health Intelligence Committee**	Public	X	Meeting Date:	20th February 2024	
		Private				
Status *(please tick one only):*	Assurance		Approval		Information	X
Lead Executive:	**Director of Digital and Health Intelligence**					
Report Author (Title):	**Director of Digital and Health Intelligence**					

Main Report
Background and current situation:

As reported previously, the Service Desk tool "Ivanti" continues to be developed and used by the D&HI teams to receive and manage service requests, incident reports and change requests. Easy access to the tool provides all CAV UHB staff and a means to inform the digital team of issues and a variety of general and specialist requests for help or advice.

At the last DHIC meeting the power BI reporting was demonstrated showing a wide collection of data being gathered for lag based KPI reporting. The aim is to provide this as a web mounted accessible report for key colleagues and to expand and share management information on the performance of the D&HI directorate's full range of services.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

The Ivanti system continues to act as the 'digital front door' for most of the D&HI services and the development of reporting functionality is useful in demonstrating user demand, service responses and how resources are deployed.

The reporting functionality gives increased details on the volume of Service Requests, Incident Reports, Automation Requests, etc. These details are contained within the Ivanti Management Report which is listed as Appendix 1 and which will be presented in more detail at the DHIC meeting itself.

As we continue to improve services, we will develop the Ivanti system and its reporting capability. The aim is to include specific core metrics as part of the organisation's integrated performance report as a key enabler to supporting operational performance.

Recommendation:

The Committee is requested to:

REVIEW and NOTE the progress since the last update on the Ivanti service desk tool in relation to KPIs.

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1. Reduce health inequalities			6. Have a planned care system where demand and capacity are in balance		
2. Deliver outcomes that matter to people	x		7. Be a great place to work and learn		X
3. All take responsibility for improving our health and wellbeing			8. Work better together with partners to deliver care and support across care sectors, making best use of our people and technology		X

4. Offer services that deliver the population health our citizens are entitled to expect		9. Reduce harm, waste and variation sustainably making best use of the resources available to us	X
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives	

Five Ways of Working (Sustainable Development Principles) considered *Please tick as relevant*							
Prevention		Long term		Integration		Collaboration	x
Involvement	x						

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: Yes

– service non-availability is reduced through faster logging and response times

Safety: No

Financial: Yes

– provides a more effective use of resources

Workforce: Yes

– provides more effective support to all users of Digital Services

Legal: No

Reputational: Yes

– enables the service to demonstrate performance against targets and to publish performance on a routine basis

Socio Economic: No

Equality and Health: No

Decarbonisation: No

Approval/Scrutiny Route:

Committee/Group/Exec	Date:

Chilcott Rachel
13/02/2024 10:28:00

Ivanti Management Report

View in Power BI ↗

Last data refresh:
09/02/2024 11:20:09 UTC

Downloaded at:
09/02/2024 11:50:50 UTC

The following slides will show stationary screen shots of the data being captured from Ivanti and displayed in Power BI for the reporting of Lag Key Performance Indicators within DH&I. We have more request offerings available on the Digital Self Service Portal than ever before.

Information for this report was pulled on the 9th of February 2024.

This will include
- Service Request information Yearly, and Monthly.
- Incident Report information Yearly, and Monthly.

Key Items to Note
Service request - a dramatic increase in service requests from last year to current.
Incident Reports – a much smaller increase
Automation Requests - an increase in the automated creation of Nadex accounts with September 2023 recording higher figures.

Executive Scorecard

Year 2022		Current Year		Current Month	
Incidents	**Requests**	**Incidents**	**Requests**	**Incidents**	**Requests**
23101 Incidents Opened	**16689** Requests Opened	**36858** Incidents Opened	**38530** Requests Opened	**2588** Incidents Opened	**2821** Requests Opened
23074 Incidents Closed	**15221** Closed Requests	**36454** Incidents Closed	**34186** Closed Requests	**2576** Incidents Closed	**2441** Closed Requests
27 Remaining Open	**1468** Remaining Open	**404** Remaining Open	**4344** Remaining Open	**12** Remaining Open	**380** Remaining Open
6.96 Avg Duration (Days)	**13.40** Avg Duration (Days)	**4.34** Avg Duration (Days)	**6.14** Avg Duration (Days)	**5.85** Avg Duration (Days)	**9.98** Avg Duration (Days)

Executive Trending

Requests
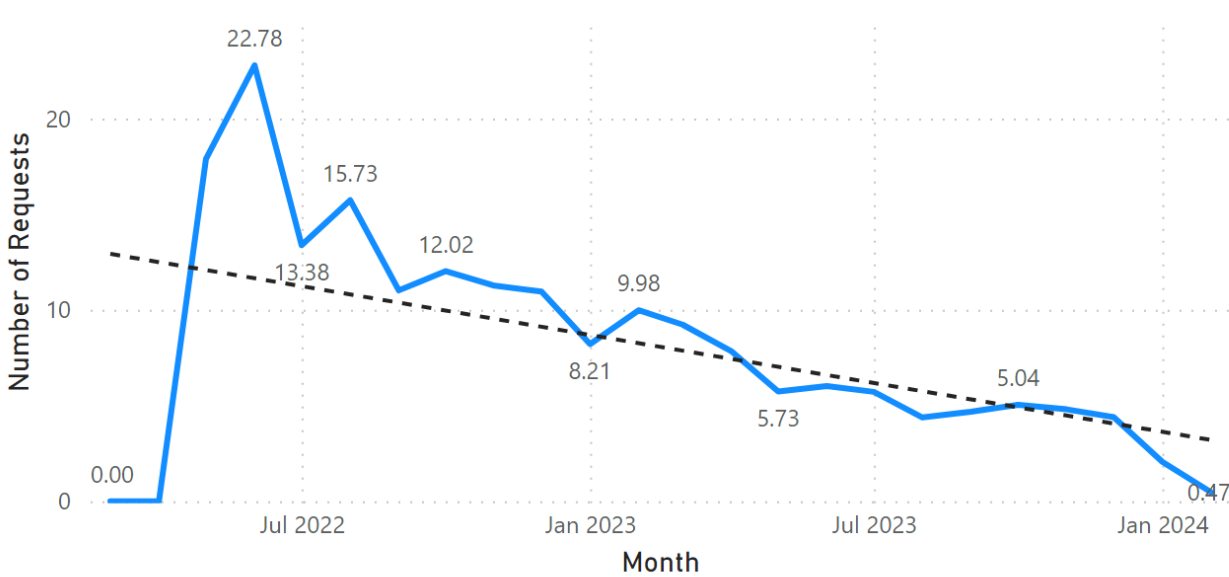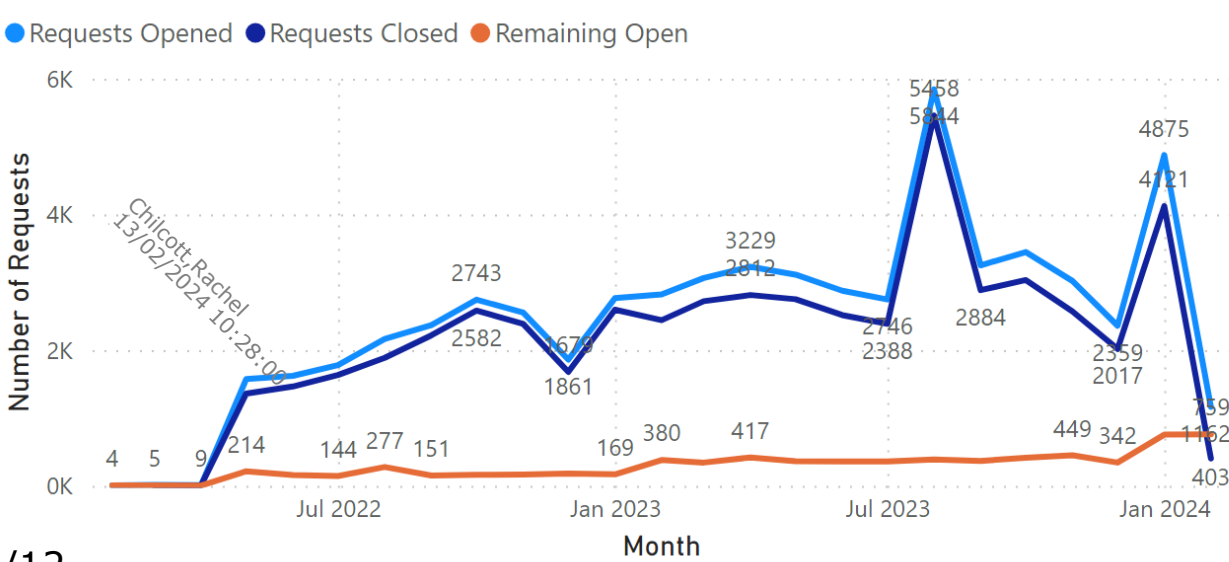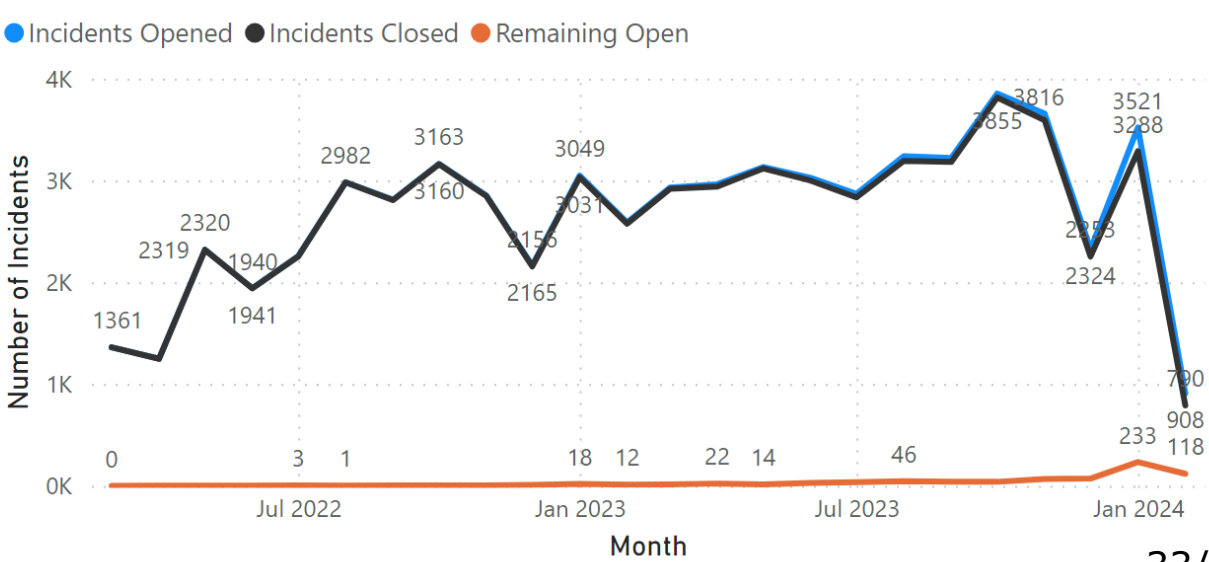
Average Duration (Days)

Requests Opened, Closed and Remaining Open

- Requests Opened
- Requests Closed
- Remaining Open

Incidents

Average Duration (Days)
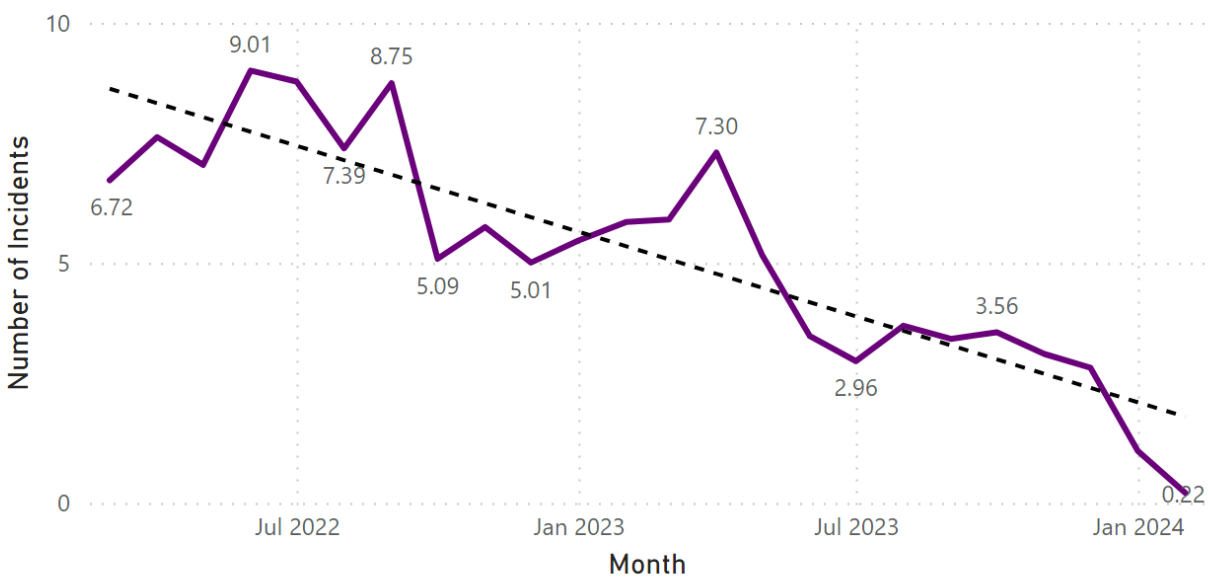
Incidents Opened, Closed and Remaining Open

- Incidents Opened
- Incidents Closed
- Remaining Open

Service Desk Scorecard

Year 2022		Current Year		Current Month	
Incidents	**Requests**	**Incidents**	**Requests**	**Incidents**	**Requests**
12554 Incidents Opened	**10607** Requests Opened	**14832** Incidents Opened	**25032** Requests Opened	**972** Incidents Opened	**1961** Requests Opened
12552 Incidents Closed	**9747** Closed Requests	**14769** Incidents Closed	**23248** Closed Requests	**971** Incidents Closed	**1730** Closed Requests
2 Remaining Open	**860** Remaining Open	**63** Remaining Open	**1784** Remaining Open	**1** Remaining Open	**231** Remaining Open
8.40 Avg Duration (Days)	**9.46** Avg Duration (Days)	**6.02** Avg Duration (Days)	**4.53** Avg Duration (Days)	**7.87** Avg Duration (Days)	**7.58** Avg Duration (Days)

Service Desk Trending

Requests
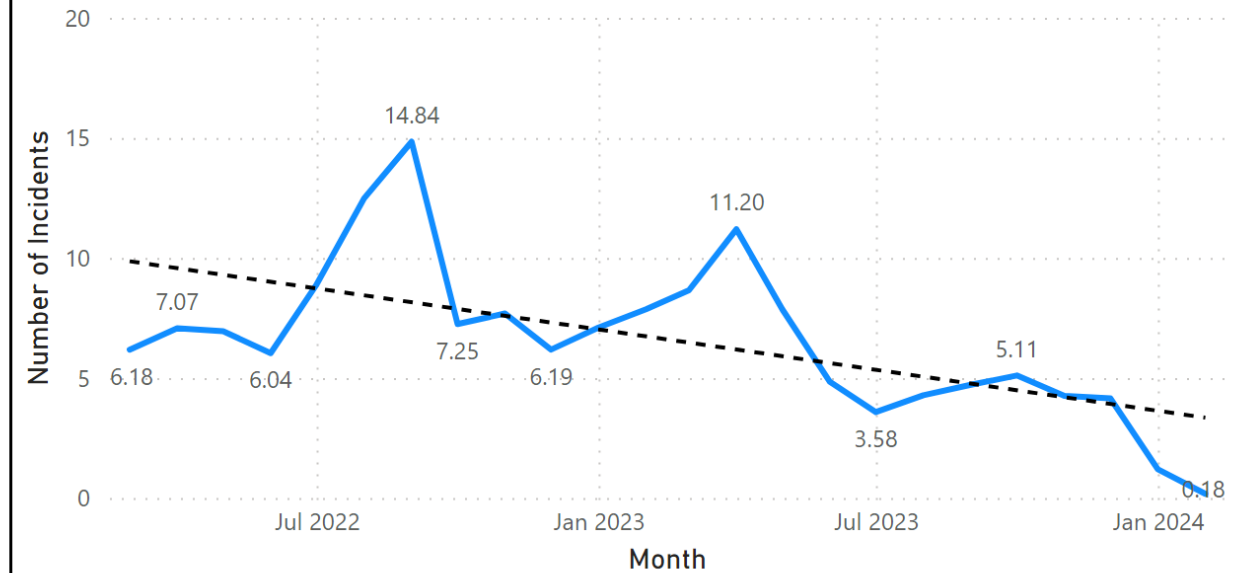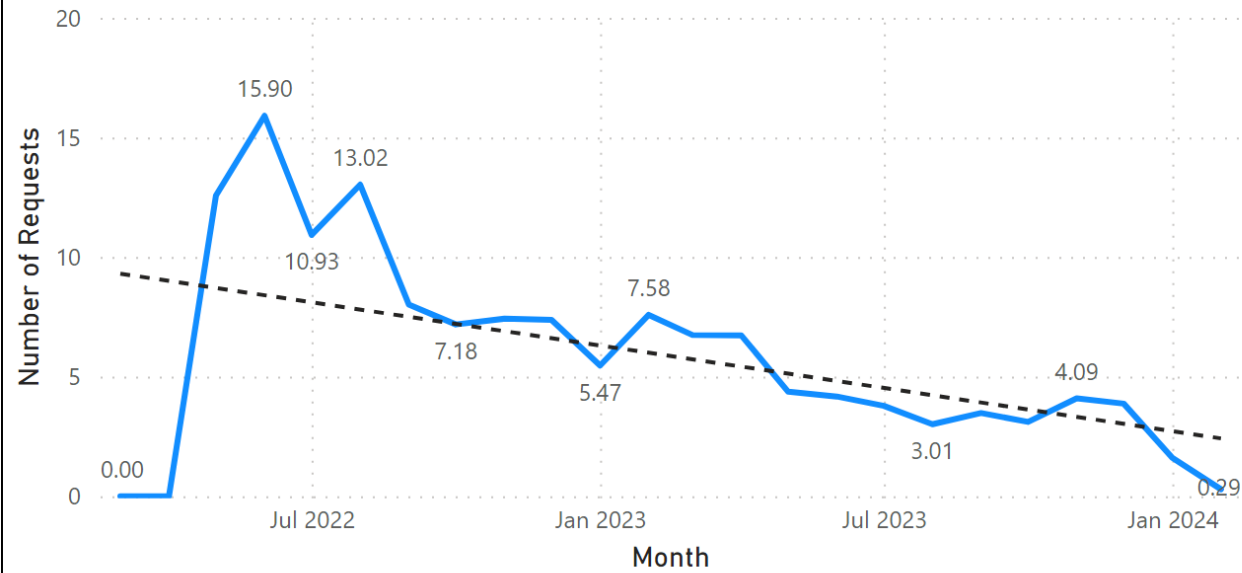
Average Duration (Days)

Requests Opened, Closed and Remaining Open

- ● Requests Opened ● Requests Closed ● Remaining Open

Incidents

Average Duration (Days)

Incidents Opened, Closed and Remaining Open

- ● Incidents Opened ● Incidents Closed ● Remaining Open
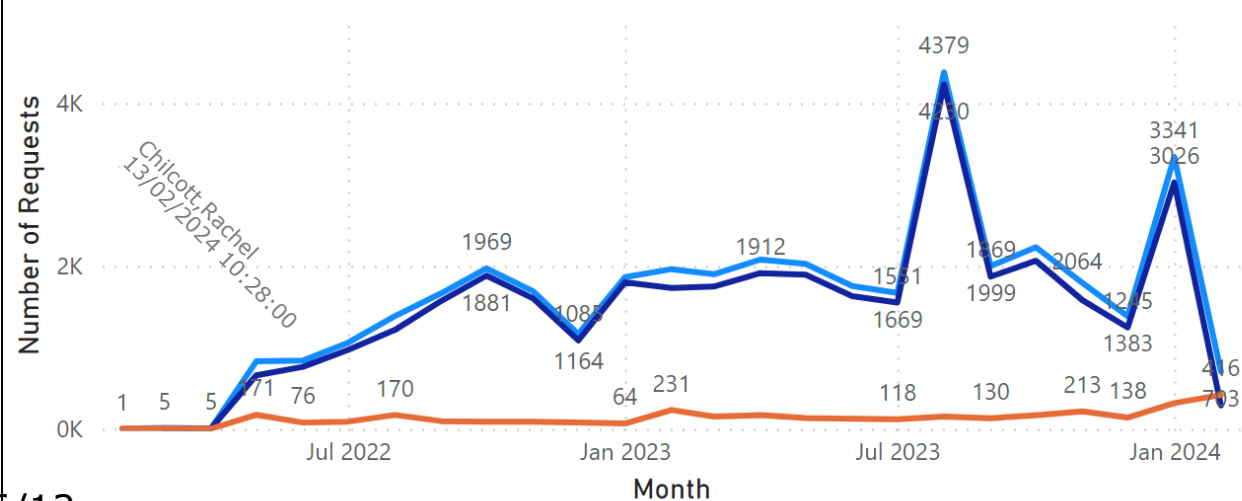
Created by Year

- ☐ 2023

Created by Month

- ☐ February 2022
- ☐ March 2022
- ☐ May 2022
- ☐ June 2022
- ☐ July 2022
- ☐ August 2022
- ☐ September 2022
- ☐ October 2022
- ☐ November 2022
- ☐ December 2022

OwnerTeam

- ☐ BI Analytics
- ☐ BI Applications and Warehouse
- ☐ Business Intelligence & Informatics
- ☐ Customer
- ☐ Digital Integration Development
- ☐ Digital Services Management (DSM)
- ☐ EUD
- ☐ IM&T Security
- ☐ Information Governance
- ☐ ISM Admin
- ☐ M365
- ■ Network
- ☐ O365/Azure
- ☐ Paris
- ☐ Paris Training
- ☐ Pharmacy
- ☐ PMS Development

264	214	16
Requests Opened	Closed Requests	Remaining Open

6.42	12	(Bla...
Duration (Days)	Older than 30 Days	Pending Approval

IT Procurement Requests

Status

Number by Service

Bar chart — Number of Requests by Service:
- Network: 243
- Desktop Service: 20
- PMS: 1

Automation Requests

Month

Date by Year

- ☐ 2023

Date By Month

- ☐ March 2022
- ☐ April 2022
- ☐ May 2022
- ☐ June 2022
- ☐ July 2022
- ☐ August 2022
- ☐ September 2022
- ☐ October 2022
- ☐ November 2022
- ☐ December 2022

OwnerTeam

- ☐ BI Applications and Warehouse
- ☐ EUD
- ☐ IM&T Security
- ☐ ISM Admin
- ☐ M365
- ☐ Network
- ☐ O365/Azure
- ☐ On-Call
- ☐ Paris

Site

- ☐ 34 Wordsworth Avenue
- ☐ At Home
- ☐ Barry Hospital
- ☐ Barry Leisure Centre
- ☐ Broad Street Clinic
- ☐ CRI
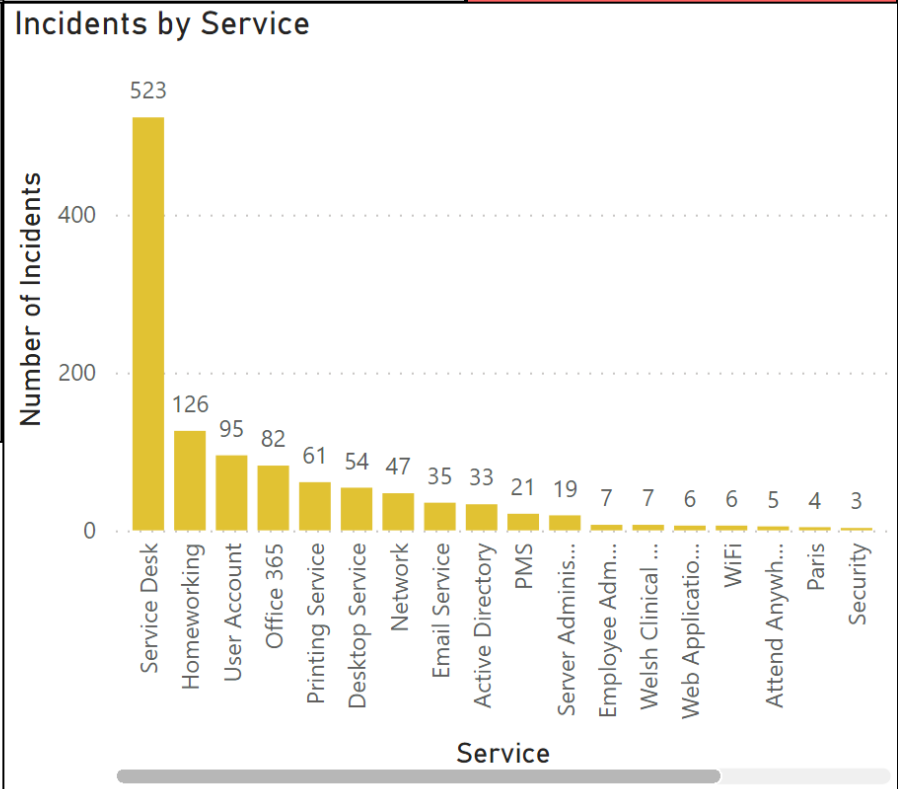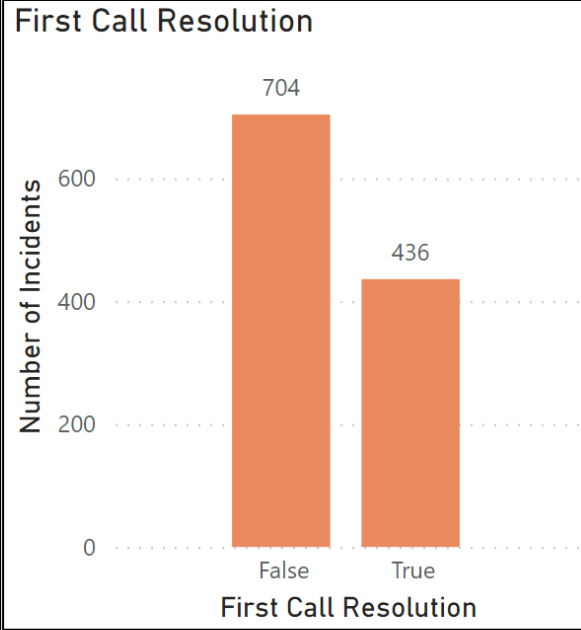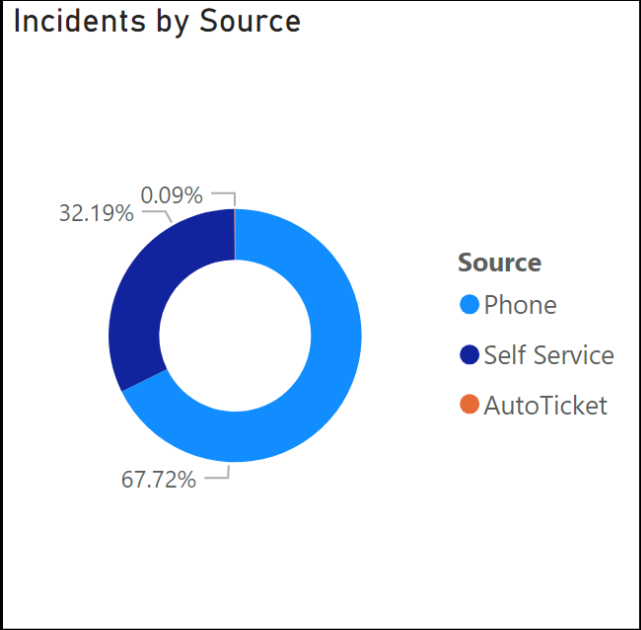- ☐ Dental Hospital

1140
Incidents Opened

1138
Incidents Closed

4.84
Avg Duration (Days)

2
Older then 30 Days

Incidents by Source

- 0.09%
- 32.19%
- 67.72%

Source
- Phone
- Self Service
- AutoTicket

First Call Resolution

First Call Resolution	Number of Incidents
False	704
True	436

Incidents by Service

Service	Number of Incidents
Service Desk	523
Homeworking	126
User Account	95
Office 365	82
Printing Service	61
Desktop Service	54
Network	47
Email Service	35
Active Directory	33
PMS	21
Server Adminis...	19
Employee Adm...	7
Welsh Clinical ...	7
Web Applicatio...	6
WiFi	6
Attend Anywh...	5
Paris	4
Security	3

Incidents by Category

Category	Number of Incidents
Software	248
Hardware	150
Connectivity	91
Service Desk	86
Reset Password	73
Vasco	68
RDS	48
Error Message	35
Administration	32
Outlook	25
Printer	20
Other	19
Meraki	17
Functionality	15
Printer Failure	13
Account Reset	12
How-To	12
O365 Apps Ge...	12
Mailbox Access	11
MFA	11
MSTeams	11
Printing	11
Account Lockout	10
Permissions	9
Installation	7
Performance	6
Print Queue	6

Trending

9/12

Number of Desktop/Laptop/Monitors

Type ●Desktop ●Display ●Laptop

Desktop: 9748
Display: 457
Laptop: 6106
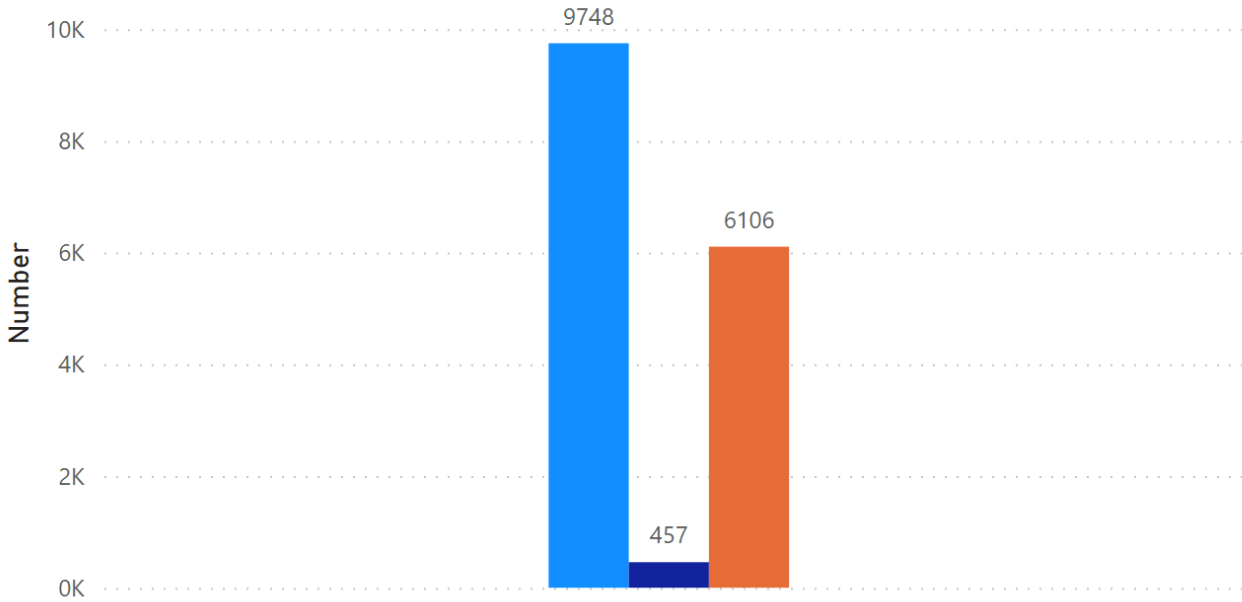
Status of Desktop/Laptop/Monitors

Type ●Desktop ●Display ●Laptop

Production: 6972, 1
Assigned: 2274, 3060
In Stock: 452, 459
Enrolled: 930
Awaiting Disposal: 27, 34
Disposed: 43, 1
Retired: 2, 14
In Repair: 2, 4
(Blank): 3, 2
Built: 4, 1
Deployment in Progr...: 3, 1, 3
Archived: 3, 1
Unenrolled: 2, 1
Destroyed: 1
On Loan: 2
Planned: 2, 1
Lost:
Under Maintenance: 1
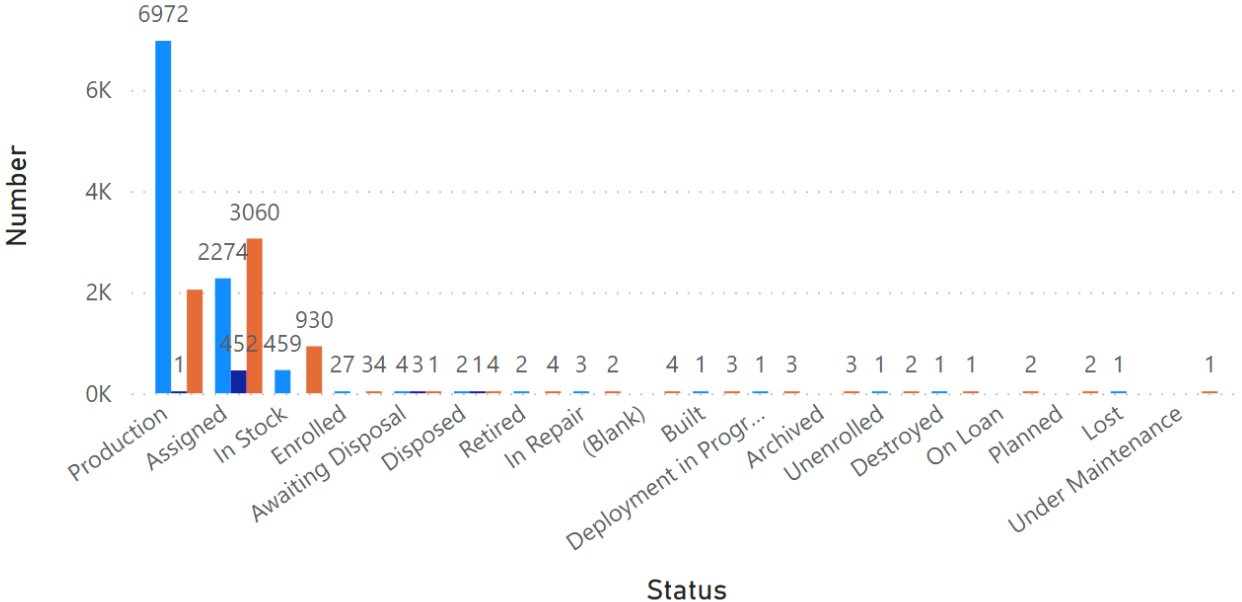
Number of Peripheral Devices

Type ●Tablet ●USB ●Virtual Desktop

Chilcott.Rachel
13/02/2024 10:28:00

Tablet: 28
USB: 2
Virtual Desktop: 2
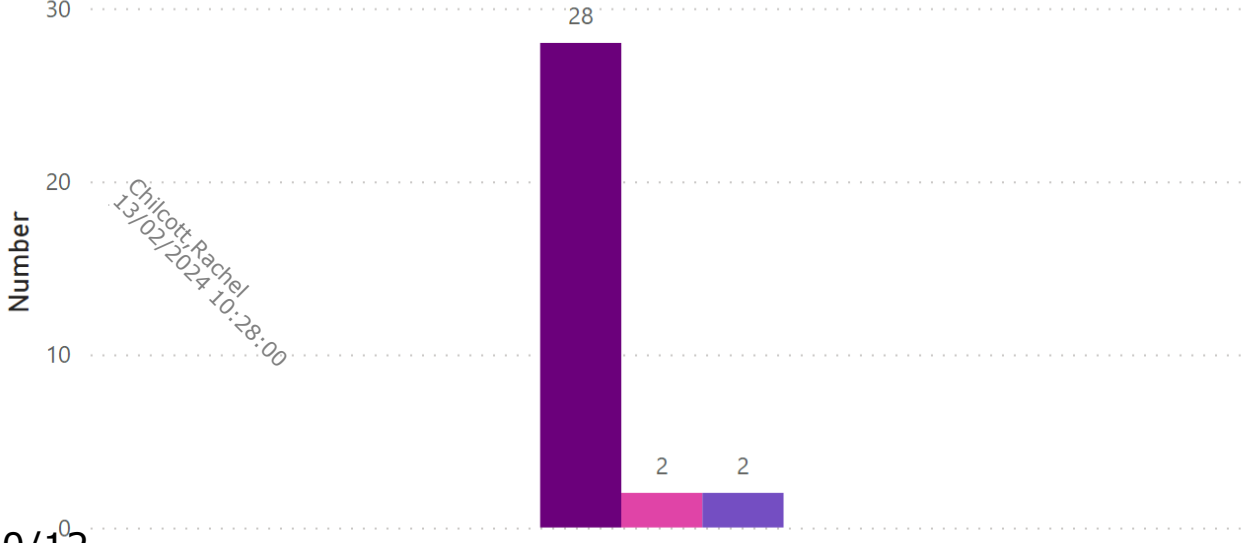
Status of Peripheral Devices

Type ●Tablet ●USB ●Virtual Desktop
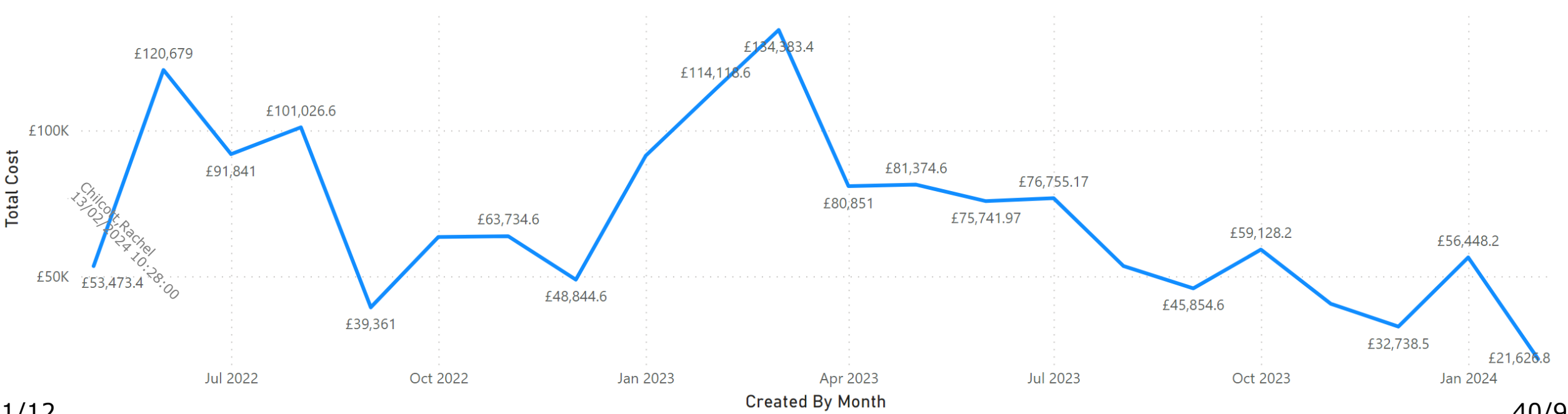

Assigned: 28, 2
Production: 2
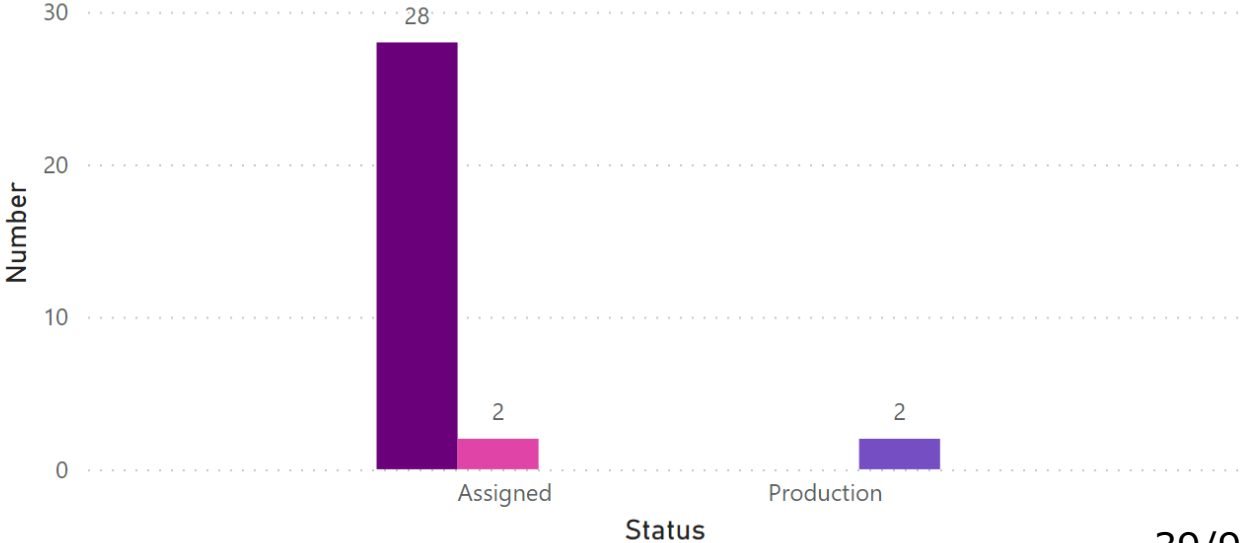
Cost by Equipment Type

EquipmentType
- ● Cabling
- ● Dell Latitude 3520
- ● Dell Latitude 3540
- ● Dell Latitude 5320
- ● Dell OptiPlex 3000/3090
- ● Dell OptiPlex 3000/3090 STANDARD PC
- ● Dell OptiPlex 3080/3090 Micro Form Factor
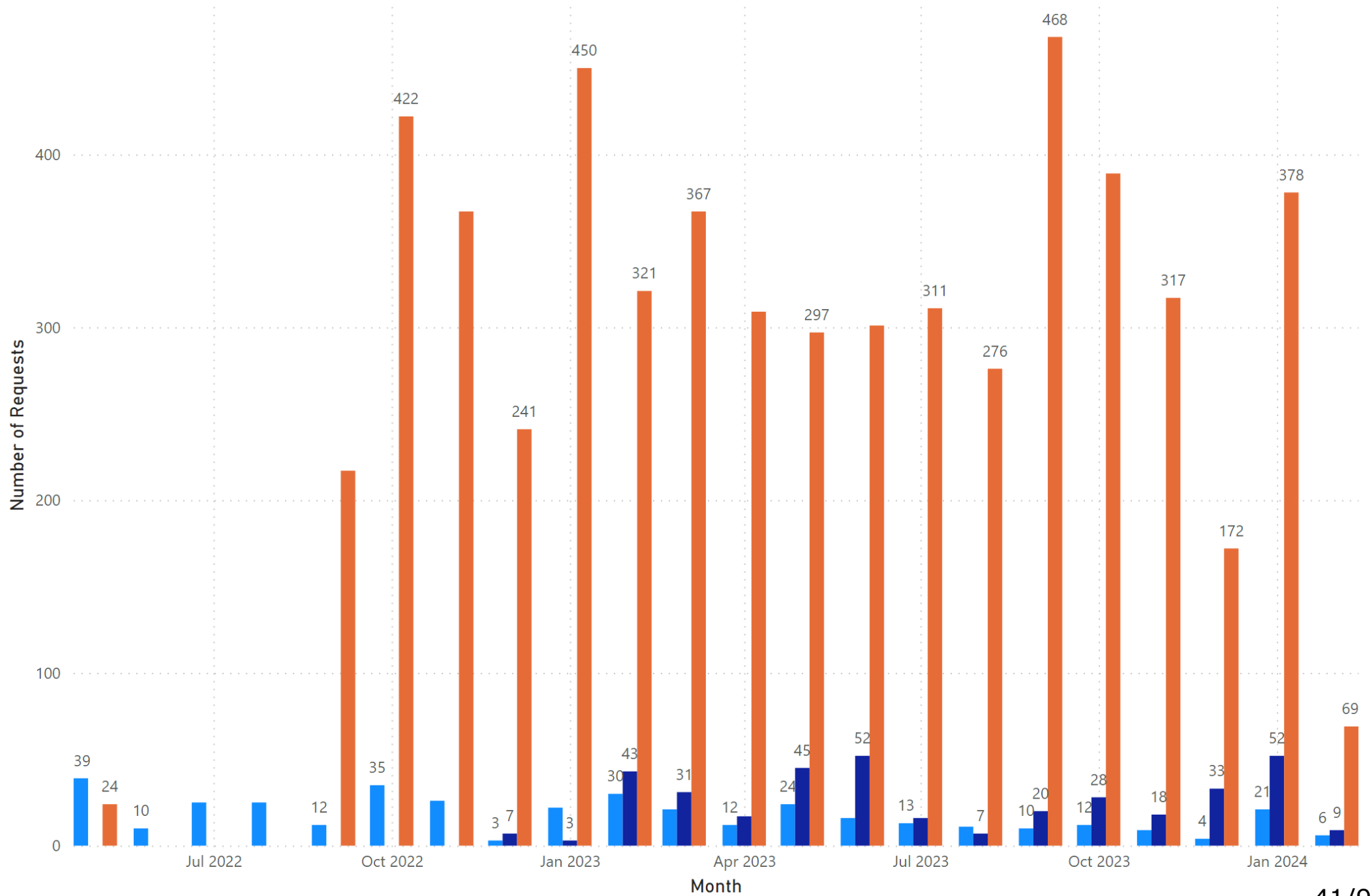- ● Desktop
- ● Docking Station
- ● Headset
- ● Laptop
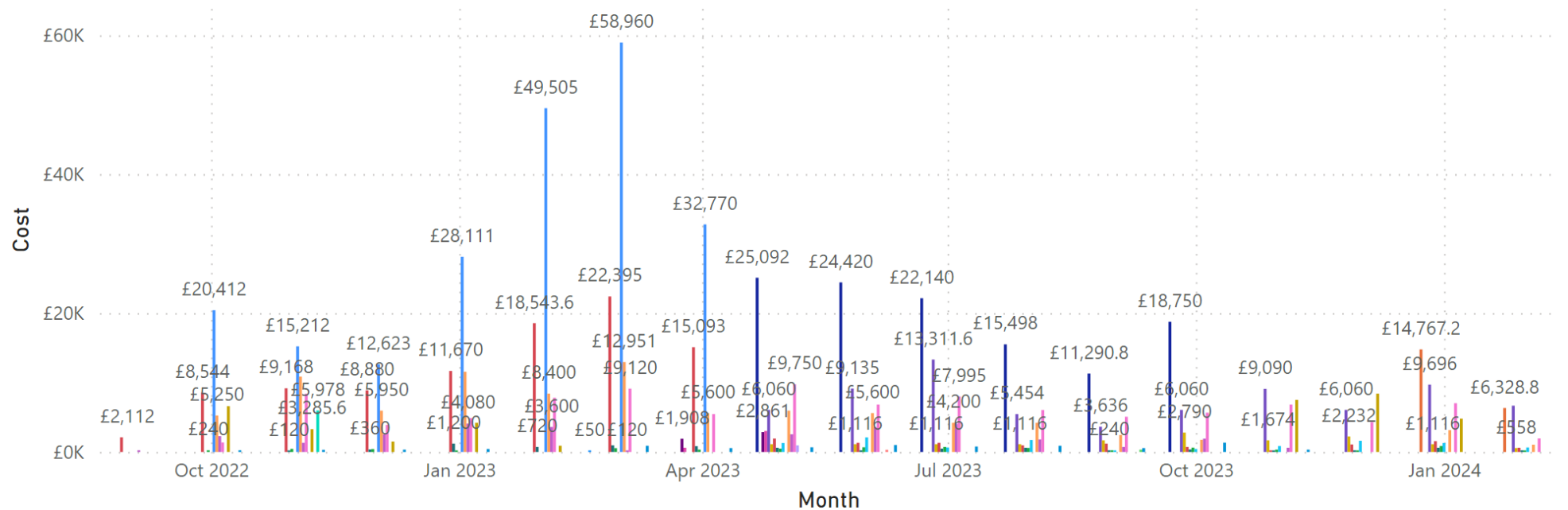
Total Cost by Month

Automation Requests

Automation Requests Summarised

- 🔵 Internet Access Request
- 🔵 New Mailbox Request
- 🟠 New NADEX Request

Report Title:	Framework Policies, Procedures & Controls			Agenda Item no.	2.5
Meeting:	Digital and Health Intelligence Committee	Public	x	Meeting Date:	20th February 2024
		Private			
Status (please tick one only):	Assurance		Approval	x	Information	
Lead Executive:	Director of Digital and Health Intelligence				
Report Author (Title):	Head of Information Governance and Cyber Security Information Governance Manager				

Main Report
Background and current situation:

As reported at the last DHIC meeting, a number of policies and procedures documents are out of date and need to be reviewed and updated.

As previously stated, the focus over the past twelve months has been to review and update those procedures and guidance documents that support our cyber security and IT security plans, as these have been deemed to be the highest priority.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

UHB 246 – Information Governance Policy will be presented to DHIC members on 20th February 2024, for their approval.

The following documents have been incorporated within this policy to create a single point of reference and guidance for IG Governance –

- UHB 207 Performance Management Framework
- UHB 002 Data Protection Act Policy
- UHB 350 Data Act Procedure

The full Document Schedule is attached as Appendix 1.

Recommendation:

The Board / Committee are requested to:

The Committee are requested to:

- Note progress

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1. Reduce health inequalities		6. Have a planned care system where demand and capacity are in balance	
2. Deliver outcomes that matter to people	X	7. Be a great place to work and learn	
3. All take responsibility for improving our health and wellbeing		8. Work better together with partners to deliver care and support across care	X

			sectors, making best use of our people and technology	
4. Offer services that deliver the population health our citizens are entitled to expect	X	9. Reduce harm, waste and variation sustainably making best use of the resources available to us		X
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives		X

Five Ways of Working (Sustainable Development Principles) considered
Please tick as relevant

Prevention	x	Long term		Integration		Collaboration	x	Involvement	x

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: Yes

Adherence to appropriate policies will further reduce risks

Safety: Yes

Patient safety supported by good governance arrangements

Financial: No

Workforce: Yes

All staff need to be aware of their role in using and accessing personal/patient identifiable data

Legal: Yes

Policies set out compliance against IT security and information governance requirements

Reputational: Yes

Compliance with GDPR and Information Governance requirements

Socio Economic: Yes/No

Equality and Health: Yes/No

Decarbonisation: Yes/No

Approval/Scrutiny Route:

Committee/Group/Exec	Date:

Controlled Documents Schedule

UHB Ref Number	Title of Document	Type of Document	Last review date	New review date	Current Status	Comments
UHB 006	Data Protection Guidance For Researchers'	Guidelines	07-Dec-2015	07-Dec-2018	Review to be scheduled	
UHB 007	Remote Access Software	Protocol	29-Sep-2010	11-Jan-2012	Review to be scheduled	
UHB 048	Internet and E-mail Monitoring, administration and Reporting Protocol	Protocol	26-Apr-2011	01-Apr-2014	Review to be scheduled	
UHB 263	Transportation of Personal Identifiable Information	Procedure	42061	43157	To be noted by DHIC on 15th August 2023	Reviewed and noted at DHIC on 15.08.23
UHB 286	Information Governance Corporate Training Policy	Policy	42206	43302	To be reviewed and approved at February 2024 DHIC	
UHB 287	Information Risk Managment Procedure	Procedure	18-Sep-2015	18-Sep-2018	Review to be scheduled	
UHB 288	Data Quality Management Procedure	Procedure	15-Sep-2015	15-Sep-2018	Review to be scheduled	
UHB 289	Information Asset Procedure	Procedure	22-Jun-2015	22-Jun-2018	Review to be scheduled	
UHB 290	Personal Information use and Disclosure of and the Duty to Share Guidance	Guidelines	22-Jun-2015	22-Jun-2018	Review to be scheduled	
UHB 298	Data Quality Policy	Policy	15-Sep-2015	15-Sep-2018	Review to be scheduled	
UHB 301	Information Goverance Operational Management Responsibilities Procedure	Procedure	19-Jan-2016	19-Jan-2019	Review to be scheduled	
UHB 326	Records Management Procedure	Procedure	42955	44051	To be reviewed by DHIC on 15th August 2023	Complete - Records Management Policy and supporting procedures were approved at DHIC on 15.08.23
UHB 142	Records Management Policy	Policy	44226	44591	To be reviewed by DHIC on 15th August 2023	Reviewed and noted at DHIC on 15.08.23
UHB 356	Contractual Clauses and Arrangements Procedure	Procedure	22-Jun-2015	22-Jun-2018	Review to be scheduled	
UHB 357	Clauses within Employment Contracts Procedure	Procedure	22-Jun-2015	22-Jun-2018	Review to be scheduled	
UHB 421	Remote Working Procedure	Procedure	18-May-2021	tbc	Review to be scheduled	
UHB 422	Malicious Software Guidance	Guidelines	18-May-2021	tbc	Review to be scheduled	
UHB 424	IT Business Continuity Guidance	Guidelines	42955	44051	Reviewed/Completed	Previously noted by DHIC - see key
UHB 427	IT Security Equipment Procurement Guidance	Guidelines	42633	43728	Reviewed/Completed	Previously noted by DHIC - see key
UHB 428	IT Security Incidents (Breach) Guidance	Guidelines	20-Sep-2016	20-Sep-2019	Review to be scheduled	
UHB 429	IT Security Software Licensing Procedure	Procedure	42633	43728	Reviewed/Completed	Previously noted by DHIC - see key
UHB 246 -	Information Governance Policy - UHB 207 Performance Management Framework - UHB 002 Data Protection Act Policy - UHB 350 Data Act Procedure	Policy	43784	44596	To be reviewed by SHIC on 20th February 2024	Previously advised that UHB 207, UHB 002 and UHB 350 will be incoporated into UHB 246.
UHB 420	IT Security Disposal of Equipment Guidance	Guidelines		44051	Reviewed/Completed	Previously noted by DHIC - see key
UHB 423	Bring your own Devices Local Procedure	Procedure		44051	Reviewed/Completed	Previously noted by DHIC - see key
UHB 430	IT Security Assets Guidance	Guidelines		44051	Reviewed/Completed	Previously noted by DHIC - see key
UHB 431	IT Security Code of Connection Guidance	Guidelines		44051	Reviewed/Completed	Previously noted by DHIC - see key

Key
For Information - For Board to note for information purposes only
Review Period (Min 28 Days 1st Consultation + 10 Days Review 1 + 5 Days Review 2 *to include EHIA (EQIA) review)
Final Draft Approved via relevant Steering Group.
Provided to DHIC for noting, adopted by CAV and do not require further approval

Report Title:	Information Governance Policy			Agenda Item no.		3.1	
Meeting:	Digital & Health Intelligence Committee	Public	X	Meeting Date:		20th February 2024	
		Private					
Status *(please tick one only):*	Assurance	X	Approval		Information		
Lead Executive:	Director of Digital & Health Intelligence						
Report Author (Title):	Head of Information Governance and Cyber Security						
Main Report Background and current situation:							

Cardiff and Vale UHB considers information to be a vital asset, and a key enabler, on which the UHB is dependent as we move forward in delivering our Shaping Our Future Wellbeing strategy and becoming a data driven organisation.

It is therefore of paramount importance to ensure that information is efficiently managed and kept securely, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

The Information Governance Policy is the cornerstone of this framework. The policy was implemented 2 years ago and therefore it is due for a review.

ASSESSMENT

The Information Governance Policy has been updated in line with the review process. A summary of the proposed changes are below:

- The inclusion of additional UK GDPR definitions. (Page 12)

- Guidance on the use of online forms used to collect personal data. (Page 15)

- A new statement explaining that unlawful access to personal data can result in disciplinary action and criminal prosecution. (Page 20)

- Guidance on what staff should do it they are required to access medical records relating to colleagues, friends or relatives. (Page 20)

- A new clause on the Network & Information Systems Regulations and Welsh Health Circular guidance. (Page 26)

- An explicit requirement to use NHS email to conduct UHB business. (Page 28)

- Clarification on the use of NHS email to receive discounts. (Page 29)

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

- The Information Governance Policy has been reviewed and a number of proposed changes made.

Recommendation:

The Board / Committee are requested to:

- RECEIVE and APPROVE the recommended changes to the Information Governance Policy.

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1. Reduce health inequalities	X	6. Have a planned care system where demand and capacity are in balance	
2. Deliver outcomes that matter to people	X	7. Be a great place to work and learn	x
3. All take responsibility for improving our health and wellbeing	X	8. Work better together with partners to deliver care and support across care sectors, making best use of our people and technology	x
4. Offer services that deliver the population health our citizens are entitled to expect	x	9. Reduce harm, waste and variation sustainably making best use of the resources available to us	x
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives	

Five Ways of Working (Sustainable Development Principles) considered
Please tick as relevant

Prevention	x	Long term		Integration	x	Collaboration	x	Involvement	x

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: Yes
Compliance with legal and mandatory requirements
Safety: Yes
Supports patient and staff safety
Financial: Yes
Non-compliance
Workforce: Yes
Applies to entire workforce
Legal: Yes compliance
Reputational: Yes
Confidence in managing assets/supporting services
Socio Economic: Yes/No

Equality and Health: Yes/No	
Decarbonisation: Yes/No	
Approval/Scrutiny Route:	
Committee/Group/Exec	Date:

Cardiff and Vale UHB
Information Governance Policy

Author: Information Governance Department
Approved by: Information Governance Executive Team
Approved by: Digital Health Intelligence Committee
Version: 0.8
Date: 01/09/2021
Review date: 2 years following ratification

Chilcott Rachel
13/02/2024 10:28:00

Contents

Chilcott-Rachel
13/02/2024 10:28:00

1.   Introduction

Cardiff and Vale UHB considers information to be a vital asset, and a key enabler, on which the UHB is dependent as we move forward in delivering our Shaping Our Future Wellbeing strategy and becoming a data driven organisation.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2.   Purpose

It is the policy of the UHB to ensure that:
- We protect the legal rights of individuals, patients and staff in respect of confidentiality and privacy.
- We safeguard our information and systems.
- We make appropriate use of ICT services, such as email and the internet.
- Our staff have access to the relevant and appropriate information they require at the point that it is required.
- The value of the information that the UHB manages is increasingly realised
- All services transition towards the appropriate adoption of the UHB's technical and data standards and achieve these by 2023.
- Opportunities to achieve improvements in clinical and cost-effective care provided by digital technologies are realised.
- We improve the ability of our population, patients, and staff to make timely, evidence-based decisions.
- Our staff are valued, trusted and enabled.
- Our staff are supported to better manage and balance work and out-of-work commitments.
- We comply and act in the intended spirit of the Welsh Government's policy and notably the 'Once for Wales' design principles.

3.   Scope

This policy applies to the workforce of Cardiff and Vale UHB including staff, students, trainees, secondees, volunteers, contracted third parties and any other persons undertaking duties on behalf of the UHB, across all areas of our business, including: the provision, planning and commissioning of direct care, teaching and training; and scientific work including research.

It applies to all forms of information controlled and processed by Cardiff and Vale UHB including video, digital and paper; and covers all business functions and the information, information systems, networks, physical environment and relevant people who support those business functions.

The policy covers the following areas:
- Roles and Responsibilities
- Use and protection of Data
- Data and technical standards

- [Privacy notices](#)
- [Information security](#)
- [Internet Use](#)
- [Email Use](#)

4.   Roles and responsibilities

This policy is intended to be enabling and expects that the professionalism of all staff to familiarise themselves with the policy content and ensure the policy requirements are implemented and followed at all times. In adopting a high trust approach, it is an absolute requirement that all staff members undertake the appropriate level of information governance training at least every two years. It is also essential that breaches of this policy and related legislation are reported by the individual via Datix or agreed local reporting mechanisms and to the Data Protection Officer at the earliest opportunity.

UHB.DPO@Wales.NHS.UK

The UHB's accountability and governance structure for Information Governance requires specific roles to be fulfilled. These are set out below:

The Chief Executive is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. The Chief Executive is responsible for ensuring that there is a designated individual within the UHB who assumes the responsibilities of three statutory positions.

The Data Protection Officer is responsible for to ensuring that the UHB processes the personal data of its staff, patients and population in compliance with the data protection legislation.

The Senior Information Risk Officer (SIRO) is responsible for ensuring that information security and information governance risks are managed. Specific responsibilities include:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners.
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.
- Owning the organisation's information incident management framework.

The Caldicott Guardian is responsible for safeguarding the processing of patient information.

The Head of each Clinical Directorate, Clinical Board & Corporate Department is responsible for appointing Information Asset Owners and Administrators to act as accountable officers and named points of contact for IG matters.

Information Asset Owners are responsible for the implementation of this policy in respect of the data held acquired, stored within their assets and transferred from their assets (e.g. IT systems, databases, video

stores, clinical record libraries). Specifically, Information Asset Owners should have undertaken a self assessment of their directorate's compliance with data protection regulation, using the ICO's tools (link: https://ico.org.uk/for-organisations/data-protection-self-assessment/) once every 24 months and have logged completion with the IG department. Information Asset Administrators will support the Information Asset Owners in fulfilling these obligations.

Managers are responsible for the implementation of this policy within their department/directorate. In addition, they must ensure that their users and staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training.

5. Data Protection and Compliance

Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.

While the emphasis on this policy is on the protection of personal data, the UHB owns and processes business and other sensitive data. The security of 'sensitive' data is also governed by this policy.

5.1.1   Definition of Personal Data

For the purpose of this policy, the use of the term "personal data" encompasses any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal data that has been pseudonymised – e.g. key-coded – will fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

5.1.2   Special Categories of Personal Data

Special categories of personal data are defined by data protection legislation as including any data concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric data where processed to uniquely identify an individual.

5.1.3   Data controller and data processor

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

5.1.4 Anonymisation and pseudonymisation

Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

5.2 Using data

5.2.1 Fair and Lawful Processing

The UHB will process personal, special category and sensitive data fairly and lawfully, in line with data protection legislation and in accordance with the UHB's patient and staff privacy notices. Processing broadly means collecting, using, disclosing, sharing, retaining or disposing of personal data or information.

In order for the processing of data to be fair, the SIRO, on behalf of the UHB will maintain and publish in a highly open, transparent and accessible way, privacy notices for patients and staff which clearly set out the information held by the UHB and how it is used are available below.

Patient Privacy Notice

Employee Privacy Notice

All sizeable patient facing areas should provide patients with clear information signposting them to the web page at which the UHB's privacy notice for patients can be viewed. It is the responsibility of the manager of the clinical area to have this in place.

Where an activity can be carried out without the need for personal or sensitive data to be disclosed, anonymised data should be used. Where personal data is required, then the minimum amount of identifiable information required should be used and, wherever appropriate, the data should be pseudonymised.

Personal or sensitive information should not be processed where the UHB does not have a lawful basis for processing such information under the data protection legislation which is not reliant on the consent of individuals (e.g. necessary for the health or social care purposes). Exceptions to this must be agreed with the SIRO and Caldicott Guardian.

Where there are any queries, staff must consult the Information Governance Office before processing or sharing personal or sensitive data.

5.2.2 Information Asset Management

5.2.1.1 Information Asset Registers

To protect individual's rights laid out in the Data Protection Act 2018 and the UK GDPR (2018), it is important that the UHB has knowledge of, and can swiftly access, all of the personal and sensitive data that it holds, regardless of the medium in which it is held. To achieve this, each Clinical Directorate, Clinical Board and Corporate Department must identify and record the lawful basis for the information it processes in an information asset register. It is the responsibility of the Information Asset Owners to ensure that the information asset registers are accurate and up to date and the responsibility of individual members of staff to store data they hold in a way it can be accessed swiftly.

As a minimum, information asset registers should document all "departmental" shared drives managed by an individual within the Directorate, all servers owned by the directorate and all systems used and contracted for by the Directorate (including messaging systems), incorporating:
- the type of information held
- where it came from,
- who it is shared with
- how this information is used
- the legal basis for holding this data – If in doubt consult the UHB's web page or ask the IG department
- When it should be destroyed (if not in the medical record or essential for business use – e.g. a contract, then the longest retention period including email should be 6 months unless specifically referenced in the UHB's retention schedule, available via Information Governance webpage.
- Who this data is shared with – e.g. Royal Colleges, WG, other NHS organisations, Local Authorities
- Where data is shared, the legal basis for sharing the data (as above, public duty should be used where the basis is patient care)
- Confirmation that no data is stored or transferred outside the European Economic Area, including for Artificial Intelligence processing within the cloud.

5.2.1.2 Registering Security, Hosting and Back up arrangements

To ensure that the UHB maintains service resilience in line with the EU directive on the security of Networks and Information Systems, all existing and new systems provided or used by the UHB should have a Security, Hosting and Back Up agreement with the UHB's informatics department, with the required details included on the information asset register. It is the responsibility of the Information Asset Owners to ensure that these details are accurate and up to date.

5.2.1.3 Managing paper care records

Members of staff who have received and are using the paper care record are responsible for ensuring that the location of the record is known and tracked on the appropriate electronic system.

The paper care record must not be split. Where only a single volume of a file containing several volumes is required, this may be moved for a very minimal time (never longer than the current working shift) and

holders of both segments of the record must be aware. This must be reflected via the tracking mechanism on the appropriate electronic system.

5.2.1.4 Storing and moving data

Section 6.1 refers to expected standards and requirements for the control and storage of data.

5.2.3   Individual's Rights & Consent

Individuals have certain rights with regard to the processing of their personal data. Information Asset Owners must ensure that appropriate arrangements are in place to manage these rights.

In particular, where the directorate is reliant on "Consent" as the legal basis for holding patient identifiable data, you must ensure that the way you have attained the consent follows the ICO's guidance:

- A request to gain consent to use information about the patient should be made prominent and be clearly separated from other requests for consent – such as those in regards to treatment.
- Consent has required a positive opt-in such as un-ticked opt-in boxes or similar active opt-in methods.
- Consent should be specific and granular. You should allow individuals to consent separately to different purposes and types of processing wherever appropriate.
- Be clear that this consent is for NHS Wales & Cardiff and Vale UHB and name any specific third party organisations that will rely on this consent.

5.2.4   Accuracy of Personal Data

Arrangements must be in place to ensure that any personal data held by the UHB is accurate and up to date, or contains a time stamp.

5.2.5   Establishing new data processing activities

New data processing activities include, but are not limited to: the introduction of new data capture systems, the collection of additional data items, the undertaking of Artificial Intelligence which does not involve the intervention of a human and extending the sharing of data.

5.2.5.1   Data Protection Impact Assessment (DPIA)

All new projects or major new flows of information must consider information governance practices from the outset to ensure that personal data is protected at all times. Any processing that is likely to result in a high risk must be assessed by a DPIA, especially any transfer outside of the European Economic Area. This also provides assurance that the UHB is working to the necessary standards and are complying with data protection legislation. In order to identify information risks, a DPIA must be completed. If there is any doubt as to what and whether a DPIA is required, the information governance department should be requested to assist.

The results of the DPIA must both be filed and discussed with the Information Governance Department (who may consult the ICO) and signed off by the UHB's Data Protection Officer and Senior Information Risk Owner. Any controls identified as being required must be acted upon and put in place.

5.2.5.2   Third Parties and Contractual Arrangements

Where the organisation uses any third party who processes personal data on its behalf, any processing must be subject to a legally binding written contract which meets the requirements of data protection legislation.

UHB documents & specifications (such as the UHB's Data Processing Contract, Security Arrangements, Contracts, Procurement technical specification, codes of conduct, access and auditing specifications) must be used in formalising the arrangements for the processing and sharing of the personal data the UHB controls or will be controllers of (that which it processes for its own purposes). This is to ensure that personal data is processed in a consistent manner and the roles of responsibilities of the parties are clearly understood.

No part of a UHB agreement can be varied without the prior written approval of the relevant Director, particularly the minimum indemnity limit of £5 million per annum.

5.2.5.3   Documents and forms used to collect personal data

All forms (both computerised and manual) used to obtain personal data must comply with the requirements of DPA. Personal information must be adequate, relevant and not excessive, and specifically no unnecessary information to be included.

Forms will be reviewed by the author and/or responsible manager and then sent to the Information Governance Department for sign off and will be periodically audited to ensure that the personal data being processes complies with the DPA.

The IG Department will be responsible for providing advice and guidance regarding compliance with 'Adequate Data'. Legal advice will be sought for any unclear or contentious issues.

5.2.6   Incident Management and Breach Reporting

Staff must be aware of their department's arrangements that are in place to identify, report (via Datix), manage and resolve any data breaches within specified legal timescales (presently 72 hours). Lessons learnt will be shared to continually improve procedures and services, and consideration given to updating risk registers accordingly. Incidents must be reported immediately following local reporting arrangements.

5.2.7   Information Governance Compliance

All information asset owners and departments must have monitoring arrangements in place to ensure that personal and sensitive data is being used appropriately and lawfully.

5.3   Records Management

Cardiff and Vale University Health Board (the UHB) understands the definition of records to be:

"Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business". *Reference BS ISO 15489.1*

"An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees including consultants, agency or casual staff." *Reference. Department of Health Records Management: NHS Code of Practice Part 1*

All records held by the UHB fall within the scope of this policy as these are either personal (relating to patients, public and employees) or corporate (for example financial records, letters, reports) and regardless of whether they are held in electronic, virtual or physical format. It applies to all areas and services within the remit of the UHB.

The UHB is committed to the handling and processing of all health records in accordance with the legal requirements, codes of practice and guidance issued by relevant authorities including, but not restricted to, the Welsh Government and the Information Commissioner's Office.

To achieve this, the UHB and its employees will follow the [Records Management Code of Practice for Health and Social Care 2022](#)

All staff should understand and be aware of the importance attached to the way in which records are managed and the relationship of records management to assist in achieving the overall business strategy of the organisation.

Records will be managed in accordance with the UHB's [Records Management Retention and Destruction Protocol and Schedule](#).

5.4 Access to Information

The UHB is in some circumstances required by law to disclose information. Examples include information requested under:

- Freedom of Information Act 2000
- Environmental Information Regulation 2004
- General Data Protection Regulation

For further detail, please see the below links or contact the Information Governance department.

[Freedom of Information Act 2000 and Environmental Information Regulations 2004 Procedure](#)

[Dealing with Subject Access Requests under Data Protection Legislation Procedure](#)

All staff have a responsibility to provide information for where requested to do so by the Information Governance team.

Processes must be in place for disclosure under these circumstances. Where required, advice should be sought from the UHB's information governance department.

5.5 Confidentiality

5.5.1 Confidentiality: Code of Practice for Health and Social Care in Wales

The UHB has adopted the Confidentiality: Code of Practice for Health and Social Care in Wales. All staff have an obligation of confidentiality regardless of their role and are required to respect the personal data and privacy of others.

Staff must not access information about any individuals who they are not providing care, treatment or administration services to in a professional capacity. Rights to access information are provided for staff to undertake their professional role and are for work related purposes only. It is only acceptable for staff to access their own record where self-service access has been granted.

Appropriate information will be shared securely with other NHS and partner organisations in the interests of patient, donor care and service management. (See section 5.6 on Information Sharing for further details).

It may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the individual concerned.

5.6 Sharing Personal Data

5.6.1 Wales Accord for the Sharing of Personal Information (WASPI)

The WASPI Framework provides good practice to assist organisations to share personal data effectively and lawfully. WASPI is utilised by organisations directly concerned with the health, education, safety, crime prevention and social wellbeing of people in Wales. << http://www.waspi.org/nhs >>

The UHB will use the WASPI Framework for any situation that requires the regular sharing of information outside of NHS Wales wherever appropriate. Advice must be sought from the information governance department in such circumstances.

5.6.2 One-off Disclosures of Personal Data

Formal Information Sharing Protocols (ISPs) or other agreements must be used when sharing information between external organisations, partner organisations, and external providers acting in the capacity of a data controller. ISPs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information. Advice must be sought from the information governance department in such circumstances.

Personal data may need to be shared externally on a one-off basis, where an ISP or equivalent sharing document does not exist. Advice must be sought from the information governance department in such circumstances.

5.7 Welsh Control Standard for Electronic Health and Care Records

5.7.1 The Control Standard

The Wales Control Standard for Electronic Health and Care Records describes the principles and common standards that apply to shared electronic health and care records in Wales, and provides the mechanism through which organisations commit to them. NHS Wales organisations have committed to abide by the Control Standard. The Control Standard will be underpinned by local level policies and procedures to ensure electronic records are accessed and used appropriately.

5.8 Data Quality

Key components of data quality include; accuracy, completeness, validity, timeliness, free from duplication or fragmentation, defined and consistent. Data from all areas should be recorded and processed at all levels in the Health Board using relevant skills and knowledge.
The Health Board has set 8 key objectives in order to achieve the policy aims. They are:

1. Data is accurate and up to date:
   - Correct and accurately reflects what actually happened
   - Precise and includes all data processed in the organisation

2. Data is complete: Data should be captured in full and where applicable a valid and traced NHS number must be included to support operational use.

3. Data is valid
   - Data should be held in a format which conforms to recognised national standards
   - Must be mapped by codes to national values where these are in existence
   - Held in computer systems that are programmed to only accept valid entries wherever possible

4. Data is timely
   - Data should be collected at the earliest opportunity, preferably at the time and place of the activity taking place
   - Data is available when required for its intended use

5. Data is free from duplication and fragmentation: Patients must not have duplicated or confused patient records e.g. should not have two or more separate records held on Patient Management Systems.

6. Data is defined and consistent: The data being collected should be understood by the staff collecting and interpreting it.

7. Coverage: Data from all areas of activity - clinical or corporate should be recorded in the appropriate place and format.

8. Data quality management: At every level across the Health Board those managing data quality must have the appropriate skills and knowledge.

5.9   Data and Technical Standards

The UHB will adopt and comply with the standards set out in Welsh Health Circulars, Data Set Change Notices and the Welsh Data Dictionary.

The UHB will adopt the WTSB technical standards as they are produced for all new systems and upgrades, and information asset owners should be establishing development programmes for systems to be fully compliant by 2023.

Asset owners will ensure that the data and images are made available to the UHB's clinical data repository, via a method agreed with the corporate informatics department.

6.   Information Security

6.1   Purpose of Security Procedures

The purpose of an IT Security protocol is to preserve:

- Confidentiality   access is confined to those with authority to view the data.
- Integrity   all systems are working in the way they were intended to work.
- Availability   information is delivered to the right person, when it is needed.

6.2   User Access Controls

Access to information will be controlled on the basis of business requirements.

System Managers will ensure that appropriate security controls and data validation processes, including audit trails, will be designed into application systems that store any information, especially personal data. The system manager for any given system will be the corresponding Information Asset Owner.

The workforce has a responsibility to access only the information which they need to know in order to carry out their duties. Examples of inappropriate access include but are not restricted to:

- Accessing your own health record;
- Accessing any record of colleagues, family, friends, neighbours etc., even if you have their consent, except where this forms part of your legitimate duties;
- Accessing the record of any individual without a legitimate business requirement.

User access will be regularly monitored using NIIAS for all national systems. Inappropriate access can result in disciplinary action in line with the Health Board's policy and procedures. In some cases, inappropriate access can even result in criminal prosecution by the Information Commissioner or by the Director of Public Prosecutions.

Employees who are asked to access information relating to colleagues, friends or relatives need to declare their relationship to their line manager, who will decide if the task could be carried out by another staff member.

6.2.1 Physical Access Controls

Maintaining confidentiality in clinical areas can be challenging and the need to preserve confidentiality must be carefully balanced with the appropriate care, treatment and safety of the patient.

Individuals, departments and Information Asset Owners are responsible for determining the relevant security measures required based on local risk assessment.

All reasonable steps should be taken to ensure high standards of security in areas where data is kept. As a minimum, offices, vehicles and computers should be locked when the user is absent. Access cards, PIN codes, key codes, etc. must be kept secure and regularly changed as required.

All central file servers and central network equipment will be located in secure areas with access restricted to designated staff as required by their job function.

6.2.2 Passwords

The workforce are responsible for the security of their own passwords which must be developed in line with NHS guidance ensuring they are regularly changed. Passwords must not be disclosed to anyone. Recognising that, at the current time, the UHB still has a limited number of generic accounts, users will be held fully responsible and accountable for any infringement and breaches of data protection legislation where they have shared their log in details.

In the absence of evidence to the contrary, any inappropriate access to a system will be deemed as the action of the user. If a user believes that any of their passwords have been compromised, they must change them immediately.

Staff must not logon to any computer system using another member of staff's log in details and password.

6.2.3 Remote Working

NHS Wales recognises that there is a need for a flexible approach to where, when and how our workforce undertake their duties or roles. Handling confidential information outside of your normal working environment brings risks that must be managed.

Examples of remote working include, but are not restricted to:

- Working from home
- Working whilst travelling on public/shared transport
- Working from public venues (e.g. coffee shops, hotels etc.)
- Working at other organisations (e.g. NHS, local authority or academic establishments etc.)
- Working abroad

As a control measure to mitigate risks involved in remote working, no member of the workforce will work remotely unless they have been authorised to do so. Remote working must not be authorised for anyone who is not up to date with mandatory training in information governance.

6.2.4 Staff Leavers and Movers

Managers will be responsible for ensuring that local leaving procedures are followed when any member of the workforce leaves or changes roles to ensure that user accounts are revoked / amended as required and any equipment and/or files are returned. Confidential, patient or staff information must not be transferred to a new role unless authorised by the relevant heads of service. A leaver's checklist should be completed in all cases.

6.2.5 Third Party Access to Systems

Any third party access to systems must have prior authorisation from both the IT and IG departments.

6.3 Storage of Information

All information stored on or within the UHB is the property of the UHB, unless there are contractual agreements that state otherwise. For legal purposes the UHB should be informed of, and agree to, all arrangements where we are hosting an information asset but are not the asset owner. An example of this is information stored in an email, which has been sent by a member of staff, but not in their capacity as an employee of Cardiff and Vale UHB (e.g. on trade union, University or Royal College business)

All software, information and programmes developed for the UHB by the workforce during the course of their employment will remain the property of the UHB.

Wherever possible, personal information should be stored on a UHB secure server. If it is to be stored outside a secure server (e.g. laptop c drive, flash stick): - the computer / device should be password protected and the data encrypted. The storage of personal data in the "Cloud" presently requires approval by the Welsh Information Governance Board

All systems should be backed up as part of an agreed backup regime. Where business critical information is held on local hard drives, portable devices or removable media, the IT department must be informed and agreements on how to back up the data reached.

Staff must:

- Ensure that all data is saved to network servers and not to the local device hard drive.
- Ensure that when leaving computers unattended for any length of time they either switch them off, lock the screen or log themselves off. Computers must not be left unattended or accessible to others.
- Staff must ensure that they use the information they have access to in an appropriate manner at all times.

6.4 Portable Devices and Removable Media

Whilst it is recognised that both portable devices and removable media are widely used throughout NHS Wales, unless they are used appropriately they pose a security risk to the organisation.

Portable devices include, but are not limited to, laptops, tablets, Dictaphones®, mobile phones and cameras. Where a portable device offers the functionality of a lock-screen, it is the responsibility of the user to ensure this functionality is securely activated.

All portable devices must either be encrypted, or access the network via NHS Wales approved applications (e.g. Mobile Device Management Software).

Users must ensure that all portable devices are physically connected (plugged in) to the UHB's network every 4 weeks and that all upgrades and cyber patches are updated at this time. Upgrades via wifi are not acceptable at the present time due to affordability and available bandwidth.

Users must not attach any personal (i.e. privately owned) portable devices to any NHS organisational network without prior authorisation.

Removable media includes, but is not limited to, USB 'sticks' (memory sticks), memory cards, external hard drives, CDs / DVDs and tapes. Appropriate controls must be in place to ensure any personal information copied to removable media is encrypted.

All removable media such as CDs must be encrypted if used to transport confidential information and should only be used if no other secure method of transfer is available. Users must not send details of how to unencrypt with the removable media.

6.5   Secure Disposal

For the purposes of this policy, confidential waste is any paper, electronic or other waste of any other format which contains personal data or business sensitive information.

6.5.1   Paper

All confidential paper waste must be stored securely and disposed of in a timely manner in the designated confidential waste bins or bags; or shredded on site as appropriate. This must be carried out in line with local retention and destruction arrangements.

6.5.2   Electronic

Any IT equipment or other electronic waste must be disposed of securely in accordance with local disposal arrangements. For further information, please contact your IT Department.

6.5.3   Other Items

Any other items containing confidential information which cannot be classed as paper or electronic records e.g. film x-rays, orthodontic casts, carbon fax/printer rolls etc, must be destroyed under special conditions. For further information, please contact your information governance team.

6.6 Transporting and relocation of information

6.6.1 Transporting Information

When information is to be transported from one location to another location, local procedures must be formulated and followed to ensure the security of that information.

6.6.2 Relocating information

When information is to be relocated to another location, local procedures must be formulated and followed to ensure no information is left at the original location.

6.7 Security of Assets

The UHB will maintain an inventory of the major assets associated with its information systems. Assets will include:

- Physical assets
- Software applications
- Data
- Back-ups

6.7.1 Physical Assets

Protection of IT equipment (including that used off site) is necessary both to reduce the risk of unauthorised access to data and to safeguard against loss or damage.

Data Centre's both local and national servers must be protected from power failures through use of uninterruptible power supplies (UPS), with backup generator power.

Ongoing maintenance arrangements are the subject of contractual agreement and only approved system engineers are allowed access to hardware.

Details of all faults on "maintained" equipment will be recorded by the UHB's IM&T Help Desks.

6.7.2 Software Applications

The IM&T Department will monitor all systems and PCs to ensure that all proprietary software products on the Local Area Network are used legally, licenced, and use SNOW as a Software Asset Management (SAM) solution.

In general the number of software installations of a given application e.g. Microsoft Office version xx cannot exceed the number of licences for that application held by the organisation. The UHB has purchased software specifically to monitor levels of usage of all software applications on the network. Regular reviews will be undertaken to ensure adequate licensing.

Copying of proprietary or organisational software, for use on computers that do not belong to the UHB, for any purpose other than authorised business, may infringe copyright and may be in breach of organisational policy. Copying of software in these circumstances may lead to disciplinary action.

Only software licensed to the UHB may be used on UHB equipment. Although it is not strictly illegal to use software legitimately belonging to an individual the installation and use of such software will not be permitted on any UHB equipment.

In the event of a dispute on the authorised validity of software the IM&T Security Manager has the authority to order the removal of any software from UHB equipment.

Software procured from academia cannot be loaded onto an NHS device i.e. students are not able to load university software onto the UHB device due to licencing restrictions.

Free software is not to be downloaded onto UHB computers due to the risk of malware, viruses and trojan's being introduced and affecting the network.

Staff need to remember that the same restrictions and requirements apply when utilising UHB IT equipment and working at home.

6.7.3 Data

Equipment (e.g. PCs, Laptops), data and software can be taken off-site but requires authorisation by the appropriate line manager.

Data must be saved to network servers and not to the local devices hard drive.
All laptops must be encrypted.

The destruction of data can only be authorised by the manager of the relevant system that the data is stored on, and "routed" via procurement.

Any storage media (e.g. hard disk, CD-ROM, diskette, magnetic or DAT tape) can only be disposed of after reliable precautions to destroy the data have been taken, and routed via procurement.

6.7.4 Back-ups

It is the responsibility of individual users to back up any systems that do not store their data centrally. The IM&T Department undertakes to back up on a daily basis the Network Servers and all centrally held data and will maintain detailed data housekeeping procedures for all systems they are responsible for.   Back-up and archive data will be accorded the same security as live data. All back-ups and archived data will be held off-site at CRI. Back-up data should be able to provide an adequate level of service and recovery time in the event of an emergency.

The IM&T Security Manager and all relevant managers and staff must be informed prior to any recovery from back-up data.

6.8   Security Incidents

An IM&T security incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of UHB business
- An embarrassment to the UHB

All incidents or information indicating a suspected or actual security breach should initially be reported to the immediate Line Manager and logged on the incident reporting system (e-Datix). In addition, the IT Security Manager or Information Governance Department should be informed for them to determine whether an actual security breach has taken place. Further comprehensive guidance will be developed to support this.

6.9 Business Continuity Planning and Risk Assessment

Business continuity planning is an organisational issue.

All Clinical Board areas will ensure that they have developed, maintained and tested adequate business continuity plans which will cover the following:

- A documented assessment of how long their users could manage without the relevant UHB system they depend on
- A documented assessment of the criticality of the loss of their system, including the impact of the short, medium and long term on UHB business activities
- Identification and agreement of all responsibilities and emergency arrangements
- Documentation of agreed procedures and processes
- An assessment of how resilience and continuity will be achieved.

The IM&T Department will ensure that it has an up-to-date Business Contingency/Disaster Recovery Plan in place that assesses the criticality of the loss of all systems managed and maintained by the IM&T Department.

6.10 The Network & Information Systems (NIS) Regulations

The Network & Information Systems Regulations 2018 (NIS Regulations) provides a legal framework to bolster the level of cyber and physical security of networks and information systems for the provisions of essential services and digital services.

The NHS is considered an Operator of Essential Services (OES) and as a Competent Authority, Welsh Ministers are responsible for overseeing the operation of the NIS Regulations. The NHS Wales Cyber Resilience Unit (CRU), hosted with DHCW provide guidance and support to Welsh Ministers.

To comply with NIS Regulations, all new implementations of a 'critical system' must be assessed by the Cyber Security Department against the Cyber Assessment Framework.

6.11 Suppliers of third-party systems

All suppliers who host or access UHB data need to comply with the Welsh Health Circular guidance on Cyber security and information governance (WHC/2017/025). For guidance on this Welsh Health Circular, please contact CV.IMT.Security@wales.nhs.uk

7.   Use of the internet

7.1   Position Statement

Internet access is provided to staff to assist them in the performance of their duties. The provision of these facilities represents a major commitment on the part of the UHB in terms of investment and resources.

All members of staff should become competent in using internet services to the level required for their role in order to be more efficient and effective in their day-to-day activities.

The UHB will support its workforce in understanding how to safely use internet services and it is important that users understand the legal, professional and ethical obligations that apply to its use. If used correctly, the internet can increase efficiency and safety within patient care.

7.2   Conditions & Restrictions on Internet Use

To avoid inadvertent breaches of this policy, inappropriate content will be blocked by default where possible. Inappropriate material must not be accessed. Exceptions may be authorised for certain staff where access to particular web pages are a requirement of the role. Subject matter considered inappropriate is detailed in the appendix.

Some sites may be blocked by default due to their general impact on network resources and access to these for work purposes can be requested by contacting the Local IT Service Desk.

Regardless of where accessed, users must not participate in any online activity or create or transmit or store material that is likely to bring the organisation into disrepute or incur liability on the part of NHS Wales.

Business Sensitive Information or Personal Data (which includes photographs and video recordings) of any patient, member of the public, or member of staff taken must not be uploaded to any form of non-NHS-approved online storage, media sharing sites, social media, blogs, chat rooms or similar, without both the authorisation of a head of service and the consent of the individual who is the Data Subject of that recording. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

It is each user's responsibility to ensure that their internet facilities are used appropriately.

7.3   Personal Use of the Internet

The UHB allows staff reasonable personal use of internet services providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental and reasonable and should be included in your personal time. In addition to this, users must not stream or download large volumes of data (e.g. streaming audio or video, multimedia content, software packages) as these may have a negative impact on network resources.

Staff must not load software packages onto their PC's or laptop's without authorisation from the IM&T Security Office. On no account must 'games software' be loaded on staff PC's or laptops.

Staff members are encouraged to use the CAV free Wi-Fi facilities by default on personally-owned devices.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to connect to the internet. Use of the internet under these circumstances must be through a secure VPN connection provided by the UHB. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of the internet is carried out at the user's own risk. The UHB does not accept responsibility or liability for any loss caused by or liability arising from personal use of the internet.

Internet access facilities must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

8.   Email

8.1.1 Use of NHS Wales email account

All UHB staff, must use their assigned NHS Wales email account when conducting UHB business. The use of private accounts, such as @gmail, @AOL and @doctors.org are not permitted when communicating any UHB activity such as, but not limited to: patient, staff or business sensitive data.

8.2   Inappropriate emails

Inappropriate content and material must not be sent by email. Inappropriate content including prohibited language in emails may be blocked. Subject matter considered inappropriate is detailed in the appendix.

Regardless of where accessed, users must not use the UHB's email system to participate in any activity, to create, transmit or store material that is likely to bring the UHB into disrepute or incur liability on the part of the UHB.

Some users may need to receive and send potentially offensive material as part of their role (for example - child protection). Arrangements must be authorised to facilitate this requirement.

8.3   Personal Data and Business Sensitive Information: Filtering and Misdirection

The NHS Wales network is considered to be secure for the transfer of any information including personal data and business sensitive information within NHS Wales and organisations with Transport Layer Security (TLS) enabled. This includes all email addresses within the NHS email directory that end in "wales.nhs.uk", which are hosted on the NHS Wales email service and the email services of TLS enabled organisations as listed on HOWIS. The list can be accessed here:

TLS Assurance (sharepoint.com)

Whilst it is safe and secure to transfer personal data between these addresses without encryption or passwords, the user must have a lawful basis for doing so. Please note that universities are not included in this list.

Transfer of personal data or business sensitive information between any email address not ending in "wales.nhs.uk", or TLS enabled is not currently considered secure. Where this type of information needs to be sent, appropriate security measures must be implemented. For example, the information should be sent via the Secure File Sharing Portal or via email with an appropriate level of encryption.

Users must be vigilant in ensuring that all emails are sent to the correct recipient and must check that the correct email address is used, for example by checking the NHS Wales email address book. Even where the recipient email address is considered secure, as a mitigating factor to avoid any inadvertent misdirection, encryption of any email attachment containing sensitive data should be considered. Misdirected emails should be reported via local incident reporting processes.

8.4   Personal Use of Email

The UHB allows staff reasonable personal use of their email account providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental and reasonable and should be included in your personal time. It is a requirement that you mark personal emails as personal in the subject heading. In doing so, staff should recognise that these emails will be monitored and may be subject to Information Access requests made to the UHB. Staff members are therefore strongly encouraged to use their personal email accessed via CAV free Wi-Fi facilities by default on personally-owned devices.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to send personal emails. Use of the email under these circumstances must be through a secure VPN connection provided by the UHB. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of email is carried out at the user's own risk. The UHB does not accept responsibility or liability for any loss caused by or liability arising from personal use of email.

The UHB's email must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

On occasion, suppliers may offer discounts that require UHB staff to validate their NHS employment, by subscribing via an NHS email accounts. The UHB does not wish to disadvantage staff by prohibiting this validation step. However, it is expected that any offers that are subscribed to must be decent, lawful and

appropriate to a professional environment, Additionally, the subscription should not hinder the performance of the individuals job role.

8.5   Records Management and Access to Information requests in respect of Email

Staff are encouraged not to use the email system as a storage facility. By design, all emails should either be deleted or saved securely to the appropriate record (e.g. to a clinical / business record or network drive).

Information held on computers, including those held in email accounts may be subject to requests for information under relevant legislation and regulation. As such any staff member who stores data in email folders should comply with section 5.2.1.1 Information Asset Registers.

All staff should be mindful that it may be necessary to conduct a search for information and this may take place with or without the author's knowledge or consent.

9.   Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for UHB staff and must be completed at commencement of employment and at least every two years subsequently. Non-NHS employees must have appropriate information governance training in line with the requirements of their role.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact their local Information Governance Department.

The UHB's workforce should become competent in using email services to the level required of their role in order to be efficient and effective in their day-to-day activities.

In order to ensure that this work is successfully supported and completed, there must be robust IGT programmes in place. To this effect, managers will:

- Complete training needs analyses for all staff as part of mandatory training in line with the Information Governance Training Programme Framework
- Manage staff training attendance -for new staff and refresher training
- Maintain ESR and local training records
- Identify and implement refresher training where incidents and poor performance has been identified

The arrangements for regular monitoring compliance are as follows:

- Overall compliance – to the DHIC via the SIRO
- Local compliance – to the clinical board performance reviews by clinical board directors
- Corporate arrangements – to the DHIC via the SIRO
- Compliance by formal assessment:

- Health and Care Standards 3.4 and 3.5
- Caldicott annual assessment - Internal Audits sponsored by the DHIC
- Annual and specific audits by the Welsh Audit Office
- Any other audits or assessments directed by the Welsh Government

10. Monitoring and compliance

The UHB trusts and respects the privacy of its employees and does not want to interfere in their personal lives. However, it reserves the right to monitor work processes to ensure the effectiveness of the service as a legitimate business interest. This will mean that any personal activities that the employee practices in work may come under scrutiny.

The UHB uses software to automatically and continually record the amount of time spent by staff accessing the internet and the type of websites visited by staff. Attempts to access any prohibited websites which are blocked is also recorded.

The UHB uses software to scan emails for inappropriate content and filters are in place to detect this. Where an email is blocked, emails may be checked for compliance when a user requests an email to be released. All email use will be logged to display date, time, username, email content; and the address to which the message is being sent.

Staff should be reassured that the UHB will take a considered approach to monitoring. However, it reserves the right to adopt different monitoring patterns as required. Monitoring is normally conducted where it is suspected that there is a breach of either policy or legislation. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

Managers are expected to speak to staff of their concerns should any minor issues arise. If breaches are detected, an investigation may take place. Where this or another policy is found to have been breached, disciplinary procedures will be followed.

Concerns about possible fraud and or corruption should be reported to the counter fraud department.

In order for the UHB to achieve good information governance practice staff must be encouraged to recognise the importance of good governance and report any breaches to enable lessons to be learned. They must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation. Ultimately, a skilled workforce will have the confidence to challenge bad information governance practice and understand how to use information legally in the right place at the right time. This should minimise the risk of incidents occurring or recurring.

11. Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;

- Practice change or change in system/technology; or

- Changing methodology.

12. Equality Impact Assessment

This policy has been subject to an equality assessment.

Following assessment, this policy was not felt to be discriminatory or detrimental in any way with regard to the protected characteristics, the Welsh Language or carers.

13. Documents to read alongside this Procedure

- Records Management Procedure
- Records Management Retention and Destruction Protocol and Schedule
- Information Governance Policy and Framework
- Data Protection Act Policy and Procedures
- Freedom of Information Act Procedure
- Risk Management Policy
- Information Risk Management Procedure
- Guide to Incident Reporting Incident Management Investigation and Reporting. [Serious incidents]
- Electronic and Paper Clinical Results Review and Retention Protocol
- Records Management Code of Practice for Health and Social Care 2016
- Data Quality Operational Management and Responsibilities
- Records Management Policy
- Records Management Retention and Destruction Protocol
- Validation at Source System (VASS) checks mandated by Welsh Government.
- Data Standard Change Notifications (DSCNs) issued by the National Wales Informatics Service
- Other relevant documents mandated by Welsh Government

Chilcott Rachel
13/02/2024 10:28:00

Appendix: Inappropriate use

For the avoidance of doubt, the UHB will generally consider any of the following inappropriate use:

- Knowingly using another person's NHS Wales email account and its functions, or allowing their email account to be used by another person without the relevant permission. Note: If an email is required to be sent on another person's behalf then this must be performed using delegated permissions functionality and must be approved for use beforehand;
- Allowing access to NHS Wales email services by anyone not authorised to access the services, such as by a friend or family member;
- Communicating or disclosing confidential or sensitive information unless appropriate security measures and authorisation are in place;
- Communicating or saving any information or images which are unlawful, or could be regarded as defamatory, offensive, abusive, obscene, hateful, pornographic, violent, terrorist, indecent, being discriminatory in relation to the protected characteristics, or using the email system to inflict bullying or harassment on any person.
- Knowingly breaching copyright or Intellectual Property Rights (IPR)
- 'Hacking' into others' accounts or unauthorised areas;
- Obtaining or distributing unlicensed or illegal software by email;
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network;
- Any purpose that denies service to other users (for example, deliberate or reckless overloading of access links or switching equipment);
- Deliberately disabling or overloading any ICT system or network, or attempting to disable or circumvent any system intended to protect the privacy or security of employees, patients or others;
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network;
- Expressing personal views that may bring the UHB into disrepute;
- Distributing unsolicited commercial or advertising materials;
- Communicating unsolicited personal views on political, social, or religious matters with the intention of imposing that view on any other person. This does not preclude Trade Union officials from communicating with staff on Trade Union related matters;
- Installing additional email related software, or changing the configuration of existing software without appropriate permission;
- Sending unlicensed or illegal software or data including executable software, such as shareware, public domain and commercial software without correct authorisation;
- Forwarding chain email or spam (unsolicited mail) within the organisation or to other organisations;
- Subscribing to a third party email notification using a NHS Wales email account for reasons not connected to work, membership of a professional body or trade union;
- Sending personal photos or videos;
- Registering an NHS Wales e-mail address with any third party company for personal use (e.g. department store accounts; online grocery shopping accounts);
- Access to internet based e-mail providers including services such as Hotmail, Freeserve, Tiscali etc is prohibited for reasons of security with the exception of:
  - Access to email services provided by a recognised professional body or a trade union recognised by the employer;
  - Any UK university hosted e-mail account (accounts ending in .ac.uk);
  - Any email account hosted by a body which the employee contributes to in conjunction with their NHS role, such as a local authority or tertiary organisation.

Annex 1: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
1/8/18	-	Andrew Fletcher, NWIS	NWIS policy documents for Information Governance, Information Security, Internet Use and Email Use
15/8/18	V0.1	Andrew Nelson	Amendments to draw documents together and include UHB 12 commandments, local variation and requirements for adoption of technical and data standards
17/8/18	V0.2	PJR, JW & AVN	Inclusion of DQ, data standards and medical records. Clarification of information ownership in respect of data stored on UHB network
15/11/2019	V0.3	JW & DJ	Incorporation of all-Wales Email Policy.
08/01/2024	V0.4	JW & DJ	

Reviewers

This document requires the following reviews:

Date	Version	Name	Position

Approvers

This document requires the following approvals:

Date	Version	Name	Position

Chilcott Rachel
13/02/2024 10:28:00

Annex 2: Equality Impact Assessment

Equality Impact Assessment (EQIA) Form		
Ref no: POL/IGMAG/IG/v1		
Name of the policy, service, scheme or project:	Service Area	
C&V Information Governance Policy	Information Governance	
Preparation		
Aims and Brief Description	The policy is a new All Wales Information Governance Policy. The policy will replace all local policies in this area.	
Which Director is responsible for this policy/service/scheme etc	Adaptation of existing policies and the NWIS policy	
Who is involved in undertaking the EQIA		
Have you consulted with stakeholders in the development of this policy?	*Yes. A sub group has developed this policy with a membership consisting of information governance leads and an OSSMB representative. IM&T leads and the Wales Partnership Forum have been consulted.* *The NHS Wales Information Governance Management and Advisory Group have approved the text of this Policy. The policy will be approved by the Wales Information Governance Board.*	
Does the policy assist services or staff in meeting their most basic needs such as; Improved Health, fair recruitment etc	*Yes. The policy will provide consistency throughout NHS Wales in having a single policy. This will ensure that staff who work across boundaries have a consistent standard to work to, hence strengthening the governance framework. A key driver during the process was the need to recognise that organisations needed to trust their staff.*	
Who and how many (if known) may be affected by the policy?	*All NHS Wales staff within the Health Boards and NHS Trusts.*	
What guidance have you used in the development of this service, policy etc?	*The policy is based on good practice and legal obligations as set out by the Information Commissioners Office and in the legislation. The policy has also been constructed from existing agreed principles and the corporate knowledge of its stakeholders.*	

Chilcott Rachel
13/02/2024 10:28:00

Equality Duties

The Policy/service/project or scheme aims to meet the specific duties set out in equality legislation.	Protected Characteristics										
	Race	Sex/Gender	Disability	Sexual orientation	Religion and Belief	Age	Gender reassignment	Pregnancy and Maternity	Marriage & civil	Welsh Language	Carers
To eliminate discrimination and harassment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote equality of opportunity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote good relations and positive attitudes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encourage participation in public life	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
In relation to disability only, should the policy / service / project or scheme take account of difference, even if involves treating some individuals more favourably?	✓										

Key	
✓	Yes
x	No
-	Neutral

Human Rights Based Approach – Issues of Dignity & Respect

The Human Rights Act contains 15 rights, all of which NHS organisations have a duty. The 7 rights that are relevant to healthcare are listed below.			
Consider is the policy/service/project or scheme relevant to:	Yes	No	N/A
Article 2: The Right to Life	X		
Article 3: the right not to be tortured or treated in a inhumane or degrading way	X		
Article 5: The right to liberty	X		
Article 6: the right to a fair trial	X		
Article 8: the right to respect for private and family life	X		
Article 9: Freedom of thought, conscience and religion	X		
Article 14: prohibition of discrimination	X		

Measuring the Impact

What operational impact does this **policy, service, scheme or project**, have with regard to the Protected Characteristics. Please cross reference with equality duties	
	Impact – operational & financial
Race	This is a high level framework approach which aims to achieve the values under the policy, it is the protection of everybody's information and gives clear guidelines. The policy details how the organization protects someone's data and security without prohibiting access to services and providing adequate access to data to meet individual needs and the appropriate sharing of data.
Sex/gender	
Disability	
Sexual orientation	
Religion belief and non belief	
Age	
Gender reassignment	
Pregnancy and maternity	
Marriage and civil partnership	

Other areas	
Welsh language	
Carers	

Outcome report

Equality Impact Assessment: Recommendations Please list below any recommendations for action that you plan to take as a result of this impact assessment					
Recommendation	**Action Required**	**Lead Officer**	**Time-scale**	**Resource implications**	**Comments**
1	Communication of the changes	Make sure staff aware of the changes	AF	ASAP	Time	

Recommendation	**Likelihood**	**Impact**	**Risk Grading**
1	2	2	4
2	2	2	4

Risk Assessment based on above recommendations

Reputation and compromise position		**Outcome**
It is providing security and reassurance to stakeholders that the information we hold is used appropriately and any breach may lead to fines and reputational damage.		To ensure that information is used and protected appropriately and a framework in place to ensure that happens.
Training and dissemination of policy		
More training and dissemination in Health Boards on this policy.		
Is the policy etc lawful?	**Yes** ☒	**No** ☐	**Review date**
Does the EQIA group support the policy be adopted?	**Yes** ☒	**No** ☐	**3 years**
Signed on behalf of C&V Equal Impact Assessment Group	S Brooks	Lead Officer	
Date:	8 May 2018	Date: 8 May 2018	

1	**2**	**3**	**4**	**5**
Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**

Chilcott Rachel
13/02/2024 10:28:00

| Statutory duty | No or minimal impact or breach of guidance / statutory duty

Potential for public concern

Informal complaint

Risk of claim remote | Breech of statutory legislation

Formal complaint

Local media coverage – short term reduction in public confidence

Failure to meet internal standards

Claims less than £10,000

Elements of public expectations not being met | Single breech in statutory duty

Challenging external recommendations

Local media interest

Claims between £10,000 and £100,000

Formal complaint expected

Impacts on small number of the population | Multiple breeches in statutory duty

Legal action certain between £100,000 and £1million

Multiple complaints expected

National media interest | Multiple breeches in statutory duty

Legal action certain amounting to over £1million

National media interest

Zero compliance with legislation
Impacts on large percentage of the population

Gross failure to meet national standards |

Risk Grading Descriptors

LIKELIHOOD DESCRIPTION	
5 Almost Certain	Likely to occur, on many occasions
4 Likely	Will probably occur, but is not a persistent issue
3 Possible	May occur occasionally
2 Unlikely	Not expected it to happen, but may do
1 Rare	Can't believe that this will ever happen

Chilcott,Rachel
13/02/2024 10:28:00

Report Title:	**Digital Directors' Peer Group**			Agenda Item no.	4.1
Meeting:	Digital & Health Intelligence Committee	Public	X	Meeting Date:	20th February 2024
		Private			
Status *(please tick one only):*	Assurance		Approval		Information	x
Lead Executive:	Director of Digital & Health Intelligence				
Report Author (Title):	Director of Digital & Health Intelligence				

Main Report
Background and current situation:

The creation of the Digital Directors' peer group in 2021 replaced the previous Digital Delivery Leadership Group meeting which came into existence in 2020 following the dissolution of the National Information Management Board which had been focused on providing an overview of information and IM&T issues nationally.

The establishment of the peer group brings Digital in line with other professions in the NHS in Wales (eg Directors of Finance peer group, Directors of Planning peer group) and is a welcome development.

Assurance is provided by the discussion and exchange of views and updates on a wide range of digital related issues via the regular monthly meetings compromising board-level leads for digital from across all NHS Wales organisations, including Welsh Government's Chief Digital Officer and members of DHCW's executive team.

Executive Director Opinion and Key Issues to bring to the attention of the Board/Committee:

The attached minutes of the last four meetings held in October 2023, November 2023, December 2023 and January 2024, provide an update on the scope and range of discussions on digital matters impacting on all NHS Wales organisations.

CAV UHB is represented by the Director of Digital and Health Intelligence (the Director of Digital Transformation acts as deputy when necessary).

Recommendation:

The Committee are requested to NOTE the minutes of the last meetings as follows:

- Minutes of Meeting – 3rd October 2023 (Appendix 1)
- Minutes of Meeting – 7th November 2023 (Appendix 2)
- Minutes of Meeting – 5th December 2023 (Appendix 3)
- Minutes of Meeting – 9th January 2024 (Appendix 4)

Link to Strategic Objectives of Shaping our Future Wellbeing:
Please tick as relevant

1. Reduce health inequalities		6. Have a planned care system where demand and capacity are in balance	
2. Deliver outcomes that matter to people		7. Be a great place to work and learn	x
3. All take responsibility for improving our health and wellbeing		8. Work better together with partners to deliver care and support across care sectors, making best use of our people and technology	x
4. Offer services that deliver the population health our citizens are entitled to expect		9. Reduce harm, waste and variation sustainably making best use of the resources available to us	
5. Have an unplanned (emergency) care system that provides the right care, in the right place, first time		10. Excel at teaching, research, innovation and improvement and provide an environment where innovation thrives	

Five Ways of Working (Sustainable Development Principles) considered
Please tick as relevant

Prevention		Long term	x	Integration	x	Collaboration	x	Involvement	x

Impact Assessment:
Please state yes or no for each category. If yes please provide further details.

Risk: No

Safety: Yes

Financial: No

Workforce: Yes

Legal: No

Reputational: Yes

Socio Economic: Yes

Equality and Health: Yes

Decarbonisation: No

Approval/Scrutiny Route:

Committee/Group/Exec	Date:

<table>
<tr><td colspan="2">Directors of Digital Peer Group Meeting
Draft Notes</td></tr>
<tr><td>Date of Meeting</td><td>Tuesday 3 October 2023</td></tr>
<tr><td>Time of Meeting</td><td>2pm – 5pm</td></tr>
<tr><td>Meeting Venue</td><td>MS Teams</td></tr>
<tr><td>Chair</td><td>Iain Bell</td></tr>
</table>

PRESENT:		APOLOGIES:	GUESTS:
Paul Solloway ABUHB	PS	Anthony Tracey HDUHB	Abigail Hayward NHS Executive
Dylan Roberts BCUHB	DR	Alison Ramsey NWSSP	Hannah Rix NHS Executive
Stuart Morris CTMUHB	SM	Pete Hopgood PTHB	Janice Jenkins ABUHB
David Thomas CVUHB	DT	Carl Taylor VNHST	Angela Jones ABUHB
Ifan Evans DHCW	IE	Leanne Smith WAST	Bryn Harries DHCW
Sam Lloyd DHCW	SL	Jonny Sammut WAST	Lee Mullin DHCW
Claire Osmundsen-Little DHCW	COL	Mike Emery WG	Carwyn Lloyd-Jones DHCW
Helen Thomas DHCW	HT	Richard Bowen 111 Programme	Lyn Rees DHCW
Sian Richards HEIW	SR	Alexander Vaughan-Mason 111 Programme	
Neil Jenkins NWSSP	NJ		
Iain Bell PHW	IB		
Vicki Cooper PTHB	VC		
Matt John SBUHB	MJ		
David Mason-Hawes VNHST	DMH		
Larissa Brock WNHSC	LB		

ITEM	DISCUSSION	ACTION
1. Welcome & Apologies, Meeting Notes and Matters Arising (Chair)	Iain Bell welcomed the group, apologies were noted as above, previous meeting notes were approved and the action log updated. Matters Arising: <u>National Portfolio and Leadership Board Reps</u> Due to the enthusiastic response to this request, it has been agreed that Stuart Morris and Anthony Tracey will attend these board meetings for the first 6 months – ie October '23 to March '24 - on behalf of the peer group. From April '24, Sian Richards and Vicki Cooper will attend for the next 6 months. <u>Nomination of New Chair of Digital Directors' Peer Group</u> Vicki Cooper and Anthony Tracey have agreed to be joint Vice Chairs for the next 3 months. A volunteer is needed for the role of peer group Chair from January 2024 and it was agreed to add this to the November meeting agenda for agreement.	
2. My Medical Record (PSA) Digital Implementation (Abigal Hayward, Hannah Rix - NHS Executive,	Presentation shared by Janice Jenkins (JJ) on the PSA Supported Self-Management Programme (for prostate cancer patients), timelines and integration into My Medical Record from the NHS Wales app. The request has been made to NHS organisations to reaffirm their commitment to the programme and consider roll out with future support in LHB IMTPs. JJ will shortly be outlining the key resources required locally and is also discussing national integration with the DSPP team.	

1

	Janice Jenkins, Angela Jones - ABUHB)	SM asked about future funding expectations and was advised that a decision was still pending regarding identifying Planned Care Boards as the main avenue for funding. There will be comms sent out shortly to clarify this, following discussions that are due to take place in the coming weeks. It was noted that urologists across organisations are keen that funding be made available. There was group discussion around strategic aims for integration in future and the need to ensure it is easy for suppliers to develop solutions that link to the NHS Wales app. Patients would also benefit from 'one front door' approach rather than having to duplicate their data using multiple apps for different health issues. IB suggested including this discussion to the next strategy session.	
3.	DHCW Strategy: Approach and Principles (Ifan Evans, Bryn Harries - DHCW)	IE introduced the item and shared a presentation explaining where the strategy needs to fit in relation to Welsh Government and the NHS in Wales. The DHCW statement of purpose has been updated to 'Making a digital force for good in health and care' and the proposal for 5 strategic principles was outlined: put people first, simplify everything we do, design for more data and digital, find more value and leave the past behind. The peer group were invited to give their input on the proposal and the following points were made: -What lessons to learn from building and rolling out systems such as RISP, LINC, SALUS etc. -How to become more agile and keep clinicians on side. -How to manage IMTP timeframes and WG funding timeframes. -How to do things differently and achieve the necessary cultural shift within the organisation. -Suggestion to change the focus on the future not the past with more specific aims to simplify the service offering. -Invitation from VC and IB to share their organisational strategies and discuss offline with IE. -Recognition of the more collaborative approach with LHBs that is already being undertaken, compared to previously with NWIS. -Don't undersell the power you have as an organisation. -Should your strategy be linked to the Duty of Quality principles etc? -Important to focus on the reprofiling and development of your workforce. Thanks were expressed for the group comments and the invitation given to send further feedback directly to IE who will aim to prepare an update for the November meeting.	
4.	SALUS Update (Richard Bowen, Alexander Vaughan-Morris - 111 Programme)	Item cancelled. Richard and Alexander sent apologies.	
5.	WCCIS Update and Next Steps	Lee Mullin shared a presentation on phase 2 of the programme, giving background on the challenges to date and the need for reshaping and	

Directors of Digital Peer Group 20231003

	(Lee Mullin - DHCW)	interoperability/data flow between systems. It was noted that the Master Services Agreement cannot be extended beyond March 2027 and many deployment orders will shortly be reaching full term. Regional workshops have been held over the past 2 weeks to elicit input from stakeholders on what the future solution should look like. There was a mixed response from the peer group with some directors expressing excitement about the future plans and others acknowledging the current negative impact on patient care and the challenge of working with certain partners. All agreed that the critical success factor would be ensuring that the data is useable and transactional in real time in the future. HT offered to discuss specific issues further after the meeting with relevant directors.	
6.	Microsoft 365: Benefits Realisation (Sam Lloyd, Carwyn-Lloyd Jones, Lyn Rees – DHCW)	SL introduced the item and Lyn Rees (LR) shared a presentation on the mission of maximising taxpayer value and investment in M365, including the aims, approach, targets and benefits. He also outlined plans for dealing with old mailboxes and legacy Exchange servers as well as the migration of all NHS Wales staff to Multi-Factor Authentication. CLJ checked that the group were definitely supportive of the following 3 product replacement projects: MailMarshal replacement, on-premises mailbox cleanup and Azure MFA migration. LR advised that the use of MS Teams to replace AttendAnywhere is still in development with the first discovery workshop due to take place this Friday. In addition, they are evaluating the security features within the toolset and working alongside the OSSMB Task & Finish Group for the migration of mailboxes. COL added that further discussion was needed over the opportunity to repurpose any savings made but that money would be released within local organisations as a result of the migration from Exchange. There was group discussion around increasing the use of M365 and the need for a clearer roll out strategy, with some directors expressing concern over its under-utilisation and therefore lack of full benefit from the investment. The suggestion was made for the Centre of Excellence to take a more active role in this process and the creation of a toolkit to support implementation.	
7.	Implications of Financial Spending Decisions (Chair/All)	There was brief discussion around local spending decisions and the main points were raised as concerns: issues around health protection (PHW), Covid response, recruitment and digital inflation.	
8.	AOB	<u>AHP Digital Investment Proposal (IE)</u> It was noted that Claire Bevan (CB) will be attending next month's meeting alongside Mathew King (Deputy DoTHS CVUHB) to discuss the DoTHS digital investment proposal and the AHP workforce development plan. CB is requesting feedback on the business case. Although the group were broadly supportive, there had been a mixed response to the proposal and	

3

Directors of Digital Peer Group 20231003

	clarity was requested regarding peer group governance and the use of voting to support items in principle.

HT stated that the peer group could agree items in principle but that each statutory NHS organisation would have to discuss proposals at local board level and also discuss funding with Welsh Government. IB added that care needed to be taken in managing expectations so that guest speakers were aware they were attending peer group meetings to share information, not to gain approval from organisations on an All Wales basis. The correct governance mechanisms should be used for programme approval instead.

It was agreed that the Terms of Reference for the peer group should be revisited and HT advised that Paul Mears is considering this issue for all Executive peer groups and a peer group governance review would be underway shortly.

<u>CGI (COL)</u>
COL advised that DHCW are working on a value statement but that some data gaps still exist. If organisations would like a workshop with CGI they would be happy to meet and COL offered to email relevant LHBs with the details. | |
| | End of meeting. | |
| **Next Meeting: Tuesday 7 November Face to Face at DHCW Cardiff**
9.30am peer group meeting
1.30pm strategy meeting | | |

Chilcott Rachel
13/02/2024 10:28:00

4

Directors of Digital Peer Group 20231003

Directors of Digital Peer Group Meeting **Draft Notes**			
Date of Meeting	Tuesday 7 November 2023		
Time of Meeting	9.30am – 1.35pm		
Meeting Venue	Board Room, DHCW, Ty Glan-Yr-Afon, 21 Cowbridge Rd East, Cardiff / MS Teams		
Chair	Iain Bell		

PRESENT: V=Virtual		**APOLOGIES:**	**GUESTS:**
Paul Solloway ABUHB	PS	Alison Ramsey NWSSP	Hamish Laing Swansea University
Dylan Roberts BCUHB **V**	DR	Pete Hopgood PTHB	Keith Farrah DHCW
Stuart Morris CTMUHB	SM	Carl Taylor VNHST	Laurence James DHCW
David Thomas CVUHB	DT	Jonny Sammut WAST	Mathew King CVUHB
Ifan Evans DHCW	IE		Claire Bevan DHCW
Sam Lloyd DHCW	SL		Natasha Dunkley WG
Claire Osmundsen-Little DHCW	COL		Ryan Perry WG
Helen Thomas DHCW (part)	HT		Rebecca Cook DHCW
Anthony Tracey HDUHB **V**	AT		Carwyn Lloyd-Jones DHCW
Sian Richards HEIW	SR		Alex Percival DHCW
Neil Jenkins NWSSP **V**	NJ		Matt Palmer DHCW
Iain Bell PHW	IB		
Vicki Cooper PTHB	VC		
Matt John SBUHB	MJ		
David Mason-Hawes VNHST **V**	DMH		
Mike Emery WG	ME		
Larissa Brock WNHSC	LB		

ITEM	DISCUSSION	ACTION
1. Welcome & Apologies, Meeting Notes and Matters Arising (Chair)	Iain Bell welcomed the group, apologies were noted as above.	
2. Digital Medicines Transformation Programme – Shared Medicines Record Update (Hamish Laing, Keith Farrar, Laurence James)	HL introduced the item, sharing a presentation and explaining the rationale of improving access to patient medicine data across the system, reducing error rates by up to 40% and thereby reducing unnecessary hospital bed occupation. The interoperability between systems was highlighted, with a central data store allowing clinicians to view prescribing information across pharmacy, dentistry, secondary care etc. GPs will then have the option to accept the updated information sent to the practice from hospital when their patient is discharged. The SMR programme is currently in private beta testing. ePMA systems are out to procurement with a specific requirement for interoperability. The team are also working closely with the Scan 4 Safety programme and are keen to ensure sufficient resourcing will be in place with timely training for staff during rollout. There was discussion around the resilience needs across all organisations, reliance on adequate WiFi provision and the importance of capturing measurable financial benefits after rollout.	

Chilcott Rachel
13/02/2024 10:28:00

1

Directors of Digital Peer Group 20231107

3.	Digital Improvement and Workforce Development Plan – Allied Health Professions and Health Care Sciences (Mathew King, Claire Bevan)	MK introduced the item and highlighted the disparity across professions regarding informatics job roles, a historic lack of engagement with AHP/HCS colleagues on system development and the need for additional funding to align AHP/HCS professions with the national digital strategy. There is currently no spare resource to contribute to the delivery of digital maturity across these services, however rolling this out would reduce waiting times, length of hospital stays etc. There was wholehearted support from the group to consider the proposal with the following points made: -An evidence base is needed to secure future IMTP funding, which takes significant time to collate. -Informatics posts need to be collaborative to bring a range of benefits across the professions. -This should be Business As Usual and would be a key contributing factor to digital maturity. -What needs to give in order for LHBs to give this request higher priority? -There is increasing need for senior leaders to view digital as a solution to help address current system pressures. CB added that the proposal would be submitted to the new National Portfolio and Leadership Board and asked that all attempt to influence leaders within their own organisations to support a coordinated approach across Wales.	
4.	New Peer Group Chair for 2024 (Iain Bell)	Anthony Tracey has volunteered to be new the Chair of the group from February 2024 with Vicki Cooper as Vice Chair.	
5.	WG Update (Mike Emery, Ryan Perry)	Slides were shared giving an update on planning, national initiatives, comms and the financial position. It was noted that MHSS has approved a £6m increase in DPIF capital allocation for FY 23-24; funding letters are currently being drafted. For FY 24-25 capital spending will be particularly pressured due to LIMS and RISP demands. ME requested that emphasis continue to be made on the return on investment/value within local organisations. There was a polite request from the group that the timing of investment offers from Welsh Government be improved to enable better planning earlier in the financial year. It was noted that the AI workplan is currently being developed for Wales, with more detail to follow in early 2024. There is a Directors of Planning / PP4L Networking event taking place next Monday 13 November with the theme of information and data. IE circulated relevant information to the group. National Portfolio Leadership Board Meeting Update A wide range of discussions around the purpose/remit of the Board took place on 30 October and the Terms of Reference will be reframed as a result, with possible amendments to the attendee list in future.	

Chilcott Rachel
13/02/2024 10:28:00

2

Directors of Digital Peer Group 20231107

	SM requested a future discussion around virtual wards/telehealth as clarity is needed across executives and policy leads. ME responded that he has been asked to lead an out of hospital care model conversation and will be working with Rhian Matthews, linking in with TEC Cymru. AT volunteered to be involved and commented on the recent work done by the Health Foundation reviewing virtual wards in England. There was group agreement to invite TEC Cymru/Mike Ogonovsky to a meeting in the near future and LB added the item to the forward planner.	
6. NDR Present and Future (Ifan Evans, Rebecca Cook)	IE introduced the item and RC brought an update on the key programme achievements since July, including the successful go-live date in August of 3 national services in the catalogues. An overview was given of the Care Data Repository and development deadlines for Q3 (demographics) and Q4 (medicines) this financial year. Work is also underway on the data catalogue for the National Data and Analytics Platform and Q4 will see work on enhanced data privacy and integrated machine learning capabilities. LHBs now have access to the APIs that read and write to the CDR. Deep dive pilot projects are underway with PHW, SBUHB, ABUHB and the NHS Executive. Each NHS organisation will have control over their own data and future spend will be monitored by DHCW. Examples of Big Data Fund winning bids were given and the resulting dashboards. There are ongoing legal conversations underway regarding a mechanism to more easily obtain and store data from Primary Care practitioners. It was noted that in HDUHB data from managed practices was already accessible. There has been excellent collaboration across partner organisations to date and RC asked the group for input on key focus areas and what would be future evidence of success. The following comments were made: -We all have constraints and boundaries within our organisations but need to ensure alignment in our thinking. -We need to decide what to focus on locally vs nationally. -Some organisations are getting rid of local warehousing and moving to NDR which will have a good impact on future strategy, business analytics and leverage towards other new technology. -SR requested that all organisations agree to share data on workforce shifts, outcomes, risks etc. -VC explained that PTHB have completed the data catalogue and linked it to the Cloud, having already signed up to Azure, and are now engaging with Heads of Service re ease of access. Thanks were expressed to RC for the programme work to date and IE added that progress is needed in relation to Information Governance. RC has requested that NDR IG leads review the challenges of joint controllership of the data and HT encouraged all to invite RC to discuss further with Heads of Information and Policy Leads.	

3

Directors of Digital Peer Group 20231107

7. Data Centre 2 Transition (Carwyn Lloyd-Jones, Alex Percival)	Presentation shared on the project background and issues encountered while merging the new network with existing NDC and CDC networks. Network implementation is therefore 4 weeks behind the original plan. Pending assurances from third parties and remedial changes being undertaken, the fabric edge release will take place on 24 November. An overview was given on the risks regarding the additional changes required and transition weekends, with possible disruption / loss of services and the need for contingency plans, as well as the financial implications of delay beyond this financial year. CLJ requested a representative from the peer group to join the DC2T Project Board and David Taylor volunteered. The group then asked that the transition dates be amended to midweek late evenings where possible due to the added pressures on health services over weekends. The group agreed on fortnightly comms updates and AP committed to providing sufficient notice periods for the transition events and to circulating a revised schedule of dates.	
8. Citrix Subscriptions (Carwyn Lloyd-Jones, Matt Palmer)	CLJ informed the group that Citrix are now part of Cloud Software Group following a recent buy-out. Details were shared of the range of contracts held across each NHS organisation and conversations that have begun regarding the cost of licence renewals which will hugely increase when renewed. DHCW are working with Citrix and all NHS organisations to align all renewals to December 2024 with the aim to migrate onto one single subscription with a fixed price deal for 3 years. There was discussion around the aim to extricate organisations from the Citrix contract in 3 years' time - some products are being decommissioned so certain licences will no longer be needed. Also, the strategic long term plan for WPAS is under review and external consultants will be brought in for advice. CLJ agreed to invite Directors of Digital and COL to a future contract meeting with Citrix. VMware Cost Increases The peer group were made aware of an increase in the price of licences used extensively by DHCW and they are being moved to a subscription model. Following the takeover of VMware by Broadcom in October, DHCW brought forward the licence renewal date to Oct 2023 to avoid further price hikes. SL advised that a long term plan and cost review will be compiled shortly. Directors of Finance have already been informed of the trajectory of SLA costs for next 3 years and there are other inflationary pressures currently unfunded and that need highlighting to Welsh Government. **ACTION COL and AT agreed to lead a discussion on finance inflationary pressures and the future narrative at a future peer group afternoon strategy session.**	**01 – AT, COL**

4

Directors of Digital Peer Group 20231107

9. AOB	No further items were raised.	
	End of meeting.	

<div align="center">

Next Meeting: Tuesday 5 December
2pm peer group meeting face to face at PHW, CQ2 / MS Teams

</div>

5

Directors of Digital Peer Group 20231107

Directors of Digital Peer Group Meeting Draft Notes	
Date of Meeting	Tuesday 5 December 2023
Time of Meeting	2pm – 5pm
Meeting Venue	MS Teams
Chair	Anthony Tracey / Vicki Cooper

PRESENT:		APOLOGIES:	GUESTS:
Paul Solloway ABUHB (part)	PS	Stuart Morris CTMUHB	Matt Cornish DHCW
Dylan Roberts BCUHB (part)	DR	Sam Lloyd DHCW	Jonathan Pinkney DHCW
Sion Jones BCUHB (part)	SJ	Neil Jenkins NWSSP	Carwyn Lloyd-Jones DHCW
Suzanne Rodgers CTMUHB	SR	Alison Ramsey NWSSP	Ryan Perry WG
David Thomas CVUHB	DT	Pete Hopgood PTHB	Rebecca Ellis-Owen WG
Ifan Evans DHCW (part)	IE	Iain Bell PHW	Kirsty Robathan-Smith NHS Executive
Claire Osmundsen-Little DHCW	COL	Carl Taylor VNHST	
Helen Thomas DHCW	HT	Jonny Sammut WAST	
Anthony Tracey HDUHB	AT	Mike Emery WG	
Sian Richards HEIW	SR	Anne Watkins DHCW	
Simon Johnson-Reynolds NWSSP	SJR		
Vicki Cooper PTHB	VC		
Matt John SBUHB	MJ		
Larissa Brock WNHSC	LB		

ITEM	DISCUSSION	ACTION
1. Welcome & Apologies, Meeting Notes and Matters Arising (Chair)	Anthony Tracey (AT) and Vicki Cooper (VC) shared the Chair for the meeting in IB's absence. Apologies were noted as above. Matters Arising: Ryan Perry (RP) updated the group on Welsh Government cyber funding allocation, advising that some letters have already been issued but PTHB, SBUHB and HDUHB bids were being reconsidered. The peer group requested transparency on which bids had been successful so that all organisations could better understand why and how money was to be allocated. RP responded that Mike Emery had asked the team to pull together this information. WG are aware of the need for more capital and revenue cyber funding and tried to show impartiality during the allocation process. For those that were unsuccessful, if there is surplus at the end of the FY then those bids will be reconsidered. RP also advised that Rebecca Andrews is taking on a new role and there will therefore be a secondment position available at Band 8b, covering RISP, cancer etc. The job description and advert will be circulated shortly.	
2. Digital Maturity & Team Wales Actions (Helen Thomas, Dylan Roberts)	Two papers were shared. Helen Thomas (HT) updated the group on discussions at the recent Leadership Board meeting about the Team Wales actions relating to digital – ie finding a blueprint for the way forwards and agreeing on a commercial procurement strategy for Wales. Dylan Roberts (DR) updated the group on Carol Shillabeer's aim to use the HIMSS/KLAS assessment work as a means to transform BCUHB by	

1

Directors of Digital Peer Group 20231205

	improving benefit realisation from existing programmes as well as undertaking some simplification and standardisation, with significant change and investment required to join up systems and handover processes. This will therefore increase clinicians' time with patients and overall efficiency, ultimately reducing system pressures but workflow is key. DR then shared 8 options currently under consideration for meeting the business need (see presentation for details). The draft strategic outline business case will be completed in early January, explaining the rationale behind the final option chosen. There was agreement from other Directors that they were facing very similar issues and enthusiasm was expressed for a wider discussion pan-Wales involving NHS Directors of Planning, Finance and Chief Executives. It was proposed that the matter be discussed again in early 2024 and the item was added to the forward planner.	2	
3. DSPP NHS Wales App – User Engagement and the Patient Facing Platform (Matt Cornish)	Matt Cornish (MC) shared update slides and advised that approximately half of GP practices have rolled out the app to date in Wales and all should do so by April 2024. MC advised that there is work yet to be done on governance and working relationships, especially for SBUHB. Work packages are being completed rapidly and next week a governance paper will be submitted to the DSPP Programme Board in relation to suppliers. The team are working on digital inclusion issues and will be evaluating who has/has not adopted use of the app. Also, clarity is being sought on how to avoid duplication and confusion between what is available to clinicians/patients in the core app and what is available via other providers. Comms toolkits will be developed to allow standardised messaging for the public and some patients will need to be moved over from My Health Online before that service is retired. The team are also engaging with the Planned Care Programme and a workshop will be held in January for clinical leads. Concern has been raised about 'user drift' in England since some of the features that users want have not been built at significant pace, causing a lack of motivation to keep using the app. It is hoped that this will not be the case in Wales. Another update will follow in a few months' time.		
4. Digital Maternity Cymru Architecture (Jonathan Pinkney)	Jonathan Pinkney (JP) shared an overview of progress to date and the future plan. HT added that the work is a Welsh Government priority and there is a variety of key background discovery work that was completed and is now available to LHBs. It was noted that the resource cost will be circa £13.8m for implementation. Sian Richards (SR) added that HEIW's workforce plan will include relevant education and training and mentioned the opportunity to align the two pieces of work. There was then a group discussion around the need to review the list of various programmes and their priorities, as well as the restrictions on resources (especially lack of funding for permanent staff). The group		

2

Directors of Digital Peer Group 20231205

		agreed that in early 2024 they would discuss the foundational systems needed, workforce requirements and priority pipeline. Kirsty Robathan-Smith (KRS) expressed support for this process on behalf of the NHS Executive.	
5.	DHCW Draft Strategy (Ifan Evans)	Ifan Evans (IE) shared a presentation on the strategy and end goals until 2030, namely: 1. Provide a platform for enabling digital transformation. 2. Deliver high quality digital services and products. 3. Expand the digital health and care record and the use of digital to improve health and care. There was peer group discussion around the strategic aims listed for each of the above and the need for greater collaborative working across organisations to turn the national focus onto digital to help resolve the current service pressures. The group also commented on some of the wording used in the strategy slides and suggested more emphasis on the role of mutual partnership in enabling NHS organisations to facilitate patient care. HT added that the DHCW Board is keen to engage more widely with other Executive peer groups regarding the strategy and there was agreement to review it again at the January peer group meeting.	
6.	Cyber Task and Finish Group Update (Carwyn Lloyd-Jones)	A presentation was shared on the progress made across organisations regarding weak passwords, obsolete accounts and operating systems, securing firewalls and MFA (the latter is now escalated to OSMMB for consideration). In addition, the request was made by CLJ for greater uptake of licences for the Microsoft 365 CoPilot with the deadline extended to 8 December, else they will be reallocated to other organisations. It was noted that the DHCW Board has approved the procurement regarding SIEM but work is still underway as to how it can be funded. Claire Osmundsen-Little is in discussion with Welsh Government over the issue - some organisations have agreed to redirect funding to DHCW to cover it but not all.	
7.	AOB	No further items were raised.	
		End of meeting.	
Next Meeting: Tuesday 9 January 2024 Face to Face at DHCW Cardiff 9.30am peer group meeting 1.30pm strategy session			

Chilcott Rachel
13/02/2024 10:28:00

3

<table>
<tr><td colspan="2">Directors of Digital Peer Group Meeting
Draft Notes</td></tr>
<tr><td>Date of Meeting</td><td>Tuesday 9 January 2024</td></tr>
<tr><td>Time of Meeting</td><td>9.30am – 12.40pm</td></tr>
<tr><td>Meeting Venue</td><td>Board Room DHCW, Cardiff / MS Teams</td></tr>
<tr><td>Chair</td><td>Iain Bell</td></tr>
</table>

PRESENT: V=Virtual		APOLOGIES:	GUESTS:
Paul Solloway ABUHB	PS	Alison Ramsey NWSSP	Ryan Perry Welsh Government
Dylan Roberts BCUHB	DR	Pete Hopgood PTHB	Lauren Harkins Welsh Government
Stuart Morris CTMUHB	SM	Anthony Tracey HDUHB	Hamish Laing Swansea University
David Thomas CVUHB	DT	Sam Lloyd DHCW	Jenny Pugh-Jones HDUHB
Ifan Evans DHCW	IE	Jonny Sammut WAST	Michelle Cook TEC Cymru
Claire Osmundsen-Little DHCW	COL		Sara Khalil TEC Cymru
Helen Thomas DHCW (part)	HT		Robert Bleasdale TEC Cymru
Carolyn Williams HDUHB V	CW		Claire Nelson NHS Executive
Sian Richards HEIW	SR		Alison Maguire DHCW
Neil Jenkins NWSSP V	NJ		
Iain Bell PHW	IB		
Vicki Cooper PTHB	VC		
Matt John SBUHB	MJ		
Carl Taylor VNHST	CT		
Mike Emery WG (part)	ME		
Larissa Brock WNHSC	LB		

ITEM	DISCUSSION	ACTION
1. Welcome & Apologies, Meeting Notes and Matters Arising (Chair)	IB chaired the meeting and apologies were noted as above.	
2. Electronic Prescription Service for Primary Care (Hamish Laing, Jenny Pugh-Jones)	HL introduced the item and shared a presentation. JPJ gave an update on the software development. In November 2023 EPS went live in Rhyl using one GP practice and one pharmacy - over 600 EPs have been generated since then and claimed successfully by patients. Work is underway with system suppliers, GP practices and pharmacists for wider rollout across Wales, with the next site due to go live in February. Life Sciences Hub Wales are managing the fund to incentivise suppliers to adapt their systems to allow EPS. It was noted that EMIS Web is assured but Cegedim Vision 3 does not include EPS and may not enter assurance in Wales until summer 2025. Half of GP practices using Vision wish to move to EMIS so a plan is needed to migrate them as soon as possible. Consensus is also needed on solutions for non-medical prescribers, GP OOH service/111 and the prison service. SM requested an update on the 111 programme and HL advised that the contract with Adastra has been extended and Richard Bowen wishes to prioritise EPS in 2024.	

1

Directors of Digital Peer Group 20240109

3.	TEC Cymru – Telehealth Update (Robert Bleasdale, Sarah Khalil, Michelle Cook)	RB introduced the item and sent apologies from Mike Ogonovsky. SK shared a presentation advising that phase 2 procurement started in December 2023 and the supplier response was received yesterday. A market analysis refresh has taken place and the main focus areas are as follows: -comprehensive evaluation -identification of barriers to adoption -collaborative development with the NHS Executive -demonstration of value in hospital admission avoidance, bed day savings etc. The 2024 plan was shared regarding governance, procurement and implementation, with go-live planned for March. DHCW have provided consultancy in preparation for future integration with the national architecture and partnership working is underway with relevant LHBs to cover their local integration requirements. There was peer group discussion around supplier engagement to ensure adherence to regulatory standards for data classification and interoperability/integration with other systems such as EMIS. MC added that the team will also be considering the future broader suite of remote patient care provision and raising this with Regional Partnership Boards. RB confirmed that the team had engaged with the Value in Health team. Sally Lewis is a member of the programme board and aiming to ensure alignment with existing PROMS work. The future rollout plan will be submitted to CEOs in due course and it was noted that the preferred term used by policy leads is 'enhanced community care' rather than 'virtual wards'.	
4.	Welsh Government Update (Ryan Perry, Lauren Harkins)	RP introduced Lauren, the new Deputy Director for Digital Strategy and Policy. ME sent his apologies and joined the meeting later. RP advised there is very tight DPIF funding for the next financial year for both capital and revenue expenditure and work is underway with the Welsh Treasury to see what flexibility there might be within wider budgets. The PSBA contract with BT is likely to be extended by a further 2 years, pending agreement from Directors of Digital. There were questions around the Investment Board meeting schedule and RP responded that all sub-groups will meet ahead of the main board meeting on the first Tuesday of each month from February onwards. The Terms of Reference need to be clarified as well as governance for the sub-group structure. It was noted that LHBs had produced 10 year spending forecasts last year but there was a funding gap in relation to legacy digital infrastructures and concern was expressed over the need for sustainable funding in future.	
5.	Diagnostics Programme – Strengthening	CN gave an overview of the Programme, its governance and the digital prioritisation process within Planned Care. It was noted there is currently no official link between the Diagnostic Programme Board and the National	

2

Links with Digital Directors (Claire Nelson, Alison Maguire)	Portfolio & Leadership Board and RP commented that this is currently under review by Mike Emery. AM brought an update on the RISP programme and the group expressed some concerns over the risk of timeline slippage. AM added that the team is working on a resource plan for data migration testing for LHBs and on aligning the plans with Philips/Soliton. There was discussion around the issues faced by whichever NHS organisation first rolls out a significant programme and the need for extra funding/resource. Mutual support is needed across organisations throughout the clinical change process and the recruitment of additional resource can take several weeks. CN and AM agreed to raise this issue at the next board meeting. The group were advised of data storage issues for LIMS 2.0 and there seems to be a lack of LHB involvement in the working group which needs to be addressed. An overview was given of projected digital cellular pathology costs and plans have been submitted to LHBs for approval (Suzanne Rankine is CEO lead). Concerns were expressed by IE at how low the DHCW support costs seemed for a programme of this scale. CN agreed to circulate further information to the group with breakdown costings for each LHB and HT added that DHCW would respond with detailed feedback on costings for extra workforce etc. **ACTION CN to circulate paper.** Other developments were highlighted such as Point of Care testing, increasing staff digital literacy, improving productivity, genomics storage requirements, as well as the need to address the poor data currently available in diagnostics. The group suggested that a one page brief be produced for Digital Directors/DoTHS and agreed to invite Claire Nelson/Alison Maguire to a future meeting for further update. **ACTION LB to add to forward planner.**	**01 – CN** **02 - LB**
6. Cancer Update (Helen Thomas)	A paper has been submitted to WG colleagues on work done so far to replace CaNISC. There will be funding of around £2.7m next FY and there is more work to be done on product development and defining how much revenue funding would be needed going forwards. The group discussed the importance of optimising cancer patient data as well as the need for PHW to use the information for screening services.	
7. AOB	<u>Terms of Reference and Representation on National Groups (SM)</u> There was agreement to review the peer group ToR and the list of representatives on national groups. It was agreed that an efficient reporting mechanism to the group is needed following attendance at various programme board meetings. **ACTION LB to add item to next meeting agenda.** <u>New Chair</u> Thanks were expressed to IB for his chairing of the group and it was noted that Anthony Tracey would be taking over the role from February.	**03 - LB**

3

Directors of Digital Peer Group 20240109

	End of meeting.	
Next Meeting: Tuesday 6 February 2024 In Person **9.30am peer group meeting / 1.30pm strategy session**		

Chilcott Rachel
13/02/2024 10:28:00

4

Directors of Digital Peer Group 20240109