



PWYLLGOR ADNODDAU CYNALIADWY SUSTAINABLE RESOURCES COMMITTEE

DYDDIAD Y CYFARFOD: DATE OF MEETING:	27 June 2023
TEITL YR ADRODDIAD: TITLE OF REPORT:	Information Governance Sub-Committee Annual Report 2022/23
CYFARWYDDWR ARWEINIOL: LEAD DIRECTOR:	Huw Thomas, Executive Director of Finance
SWYDDOG ADRODD: REPORTING OFFICER:	Anthony Tracey, Digital Director

Pwrpas yr Adroddiad (dewiswch fel yn addas)

Purpose of the Report (select as appropriate)

Er Sicrwydd/For Assurance

ADRODDIAD SCAA

SBAR REPORT

Sefyllfa / Situation

The purpose of this paper is to present the Information Governance Sub-Committee (IGSC) Annual Report 2022/23 to the Sustainable Resources Committee (SRC). The Information Governance Sub-Committee Annual Report provides assurances in respect of the work that has been undertaken by the Sub-Committee during 2022/23 and outlines the main achievements which have contributed to robust integrated information governance across the Hywel dda University Health Board (HDUHB).

Cefndir / Background

The Health Board's Standing Orders and the terms of reference for the Information Governance Sub-Committee require the submission of an Annual Report to the SRC to summarise the work of the Sub-Committee and to identify how it has fulfilled the duties required of it.

The fundamental purpose of the Sub-Committee is to provide assurance to the SRC on the Health Board's information governance assurance frameworks, including risk assurance, and compliance with information governance legislation, guidance and best practice.

The Annual Report specifically comments on the key issues considered by the Sub-Committee in terms of the information governance and security framework, statutory compliance, and the adequacy of the policies, procedures and action plans in place.

Asesiad / Assessment

The IGSC Annual Report is attached at Appendix 1.

Argymhelliad / Recommendation

The Committee is asked to **RECEIVE ASSURANCE** from the report that the IGSC has fulfilled the duties required, as per the Sub-Committee's Terms of Reference.

Amcanion: (rhaid cwblhau) Objectives: (must be completed)	
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Not Applicable
Galluogwyr Ansawdd: Enablers of Quality: Quality and Engagement Act (sharepoint.com)	6. All Apply
Parthau Ansawdd: Domains of Quality Quality and Engagement Act (sharepoint.com)	7. All apply
Amcanion Strategol y BIP: UHB Strategic Objectives:	All Strategic Objectives are applicable
Amcanion Cynllunio Planning Objectives	All Planning Objectives Apply
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2021-2022	9. All HDdUHB Well-being Objectives apply

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	GDPR Compliance Action Plan
Rhestr Termiau: Glossary of Terms:	UK GDPR – General Data Protection Regulations 2016 DPA – Data Protection Act 2018 IG – Information Governance IAO – Information Asset Owner IAA – Information Asset Administrator/Assistant IAR – Information Asset Register
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Adnoddau Cynaliadwy: Parties / Committees consulted prior to Sustainable Resources Committee:	Information Governance Sub-Committee

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Failure to comply with data protection legislation could result in a monetary fine or penalty.
Ansawdd / Gofal Claf: Quality / Patient Care:	Poor practice around information governance in relation to poor understanding, loss of information and a lack of training for staff has a direct impact on the quality of patient care
Gweithlu: Workforce:	Ensuring that all Health Board staff have the required information and training to assist them in complying with Information Governance procedures.
Risg: Risk:	Failure to comply with data protection legislation will result in poor IG practices being in place throughout the Health Board. It may also lead to investigations by the Information Commissioner's Office and could result in a monetary fine or penalty.
Cyfreithiol: Legal:	Failure to comply with the UK General Data Protection Regulations 2018, the Data Protection Act 2018, the Freedom of Information Act 2000 and the common law duty of confidentiality will result in the Health Board not being fully compliant with data protection legislation.
Enw Da: Reputational:	A lack of trust by patients in the HDUHB's ability to safeguard their information may dissuade people from providing information that is essential to providing them with quality care.
Gyfrinachedd: Privacy:	Privacy is very important within the Health Board and the impact on the individual's privacy should be considered when processing personal data.
Cydraddoldeb: Equality:	All personal data should be managed appropriately and in the same manner across the Health Board.



Information Governance Sub-committee



GIG
CYMRU
NHS
WALES

Bwrdd Iechyd Prifysgol
Hywel Dda
University Health Board

1. Introduction

The Information Governance Sub-Committee (IGSC) has been established under Board delegation with the Health Board approving terms of reference for the Business Planning & Performance Assurance Committee at its Board meeting on 26th January 2010. The terms of reference of the Information Governance Sub-Committee were subsequently approved at its meeting on 27th November 2010.

These terms of reference clearly detailed the Sub-Committee's purpose to provide assurance to the Business Planning & Performance Assurance Committee around the organisation's information governance framework, ensuring that there is an accurate reflection of Sub-Committee activity, work programmes, action plans, and policies and procedures to deliver against gaps in assurance.

Most recently the Information Governance Sub Committee (IGSC) terms of reference have been reviewed and updated at its meeting on 30th November 2022 to reflect the changes to the membership, the outcome of a review of the function of the IGSC, a change to the reporting groups to align with the updated information governance work plan and to include more specific detail on Cyber Security. The changes to the reporting body were also reflected to include **Sustainable Resources Committee (SRC)** instead of People Planning and Performance Assurance Committee (PPPAC).

In discharging this role, the Sub-Committee is required to oversee and monitor the information governance agenda for the Sustainable Resources Committee in respect of its provision of advice to the Board, and ensure the implementation of the information governance agenda against the following areas of responsibility:

- Meetings
- Governance
- Assurance
- Policies and Procedures
- IGSC's Groups

2. Meetings

Since 1st April 2022, Information Governance Sub-Committee meetings have been held on a bimonthly basis as follows:

- **1st April 2022** (quorate)
- **7th June 2022** (not quorate)
- **3rd August 2022** (not quorate)
- **24th October 2022** (quorate)
- **30th November 2022** (quorate)
- **31st January 2023** (not quorate)

During 2022 – 2023, the Sub-Committee met on six occasions and was quorate for three meetings. The meetings were held virtually through the Microsoft O365 Teams.

Anthony Tracey, Digital Director is acting as the Chair of the IGSC, and he is also the Deputy SIRO for the Hywel Dda University Health Board.

3. Governance

IGSC has been set up to:

- Promote and develop a robust information governance and security framework within the Health Board.
- Encourage a culture of information governance and information security across the Health Board.
- In conjunction with key Committees/sub-committees/groups develop appropriate systems, policies, procedures, work plans and action plans including (but not restricted to) the following areas:
 - Information and Cyber Security (including SIRO related issues)
 - Information Sharing Protocols
 - Contracts, partnership and third party and supplier agreements
 - Confidentiality and Data Protection
 - Freedom of Information
 - Subject Access Requests
 - Records Management
 - Information Quality Assurance
 - Risk Management and Incident Management
 - Data Protection Impact Assessments
 - Patient records

3.1 Information Governance (IG) Workplan

The main emphasis for the workplan has been:

- The Provision of IG training to staff (Raising the compliance to over 80% for the Health Board)
- IG Intranet Update
- To promote the Cyber Security within the Health Board, ensuring that all staff are targeted to undertake the on-line cyber security programme
- Provide IG service to Managed Practices
- Review of Procedures under the All-Wales Information Governance Policy, and All Wales Information Security Policy.
- Improve compliance with Welsh IG Toolkit
- Delivering Corporate Records Management Strategy and Policy
- Continue the implementation of UK GDPR within the Health Board
- Ensure the recommendations from Internal Audit/Welsh Audit Office reviews are implemented
- Improve the NIIAS monitoring
- Reviewing Privacy Notices available on the HDUHB's internet site
- Promoting WASPI and Information Sharing across Health Board / Setting up Information Sharing Register
- Setting up Virtual IAR with Annual Review and ongoing Risk Management (Through Teams Channels)
- The provision of specific IG Guidance (Staff Handbook) as well as generic good practice:
 - Live Virtual IG Training Sessions
 - IG Training Videos
 - Short IG Movies re: specific issues, e.g., Sharing Information with Police
- Supporting the Health Board in implementing new solutions across organisation through the use of Data Protection Impact Assessments (DPIAs)

3.2 Cyber Security

3.2.1 Cyber Security Team

A Cyber Security Operations Manager has been appointed to lead the Cyber Security Team. Further appointments have been made and by August 2023 the team was fully resourced.

3.2.2 Network and Information Systems Regulations (NIS-R)

In response to the Network and Information System regulations (NIS-R) the Cyber Security team has completed an assessment against the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). This assessed the Health Board against the four objectives of the CAF:

- **Managing Security Risk** – this ensures the Health Board has appropriate structures, policies, and processes to manage security risks.
- **Protecting Against Cyber Attack** – to assess measures are in place to protect our networks and systems from cyber-attack.
- **Detecting Cyber Security Events** – measures within the Health Board to detect cyber security events with an effective monitoring and reporting regime.
- **Minimising the Impact of Cyber Security Incidents** – ensure the Health Board can minimise the impact of any cyber incident and restore services in an appropriate timeframe.

A cyber security sub-group terms of reference and programme workplan have been completed to address the gaps identified in the CAF assessment and several workstreams will now be progressed under the auspices of this sub-group (prioritised into tranches of work):

Tranche 1

- Leadership and Communications
- Policies and Processes
- Training and Awareness
- Securing Endpoints
- Securing the Boundary
- Security Monitoring and Incident Response
- Supply Chain Management (Direct Connectivity)

Tranche 2

- Risk Management and Compliance
- Asset Management
- Vulnerability Management
- Securing the Servers

Tranche 3

- Securing Medical Equipment and Devices
- Cloud Security
- Business Continuity and Disaster Recovery

Work is progressing well with the cyber security programme, with significant progress made in items identified in all Tranches.

3.2.3 Vulnerability Management

The vulnerability management work stream has developed well, with the introduction of identifying and remediation vulnerabilities against our endpoint devices in addition to our infrastructure. Focus is on reducing the number of end-of-life software in the environment.

3.2.4 **Anti-Virus / Anti-Malware**

As part of the NHS Wales Office 365 Enterprise Agreement, we now have licensing available for Microsoft Windows Defender. This highly rated security platform is only one of six software products in the leader's magic quadrant which Gartner creates annually and so we can have assurance that it provides the appropriate security protections for Hywel Dda.

3.2.5 **Cyber Security Programme**

Following the good progress made, the cyber security programme will be looking at finalising tranche 1 tasks and moving onto tranche 2 to further improve cyber resilience within the health board.

3.2.6 **Phishing Campaigns**

Phishing is one of the easiest cyber-attack vectors. Staff awareness combined with technical controls is crucial to defend against phishing attacks. There is evidence of users clicking on malicious links within phishing emails and not reporting these actions. Following the purchase of a phishing exercise platform we are regularly running phishing campaigns which also makes a short training video available to anyone who clicked on our phishing exercise emails. We've recently deployed a report phishing button to all clients so that staff can easily report any phishing emails directly to the Cyber Security Team.


4. Assurance

- Ensure the Health Board is compliant with the Data Protection Legislation (the Data Protection Act 2018 and UK GDPR (General Data Protection Regulation) - together referred to as the Data Protection Legislation).
- Ensure quality and statutory compliance in relation to all information processed by the Health Board.
- Ensure that new projects, processes and the development of systems are compliant with statutory requirements in relation to information governance.
- Ensure that there is a process of Data Protection Impact Assessment in accordance with Information Commissioner's guidance.
- Ensure that information sharing and transfer with third party organisations are compliant with statutory requirements in relation to information governance.
- Ensure that the Health Board is following the Caldicott Principles when processing patient information.
- Caldicott Principles into Practice (C-PIP).
- Welsh Information Governance (IG) toolkit.
- Internal and External Audit reviews.
- Information Commissioners Officer (ICO) standards.
- Any other relevant National or Welsh requirements/assessments.

The IG Activity Report is presented at every IGSC meeting. The purpose of this report is to provide an overview to the Information Governance Sub Committee (IGSC) of the day-to-day work that has been undertaken by the IG Team. It also includes access requests made to the Access to Health


Records Team, and to Freedom of Information Requests Team, Corporate Office. The Report provides an overview of the activities of the IG Team in relation to the following areas:

4.1 Assurance – Advice

Advice		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Advice (P1 - Fair & Lawful Processing)	2	3	5	10	15	8	13	17	9	9	5	21
	Advice (P2 - Specified & Legitimate Purpose)	0	0	0	1	3	2	0	1	1	0	2	0
	Advice (P3 - Adequate, Relevant & Limited)	1	1	3	0	1	1	0	0	0	0	0	0
	Advice (P4 - Accuracy)	0	0	1	1	5	0	0	0	0	1	0	1
	Advice (P5 - Retention)	0	0	0	1	3	1	1	0	1	3	1	2
	Advice (P6 - Security)	16	14	23	13	25	13	36	20	20	24	22	22
	Advice (P7 - Accountability)	0	1	2	1	4	1	0	2	0	0	1	0
	Secure transfer of information (Email, Post and other means)	0	1	1	0	0	0	1	0	0	0	0	1
420		19	20	35	27	56	26	51	40	31	37	31	47
		Enquiries on Data Protection Framework											

The IG Team provides guidance on variety of topics to the Health Board's employees on a daily basis. Most enquiries are about lawfulness of processing personal data, e.g., providing Privacy Notices, retention schedules and information security. The aim is to make sure that IG guidance is clear and consistent for everyone working in the Health Board. We have supported many service areas who needed Privacy Statements for forms or leaflets.

4.2 Assurance – Information Sharing


Information Sharing		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Information Sharing	2	8	6	6	3	5	2	7	3	3	2	5
	WASPI Information Sharing Protocol (ISP)	8	1	2	0	0	1	0	2	0	3	3	0
	WASPI Data Disclosure Agreement (DDA)	1	0	0	0	0	0	0	0	0	0	0	0
	Caldicott Guardian Review	6	9	5	9	4	13	5	13	7	10	2	12
	Research Proposal (containing PII)	1	1	1	2	0	1	0	0	0	0	2	0
	Service Evaluation / Research (Internal)	0	0	0	0	0	0	3	0	0	1	0	1
	Service Evaluation / Research (External)	0	0	0	0	1	0	1	3	1	3	2	5
		18	19	14	17	7	20	7	22	10	16	9	17
176		Enquiries on Information Sharing											

The Caldicott Guardian's role is to ensure that procedures are in place to govern access to and the use of patient (client) identifiable information and, where appropriate, the transfer of that information to other organisations for a given purpose that is outside of direct patient care. This is to ensure that information is used legally, ethically, and appropriately, and that confidentiality is maintained. With this in mind, the Caldicott Guardian reviews and approves protocols or agreements which address the sharing of patient data between organisations, for official registers, external research projects etc., to which the Health Board is party and reviews and approves staff post graduate projects. The IG Team maintains a Caldicott Guardian Register of the above areas.

4.3 Assurance – Personal Data Breaches


The Health Board has adopted and implemented a robust procedure for managing IG incidents across the organisation that ensures incidents are reported in line with statutory requirements and

lessons are learnt to improve future practice. Where they meet the threshold, the Health Board reports to the Information Commissioner's Office (ICO) as detailed below.

Personal Data Breaches		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Personal Data Breach (Recorded Internally)	13	14	21	8	9	17	19	22	4	12	16	18
	Personal Data Breach (Reported to ICO)	1	0	1	0	1	0	0	0	1	0	0	1
	Personal Data Breach (Minor)	4	9	12	12	22	18	35	29	26	34	26	37
	Personal Data Breach (Near Miss)	3	5	4	6	9	14	6	4	15	21	7	16
	Personal Data Breach (Not Upheld)	3	4	3	4	1	1	0	1	2	2	1	2
	Personal Data Breach (Not Owned by HDUHB)	3	1	2	2	2	4	3	7	2	3	2	4
	Personal Data Breach (Withdrawn by patient)	0	0	0	0	0	1	0	0	0	0	0	0
	Incident (No IG Considerations)	72	168	133	122	134	124	78	88	102	94	106	69
		99	201	176	154	178	179	141	151	152	166	158	147
	Lost in Transit	0	0	0	0	0	0	1	0	0	0	0	0
	Lost or stolen hardware	0	0	0	0	0	0	0	0	0	0	2	0
	Lost or stolen paperwork	4	0	3	1	2	3	3	2	2	2	0	1
	Disclosed in Error	10	12	8	8	9	9	10	17	18	9	13	15
	Uploaded to website in error	0	0	0	0	0	0	1	0	0	0	0	0
	Non-secure Disposal – hardware	0	0	0	0	0	0	0	0	0	0	0	0
	Non-secure Disposal – paperwork	0	0	0	0	0	0	0	0	0	0	0	0
	Technical security failing (including hacking)	0	1	1	1	1	0	0	0	0	1	0	1
	Corruption or inability to recover electronic data	1	0	0	0	0	0	0	0	0	0	0	0
	Unauthorised access / disclosure	3	5	5	0	4	10	9	1	6	16	9	20
	Other	4	11	22	12	20	22	33	33	20	38	23	31
552		Personal Data Breaches											

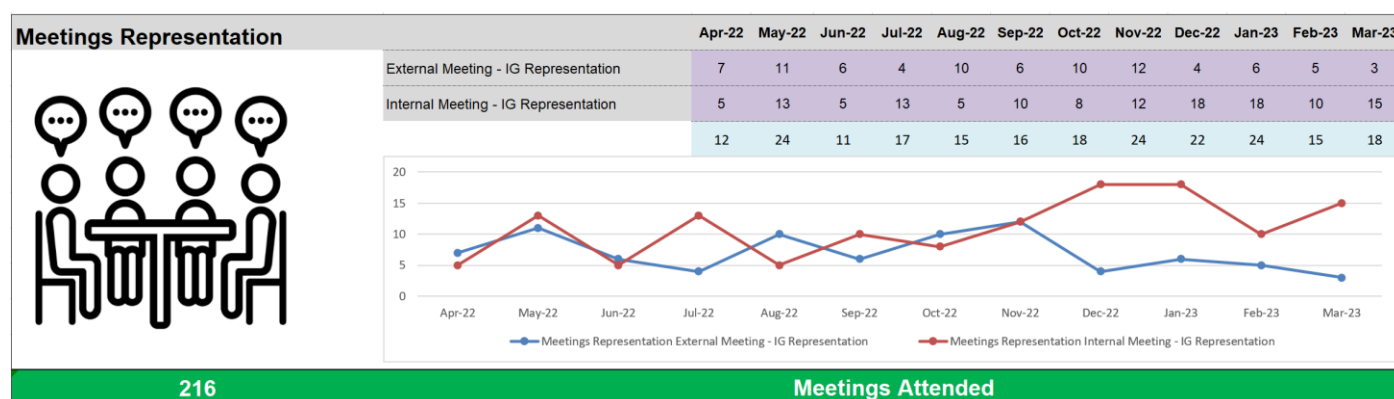
The Health Board has had contact with the Information Commissioner's Office (ICO) in relation to 5 incidents during the financial year 2022 -2023. This is a significant decrease on 2021 – 2022 when 14 incidents were reported to the ICO. All incidents reported via Datix and directly to the IG Team are risk assessed to determine if they meet the criteria to be reported to the Information Commissioner's Office as a personal data breach. The risk assessment criteria are in line with the guidance provided by the ICO and the risk scoring is entered into each incident report.

4.4 Assurance – Documents Review

Documents Reviews		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Memorandum of Understanding	0	2	1	2	1	1	0	0	0	1	0	1
	Contracts	0	0	0	2	1	2	0	1	3	3	0	0
	Data Processing Agreements (DPAs)	1	2	1	0	1	0	1	1	3	0	3	5
	Policy and Procedure Review	0	1	0	1	1	1	2	3	3	0	1	0
	Service Level Agreements (SLA)	2	0	2	1	1	0	2	2	0	3	5	1
		3	5	4	6	5	4	5	7	9	7	9	7
71		Documents reviewed											

The Information Governance Service reviews Contracts, Terms and Conditions, Memoranda of Understandings (MOUs), Data Processing Agreements (DPAs) and Service Level Agreements (SLAs). These documents govern how the Health Board shares personal data with other organisations. It is important so that both parties understand their responsibilities and liabilities, and this is clear within the agreements. IG Service also reviews internal policies and procedures and provide relevant guidance in line with the current Data Protection Legislation.

4.5 Assurance – IG Meetings Representation

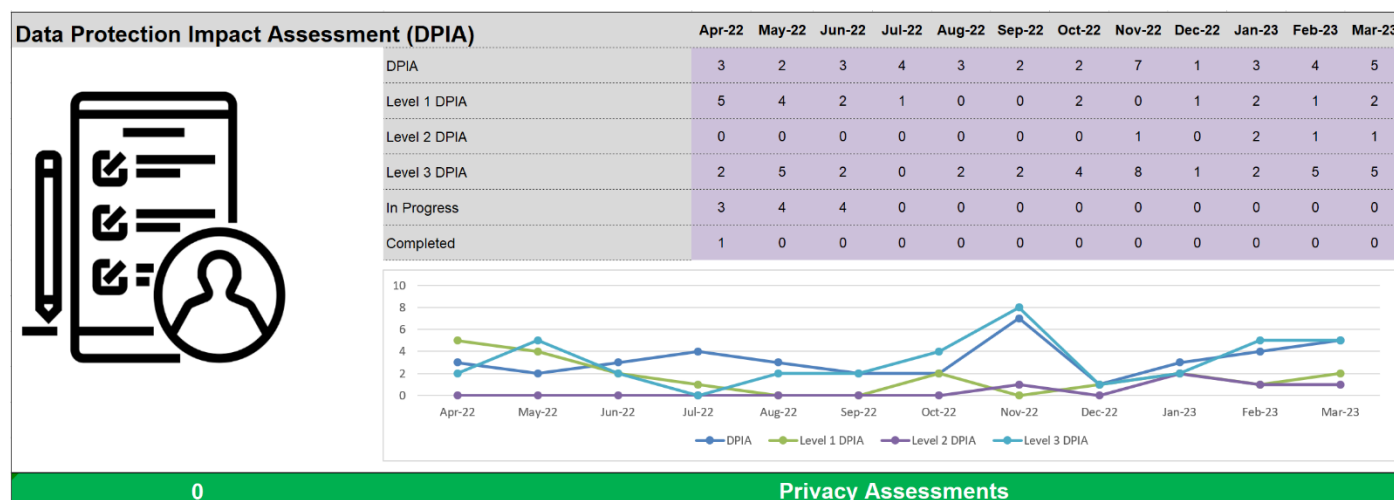


The IG Team represents HDUHB at internal and external meetings where they can be called upon for IG advice and guidance. For instance, HDUHB's Data Protection Officer regularly attends external Information Governance Management Advisory Group (IGMAG) meetings, where All Wales NHS Policies are developed, and national guidance is distributed. Detailed reports from the meetings were presented at every IGSC meeting in 2022-23.

Currently reports from the following external meetings are presented to IGSC:

- IGMAG – Information Governance Management Advisory Group
- HRMAG – Health Records Management Advisory Group
- OSSMB – Operational Security Service Management Board

4.6 Assurance – Data Protection Impact Assessments



Data Protection Impact Assessments (DPIAs) are a tool to assess the risks when completing any work involving personal data. Since the pandemic, there has been a dramatic increase in the need for DPIAs due to the new ways of working and the innovative solutions that the clinical teams require to provide patient care. It has also led to an increase in sharing patient data with other organisations, all of which require careful consideration of the risks to personal data. Each DPIA involves working with the project lead in HDUHB, plus the Digital/Cyber team for the completion of Cloud Assessments and the

external service/system providers where necessary. The DPIA process is complex and includes significant dialogue between all partners.

During 2022 – 2023 there have been changes in the way the IG Team record and process DPIAs with there now being 4 classifications. A DPIA Procedure reflecting these changes has been developed and is currently going through the Consultation and Approval process and will be implemented in 2023 – 2024.

4.7 Assurance – Individual Rights

Corporate Subject Access Requests:

Under the Data Protection legislation, data subjects have rights with regards to their personal information, the majority of work and enquiries to the IG Team continues to be around Workforce Subject Access Requests, the volume of requests continues to make the target timescales for release difficult to achieve. The IG team have provided technical support to the Access to Health Records Team over the last 12 months, which has impacted on our SAR figures and compliance rates.

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	March	Total
Received	3	7	0	2	13	2	5	6	4	7	0	1	51
Breached	0	1	0	0	1	0	0	5	1	0	0	1	12
Compliance	100%	86%	-	100%	92%	100%	100%	17%*	75%	100%	-	0%**	77%

*Please note that some initial information was disclosed within statutory timescales, and due to further releases of data past deadline the overall compliance for the month is low.

**there was a significant delay in forwarding this request to IG team for processing.

Health Records Subject Access Requests:

Over the 12 months we have again witnessed an increase in the number of subject access requests (SARs) received within the Health Records Service. In total the service received 3,734 requests, an increase of nearly 20% on last year's figures and a total of 3,265 requests were completed within the agreed timescale. The average number requests also increased on a monthly basis from 250 last year to 311, which again reflects the 20% increase identified above. This is an overall increase of 709 requests, which is a considerable increase and has made it extremely difficult for staff to attain the compliance targets. This is reflected in our compliance figures for the last 12 months, where we have seen a 5,51% decrease from last year's 92.91% compliance to this year's 87.40% compliance. Even by placing additional staff resource into this particular area within the department we are still unable to attain compliance levels that we are satisfied with, and this remains an ongoing challenge and concern. Working with the IG team we are currently reviewing the structure in readiness for a paper to be submitted to Information Governance Sub Committee (IGSC) in June 2023.

	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	March	Total
Received	365	333	295	255	294	275	314	316	267	350	320	350	3,734
Breached	47	49	44	23	43	44	61	32	35	34	23	34	469
Compliance	87%	85%	85%	91%	85%	84%	81%	90%	87%	90%	93%	90%	87%

Additionally, IG team has dealt with:

Data Subject Rights: Right to be informed – 5

Data Subject Rights: Rectification – 7

Data Subject Rights: Object – 1

4.8 Assurance – Freedom of Information (FOI)

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar*	Total
Received	36	37	41	49	61	51	50	51	32	52	51	55	566
Breached	3	3	6	8	7	11	16	24	20	17	7	8	130
Compliance	92%	97%	85%	84%	89%	79%	68%	53%	38%	67%	86%	85%	78%
Internal Review	0	0	2	0	1	1	0	1	1	0	0	1	7

**Please note – the figures provided within the table above are incomplete, as some FOIs received in March 2023 are not due for issue until the end of April 2023.*

Since pre-Covid (2019/20) when the total number of requests received was 470, there has been a rise in requests; 553 in 2021/22 with a further increase to 566 in 2022/23.

Compliance levels remained consistent during the first two quarters but were impacted negatively by staffing levels during the third quarter. During this period, Health Board services as a whole have been challenged to fulfil the number of FOI requests received.

In December 2022 when our compliance figure was at its lowest for some time, winter pressures added to this challenge, and this together with the staffing issues in the FOI team, resulted in a lower compliance figure.

Of significance this year, is the complexity and scope of the requests received that has affected the Health Board's ability to respond in a timely manner at times. Staffing levels have now recovered, with the team working hard during quarter four to review processes and trends to close historical requests and improve response rates further during the next financial year.

Themes throughout the year remain consistent with previous years, though the team has identified increased interest in workforce related requests and other commercial activities.


Seven internal reviews were received within the last financial year, which is a reduction from the 18 in 2021/22, and returning to typical figures from 2019/20. Two cases progressed to the Information Commissioner's Office (ICO) last year, one was a complaint submitted in October 2021 and was closed on provision of updated information; the second was closed by the ICO due to lack of further contact from the complainant.

4.9 Assurance – Information Asset Registers

The information asset register is a list of personal and non-personal information assets held by service areas within the Health Board. It is important that we know what information we hold in order for us to protect it. We aim to capture all records and systems that contain personal and special category data, flows of data out of the UK, location of data, the retention periods for the records we hold and the legal basis for processing this data.

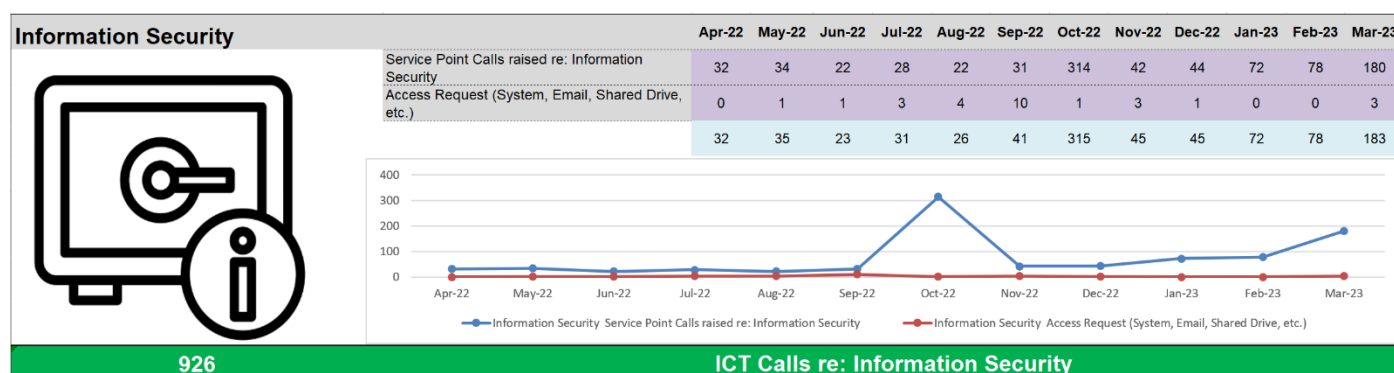
We have continued to work with services to build and review asset registers and pick up any associated work highlighted within the register for example a new application is in development and will need a Data Protection Impact Assessment completed and or a Data Sharing Agreement.

4.10 Assurance – Requests for Information (Third Party)

Requests for Information (Third Party)		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Schedule 2(2)(1) - Police Request	21	24	17	21	18	22	25	18	17	15	13	19
	Schedule 2(5)(2) - Required by Law	22	19	30	33	17	15	21	24	26	27	29	18
	Schedule 2(5)(3) - Legal Proceedings	0	0	0	0	0	0	0	0	0	0	0	0
	Police Request - With Patient Consent	14	23	13	11	17	16	20	23	16	30	30	28
	Schedule 3(2)(2) - Serious Harm Test	0	0	0	0	0	0	0	0	0	0	0	0
	Access to Deceased Patient Records	4	3	4	4	2	0	1	0	1	5	2	2
		61	69	64	69	54	53	67	65	60	77	74	67
780		Requests from Third Parties											

Requests for information can be made by Third Party organisations (Police, CPS, Solicitors, Social Workers, Department of Work and Pensions (DWP), Local Authorities, the Probation Service etc). In some cases, these requests come with the patient consent however, there are instances where patient consent is not required and an exemption in the Data Protection legislation may allow for the release. The IG Team will check if the release is necessary, relevant and proportionate for the purpose of the request, and keep all documentation as evidence if a disclosure is ever challenged.

4.11 Assurance – Information Security




The Hywel Dda Service Desk records all incidents, requests and queries related to Digital Services. The below graph shows the number of calls logged by the Service Desk to the 'Security Incidents' group, dealt with by the IT Security Manager. The calls relate to all aspects of Information Security including:

- Website access
- Email filtering
- Antivirus incidents
- Hardware encryption
- Secure transfer of Personal Data

There was a total of 926 calls logged over the year - a 137% increase compared to 2021-22 figures (a major factor to the large increase in calls recorded over the year was the introduction of staff 'phishing' email campaigns which were run in October 2022 and March 2023)

4.12 Training Compliance


Training Compliance		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Cyber Security E-Learning Compliance	0	0	2	2	8	0	17	5	7	4	5	2
	Cyber Ninjas E-Learning Compliance	1	0	0	0	0	0	2	22	1	1	0	0
	Information Governance E-Learning Compliance	77.48%	76.89%	76.65%	76.72%	77.09%	77.43%	77.21%	77.79%	78.06%	78.36%	78.61%	80.15%
	Level 1 Training	2	3	2	2	2	3	2	3	2	2	2	3
	Level 1 Staff Trained	22	39	41	18	17	45	31	53	42	37	41	83
	Level 2 Training	0	0	0	0	0	0	0	0	0	0	0	0
	Level 2 Staff Trained	0	0	0	0	0	0	0	0	0	0	0	0
	Training Enquiry	17	18	2	1	13	10	3	4	2	2	5	4
	Training (Informal)	1	0	0	0	1	0	1	0	0	1	0	1
		20	21	4	3	16	13	6	7	4	5	7	8
28		Training Sessions Delivered											
469		Employees Trained											

Information Governance training and guidance is designed to be clear, concise and engaging so we enable staff to understand and confidently discharge their data protection responsibilities. Data Protection Legislation requires individuals who process personal information to undertake regular data protection training. In NHS Wales refresher training in data protection is included in the Information Governance (IG) and is mandated for ALL staff to complete every two years as a minimum.

Information governance compliance within HDUHB steadily increased to 80.15% at the end of the year, the highest percentage achievement since October 2019. The IG Team aims to continue to improve this figure in 2023-24 by working with the sectors with the lowest compliance to encourage staff through the training programme.

4.13 Assurance – NIIAS Monitoring

The National Intelligent Integrated Audit Solution (NIIAS) audits staff access to patient records, it has now been fully implemented within the Health Board with procedures for managing any inappropriate access to records. There are regular staff communications, Newsletters, Information Governance Videos, Posters, leaflets, that have all been used to disseminate information to staff around the importance of confidentiality, appropriate access to patient records and ensuring information is shared in an appropriate way.

NIIAS Monitoring		Apr-22	May-22	Jun-22	Jul-22	Aug-22	Sep-22	Oct-22	Nov-22	Dec-22	Jan-23	Feb-23	Mar-23
	Own Records	11	12	5	5	5	14	10	6	7	10	5	4
	Family Records	8	9	1	2	10	16	9	7	10	5	5	9
	Person of Interest	1	2	1	0	1	1	0	0	2	0	0	1
	Choose Pharmacy												
	Own Records	0	1	2	3	0	3	2	2	0	0	0	0
	Family Records	0	1	3	2	0	1	4	1	1	0	2	1
		NIIAS Notifications											

HDUHB's IG Team regularly meets with the DHCW's National Monitoring System Development Manager, whose team is responsible for maintaining NIIAS, to discuss how the system supports HDUHB in monitoring Staff Accesses notifications. DHCW continues to integrate new systems with NIIAS.

All confirmed personal data breaches caused by inappropriate access to patient records are reported to the Data Protection Officer, Deputy Caldicott Guardian and Deputy SIRO, and where necessary

reported to the Information Commissioners office. Workforce Department is also notified and internal disciplinary investigations take place if required.

4.14 Assurance – IG Compliance

The IG Team visited different sites to carry out Audits. The audit is to check for any Information Governance and Information Security risks, and seeks assurance that Management Services are taking appropriate actions to ensure that data and assets are protected. The IG team are inspecting all areas within the Health Board that store large volumes of files which contain personal data, this is cross referenced with Services' Information Asset Registers, so we ensure the Health Board knows where all its information is stored and appropriate security is in place.

4.15 Compliance with the Data Protection Legislation

The General Data Protection Regulation (GDPR) came into force on 25th May 2018. It is now commonly referred to as the UK-GDPR, as a result of the UK leaving the EU. The UK GDPR and Data Protection Act 2018 both update and strengthen current data protection legislation with more emphasis on accountability and the individuals' information rights. In addition to the risk to the organisation of increased fines for non-compliance, because of the highly sensitive nature of the information we hold about individuals, the organisation has an ethical and moral duty to protect the information it is responsible for.

An invasion of a person's privacy whether by an accidental loss of their data, a security attack on our systems or by the dishonest actions of a staff member will all have a major impact upon our patients and the trust they put in the organisation to deliver safe and effective care. The IG Team produces a report which is submitted to every bi-monthly IGSC meeting on the progress in meeting key areas of the UK GDPR requirements to improve systems and processes to better safeguard personal data within the Health Board. The IG Team has complied with agreed work plan in regards to compliance with the legislation. Actions were identified within the UK GDPR Compliance Action Plan which incorporates the previous GDPR work plan, GDPR elements of the Stratia Cyber Assessment, Caldicott Principles in Practice (C-PIP) and Information Governance Risk Register. All actions have now been completed.

4.16 Assurance – Data Quality and Clinical Coding Update

Clinical Coding Update

Clinical coding is the process whereby information recorded in the patient notes or record which describes a patient's symptoms, diagnosis and treatment is translated into internationally and nationally recognised coded data and entered onto hospital information systems which can then be used for statistical and clinical purposes. Coding usually occurs after the patient has been discharged from hospital and must be completed to strict deadlines and rules in order for hospitals to understand their activity both locally, nationally and internationally. Hospital coded data on inpatient activity is important, being used for many purposes including NHS financial planning, performance management, epidemiology, clinical governance as well as monitoring of health provision and clinical audit.

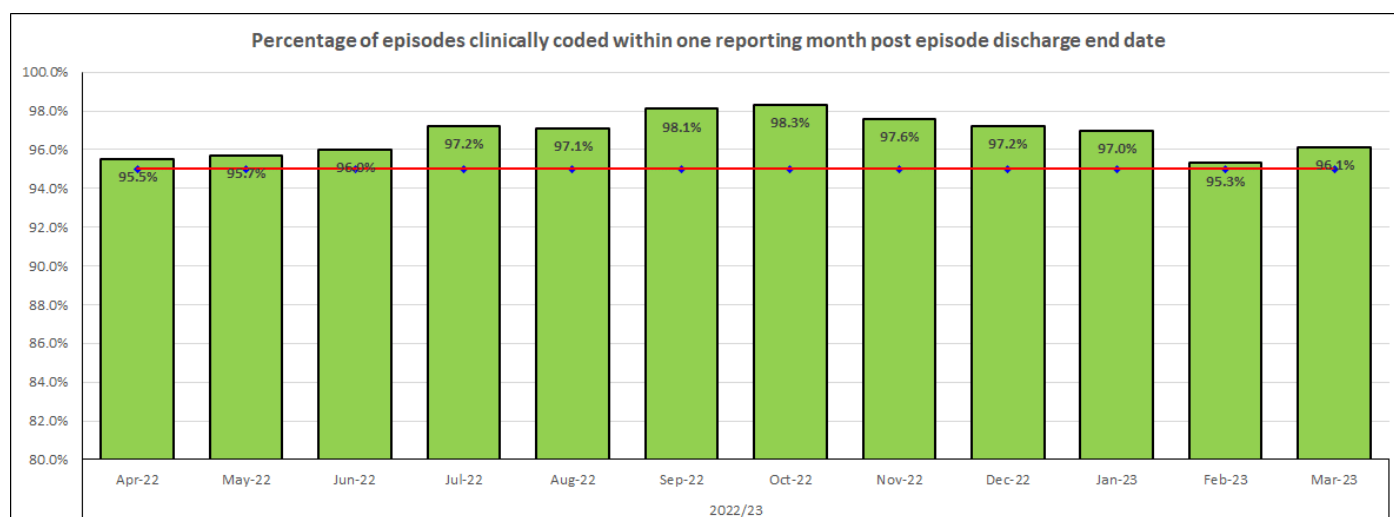
The Clinical Coding Department have two Welsh Government Targets in place which normally form part of the NHS Wales Delivery Framework:

- 1) Percentage of episodes clinically coded within one reporting month post episode discharge end date;

- 2) Percentage of clinical coding accuracy attained in the DHCW national clinical coding accuracy audit programme

Percentage of episodes clinically coded within one reporting month post episode discharge end date performance – 2022/23

- The Health Board has achieved the 95% monthly completeness every month this financial year, first 11 months (April to February)
- The Health Board are also on course to achieve the 98% year end completeness target for Welsh Costing Returns with provisional performance (April to February) at 98.4% with March activity still to be coded over the next month



Percentage of clinical coding accuracy attained in the DHCW national clinical coding accuracy audit programme performance – 2022/23

- The Health Board have achieved above the recommended accuracy for all 4 targets – primary diagnosis, secondary diagnosis, primary procedure and secondary procedure coding
- The number of episodes that were completely correct, with no errors in any position was 65.2%

Other work in the year

- A new internal audit program has been started with both supervisors and senior coders being involved
- A trial of the 3M Medical History Assurance (MHA) and Data Quality Analytics (DHA) tools has been undertaken for a 6 month period
- Initial discussions held around Robotic Process Automation (RPA). A process excellence workshop was held with representatives of Northampton General Hospital Trust to understand the workflow in the clinical coding team for Endoscopy coding
- Further work with 3M, which was focusing around the potential to clinically code some of the longest waiting patients in the Health Board Emergency Departments has been given formal approval and we are now in the process of awaiting a kick off date to get the initial work done. This will give the Clinical Coding team the tools to allow us to clinically code some of the A&E activity across the Health Board

Information Quality Assurance Update

It is important that the quality of data collected in the healthcare environment is of a high standard and be fit for purpose. High data quality leads to effective decision making which in turn results in better patient care, wellbeing and safety. It is essential in the production of management information to enable the efficient running of the Health Board and to maximise the utilisation of resources. Data

quality is the foundation of information and needs to be of a high standard and fit purpose in order to enable the efficient running of the Health Board and to maximise the utilisation of resources. The six dimensions of data quality are defined as Timeliness, Completeness, Accuracy, Consistency, Precision and Validity.

Work in the year:

- The Information Assurance Policy (policy number 250) has been reviewed and updated
- A priority matrix has been developed to allow the team to 'score' any of the issues that are in the issues log and ensure we can provide assurance as to the reasons for picking certain pieces of work to do next
- An escalation process has also been developed to ensure the IQA reports are being looked at and any actions/recommendations being followed through
- A scoring mechanism for data quality metrics has been developed to show areas that are doing well and those in need of improvement
- Deep dive audits completed on the following which include recommendations for improvement that are monitored by the team to ensure they have been actioned - Theatre completeness, Discharge Lounge activity comparison, Maternity activity recording, AMAU ward attender activity recording, Clinical Decisions Unit activity
- Regular data quality tasks/reports continue to be sent weekly/monthly to staff across the Health Board

4.17 Assurance – IG Risk Register

The Information Governance Sub-Committee Terms of Reference state that it will: "Provide assurance that risks relating to information governance are being effectively managed across the whole of the UHB's activities (including for hosted and contracted services, through shared services, partnerships, independent contractors and Joint Committees as appropriate)."

The 1 risk contained in the Information Governance Sub Committee Risk Register (Appendix 3) has been extracted from Datix Risk Module on the 17th January 2023 based on the following criteria:

- The Information Governance Sub Committee has been selected by the risk lead as the 'Assuring Committee' on Datix Risk Module
- Risks are above the proposed tolerance level that will be discussed and agreed by the Board on 27th September 2018
- Risks that have been approved at Directorate level on Datix
- Risks have not been escalated to the Corporate Risk Register.

The risk has been scored against the following 'impact' domains':

- Statutory duty and inspections

Risk Ref & Title	Date Risk Identified	Directorate	Risk Score Nov 22	Current Risk Score	Rationale for the current risk score	Target Risk Score
1369 - Corporate and Medical Records Storage	04/04/22	Finance: Digital: Information Governance	12	15 ↑	<p>IG are providing regular updates to the IGSC on Records Storage, a new internal storage facility will be ready shortly and this should alleviate some of the storage pressures across the Health Board.</p> <p>High Impact score due to potential prosecution from patients and the change in system currently in process. Impact score will only be reduced once digital records start to replace paper records - physical storage locations will not be needed as much. Digital storage overseen by Digital team and therefore more secure and within IG compliance criteria.</p>	6

The Sub-Committee continues to monitor not only the risks outlined above, but also the wider IG themed Risk Register. The monitoring of the Risk Register is a standing agenda item for consideration by the Sub-Committee.

4.19 NHS Wales IG Toolkit

NHS Wales IG Toolkit – Hywel Dda University Health Board

Common to other organisations in NHS Wales, the HB completes a self-assessment of our level of maturity and competency in management information risk and compliance with data protection and Caldicott principles in NHS Wales by completing the [NHS Wales IG Toolkit](#). This self-assessment is then review by the Information Governance Team in DHCW and scores are attributed against 7 core areas:

- Business Responsibilities
- Business Management
- Information Governance Incident Management
- Individual's Rights and Obligations
- Managing and Securing Records
- Cyber Security
- Technical Security, Physical Security and Organisational Measures

The aim of this breakdown enables the UHB to identify areas for improvement, and to support the prioritisation of our improvement efforts.

There are 3 levels of maturity assessed by the toolkit:

- Level 1: Policies and procedures are in place, staff awareness and responsibilities outlined
- Level 2: Appropriate training is provided, job descriptions updated for certain roles, policies and procedures are followed
- Level 3: Processes are in place to monitor, audit and report on operation and compliance

The 2022 – 2023 submission deadline has been moved to 30th June 2023 and the report is not yet available. The level of compliance is anticipated to be in line with previous years' submissions.

NHS Wales IG Toolkit Managed Practices

The Welsh Information Governance Toolkit is a self-assessment tool enabling organisations, including General Practices, to measure their level of compliance against national Information Governance standards and legislation. The IG Toolkit consists of simple to follow assessments, comprising of a range of rudimentary questions requiring tick box answers, one-line statements and the facility to upload or link to documents as evidence.

IG team supports HDUHB's Managed General Practices in their submissions. Currently there are 6 Managed Practices:

- Ash Grove Medical Centre
- Meddygfa'r Sarn
- Minafon Surgery (Meddygfa Minafon)
- Neyland Health Centre
- Solva Surgery
- Tenby Surgery

In the last financial year 2 practices (Solva Surgery and Neyland Health Centre) joined HDUHB, increasing the workload for IG service by 50%.

Using the information from the IG Toolkit submissions by the 6 Managed Practices, the IG Team have developed an Improvement and Action Plan for each Practice. These will be reviewed and updated annually. The Improvement Plans identified key areas across all the Practices which required action to ensure compliance and to improve their IG Toolkit Submission for 2022 – 2023. The IG Team are in the process of delivering sessions to address each of these areas, with the first being held on the 18th April 2023 providing guidance around completion of Information Asset Registers.

The aim of the IG Toolkit and Improvement Plans is to demonstrate that organisations can be trusted to maintain the confidentiality and security of both personal and business information. This will provide re-assurance to staff and patients that their information is processed securely and appropriately, and assure other organisations where sharing is made that appropriate IG arrangements are in place.

The 2022 – 2023 submission deadline for Managed Practices is 30th September 2023.

4.20 C-PIP (Caldicott Out-turn Report) 2021 - 2022

The Foundation Manual for Caldicott Guardians, Caldicott Leads and Information Governance Leads sets the requirements that organisations should endeavour to achieve. This manual provides all involved with protecting and using patient identifiable information with a knowledge framework containing what they need to know, why they need to do it and how to do it. It also includes an online Self-Assessment tool, (C-PIP Assessment) which enables organisations to quickly evaluate where they are with compliance and plan improvement.

The out-turn report provides a summary of the completed assessment and the improvement plan for 2022 – 2023. This improvement plan will run concurrently with the IG toolkit work plan but will draw on those elements where there is an equivalence within the Toolkit. While staff shortages have had an impact on the number of achieved improvements, the assessment shows an increased compliance with the previous year assessment with having 36 standards being fully compliant and, 5 being partially compliant.

Year of submission	Full Compliance	Partial Compliance	Non-Compliance	Percentage of compliance
2021 – 2022	36	5	0	93%
2020 – 2021	29	12	0	86%
2019 – 2020	29	12	0	86%
2018 – 2019	28	9	4	76%
2017 – 2018	26	9	6	-

It has been confirmed that 2021 –2022 was the last C-PIP Assessments for organisations in NHS Wales.

5. Policies and Procedures

Annual Review of Information Governance related written control documentation

The IGSC is the ‘owning’ Sub-Committee identified for 29 approved corporate written control documents. The overview below provides an outline of the current status of the relevant written control documentation including review dates and details of those approved in line with the UHB’s 190 – Written Control Document Policy. The overview also highlights where relevant written control documents are out of date or due for review. Due to work pressures faced as a result of COVID-19 the Digital Services Department were unable to review all policies to meet the deadlines indicated. Assurance was provided that the documents remained fit for purpose and an extension of 12 months to the review dates of all policies / procedures was requested. As detailed in the table below, most written control documents are now either back in date or have been reviewed and approved at IGSC but require approval from Sustainable Resources Committee prior to being uploaded to the website.

Policy or Procedure	Date of Review	Responsible Officer	Action Required / Current Position
<u>494 AW Email Use Policy</u>	17/12/2023	Head of Information Governance	No action required.
<u>495 AW Internet Use Policy</u>	27/04/2024	Head of Information Governance	No action required.
<u>836 AW Information Governance Policy</u>	27/04/2024	Head of Information Governance	No action required.
<u>837 AW Information Security Policy</u>	27/04/2024	Head of Information Governance	No action required.
<u>224 Information Classification Policy</u>	22/08/2020	Information Governance Manager	Under review with the sub-committee.
<u>275 Secure Transfer of Personal Information Policy</u>	28/02/2026	Information Governance Manager	Reviewed and approved by IGSC 31/01/2023 and SRC on the 28/02/2023.
<u>172 Confidentiality Policy</u>	26/06/2021	Information Governance Manager	Reviewed and approved by IGSC 13/04/2023. To be presented to SRC on 27/06/2023.
<u>238 Information Governance Framework</u>	26/06/2021	Information Governance Manager	Reviewed and approved at IGSC 13/04/2023. To be presented to SRC on 27/06/2023.
<u>279 Third Party Supplier Policy</u>	26/06/2021	Information Governance Manager	Under review with the sub-committee.
<u>Unauthorised Access (previously NIASS) Procedure</u>	New	Information Governance Manager	Reviewed and approved at IGSC 24/10/2023.
<u>1088 Information Rights (including Subject Access Requests) Procedure</u>	New	Information Governance Manager	Reviewed and approved at IGSC 24/10/2023.
<u>1160 Data Protection Impact Assessment Procedure</u>	New	Information Governance Manager	Reviewed and approved by IGSC 13/04/2023.
<u>347 Corporate Records Management Policy</u> (Replaces previous Corporate Records Management Policy and Corporate Records Management Strategy)	25/4/2025	Head of Information Governance	No action required.
<u>193 Retention and Destruction of Records Policy</u>	28/02/2026	Health Records Manager	No action required.
<u>249 Access to Health Records</u>	21/08/2023	Health Records Manager	No action required.
<u>191 Health Records Management Policy</u>	25/02/2022	Health Records Manager	To be reviewed and approved at IGSC on 08/06/2023.
<u>192 Health Records Management Strategy</u>	25/02/2022	Health Records Manager	To be reviewed and approved at IGSC on 08/06/2023.
<u>173 Freedom of Information and Environmental Information Policy</u>	21/12/2024	Senior Corporate Information Officer	No action required.
<u>174 Reuse of Public Sector Policy</u>	28/02/2026	Senior Corporate Information Officer	No action required.

<u>465 AW Social Media Policy</u>	31/03/2024	Deputy Digital Director	No action required.
<u>250 Information Quality Assurance Policy</u>	20/12/2025	Deputy Digital Director / Digital Director	No action required.
<u>281 Mobile Working Policy</u>	27/02/2021	Deputy Digital Director	Reviewed and approved by IGSC 24/10/2023.
<u>282 Network Security Policy</u>	28/02/2026	Deputy Digital Director	No action required.
<u>301 User Account Management Policy</u>	26/06/2021	Deputy Digital Director	Reviewed and approved by IGSC 24/10/2023.
<u>319 Disposal of Digital Assets Policy</u>	15/03/2026	Deputy Digital Director	No action required.
<u>320 Acceptable Use of Information and Communication Technology Policy</u>	25/04/2026	Deputy Digital Director	No action required.
<u>240 Digital Procurement and Request Procedure</u>	25/05/2026	Deputy Digital Director	No action required.
<u>422 Consumer Device Policy</u>	28/02/2026	Deputy Digital Director	No action required.

6. INFORMATION GOVERNANCE SUB-COMMITTEE GROUPS

The Information Governance Sub-Committee Annual Report 2022-2023 is intended to outline how the Sub-Committee and its Groups have complied with the duties delegated by the SRC through the terms of reference set, and also to identify key actions that have been taken to address issues within the Sub-Committee's remit.

The Groups reporting to the Information Governance Sub-Committee during 2022– 2023 were as follows:

6.1 Information Asset Owners (IAO) Group

The Group has been established to:

- Agree and oversee the UK GDPR / Data Protection Act 2018 compliance project work plan.
- Develop and oversee a programme of information asset audits and asset mapping.
- Ensure that Information Asset Owners are in place across the organisation and are fully briefed in relation to their role.
- Agree a process for identifying, recording, and mitigating any information risk identified through the information asset audit programme.
- Develop and agree a communication and engagement programme for staff around the UK GDPR and information governance, including information security.
- Progress the implementation of Data Protection Impact Assessments (DPIAs) across the Health Board.

The terms of reference for the group were updated and approved at the IGSC in April 2022, the main changes were due to the Health Board's Committee changes. Business Planning & Performance

Assurance Committee changed into People Planning and Performance Assurance Committee (PPAC), and now changed to Sustainable Resources Committee (SRC).

The group met 6 times during the financial year to oversee the work progress made by Information Governance which included assuring 6 Information Asset Registers.

6.2 The Health Records Group

A Health Records Group has been established and reported to the Information Governance Sub Committee (IGSC) as a Sub-Committee from April 2018 and terms of reference and key activities for the group had been approved by the IGSC. Unfortunately, the Health Records Group has been unable to meet over the last 12 months, initially following the challenges experienced in identifying a permanent chair, but mainly due to the fact that the Health Board has made significant strides in its transition towards a digital record. In line with the Health Boards digital strategy, considerable progress has been made in terms of the procurement of an electronic document records management system (EDRMS) and records starting to be ingested digitally, as serviced by scanning providers. This has been a significant undertaking and required cohesive working arrangements and project management leadership across the Informatics and Health Records services. Following discussions with senior Executive leads, it was agreed that this project had to take precedence over the last 12 months and was seen as a “kick start” towards our digital transition. As an interim measure the Health Board implemented a digital records programme group, but this was of an informal nature and simply recorded ongoing actions, implementation timescale and any issues or risks to project delivery. The project management team have now commenced work on a Digital Steering Group that will not only encompass elements and requirements of the previous Health Records Group, but the overall digital requirements of the Health Board. The proposed alteration in the historical meeting forums and meeting arrangements is viewed as a key driver for the successful implementation and delivery on a single digital patient record across the Health Board.

6.3 Caldicott Guardian Group

The Caldicott Guardian Group has been established as a subgroup of the Information Governance Sub-Committee and constituted from 25th August 2020.

The purpose of the Caldicott Group is to provide assurance to the Information Governance Sub-Committee around Caldicott Guardian functions. The Group will:

- Support Caldicott Guardian in understanding their responsibilities and those of the Health Board.
- Share good Caldicott/confidentiality and information sharing practice between the Health Board and partners.
- Supporting Caldicott Guardian in raising the profile of Caldicott / confidentiality issues and appropriate information sharing across the Health Board and partners.
- Notify the Caldicott Guardian of incidents which result in a negative clinical impact or reduced level of care to patients. (As agreed at Caldicott Guardian Group on the 21st September 2022 and approved at IGSC on the

Following the Covid-19 Pandemic, the group meetings recommenced during 2021 – 2022 with 3 meetings held in this time. During 2022 – 2023, there were 5 meetings which were held on 11th July 2022, 21st September 2022, 23rd November 2022, 18th January 2023 and the 3rd May 2023.

The Terms of Reference were last reviewed in September 2022 and will be reviewed on an annual basis.

6.4 Information Governance Incident Group

The group has been established to:

- Receive updates on new Information Governance Incidents reported including the presentation of any Information Governance Incident Investigation Reports.
- Receive detailed updates on ongoing incidents/breachers reported to the ICO.
- Agree recommendations and actions in relation to any new Incidents reported.
- Receive updates on the Information Security Incident Action Plan.
- Reach agreement to close any completed Information Security Incidents.
- Agree any further recommendations/work required around managing Information Security Incidents within the Health Board.
- Develop an Information Security Incident reporting procedure

Following the Covid-19 Pandemic, the group meetings recommenced during 2021 – 2022, and the group now meets prior to the IGSC, as IGSC In-Committee. During 2022 – 2023 there were 6 meetings held which were on the 1st April 2022, 7th June 2022, 3rd August 2022, 24th October 2022, 30th November 2022 and the 31st January 2023. The In-committee is subject to the same Terms of Reference as IGSC.