

# Information Governance – Contract Management

## Internal Audit Report

May 2023

Public Health Wales NHS Trust



Partneriaeth  
Cydwasaethau  
Gwasanaethau Archwilio a Sicrwydd  
Shared Services  
Partnership  
Audit and Assurance Services



Iechyd Cyhoeddus  
Cymru  
Public Health  
Wales



## Contents

Executive Summary .....	3
1. Introduction.....	5
2. Detailed Audit Findings.....	5
Appendix A: Management Action Plan.....	10
Appendix B: Assurance opinion and action plan risk rating .....	15

Review reference:	PHW-2223-07
Report status:	Final
Fieldwork commencement:	12 October 2022
Fieldwork completion:	1 December 2022
Debrief meeting:	19 December 2022
Draft report issued:	20 December 2022
Management response received:	04 May 2023
Final report issued:	05 May 2023
Auditors:	Kevin Bridgman, IT Audit Manager Martyn Lewis IT Audit Manager
Executive sign-off:	Rhiannon Beaumont-Wood, Executive Director Quality, Nursing & AHPs
Distribution:	John Lawson, Head of Information Governance
Committee:	Audit & Corporate Governance Committee



Audit and Assurance Services conform with all Public Sector Internal Audit Standards as validated through the external quality assessment undertaken by the Institute of Internal Auditors.

### Acknowledgement

NHS Wales Audit and Assurance Services would like to acknowledge the time and co-operation given by management and staff during the course of this review.

### Disclaimer notice - please note

This audit report has been prepared for internal use only. Audit and Assurance Services reports are prepared, in accordance with the agreed audit brief, and the Audit Charter as approved by the Audit and Corporate Governance Committee.

Audit reports are prepared by the staff of the NHS Wales Audit and Assurance Services, and addressed to Independent Members or officers including those designated as Accountable Officer. They are prepared for the sole use of Public Health Wales NHS Trust no responsibility is taken by the Audit and Assurance Services Internal Auditors to any director or officer in their individual capacity, or to any third party.

## Executive Summary

### Purpose

To review of the arrangements in place for the management of Information Governance (IG) requirements within the contracts management process.

### Overview

The purchasing and contracting processes ensure that Information Governance requirements are stated, and suppliers have to provide evidence of this to win contracts. There is a register of information assets, and data protection impact assessments and data processing agreements are in place.

We note that there is no overall register of suppliers within PHW, and the requirement to check temporary staff IG training is not formalised. In addition, there is no process for the annual review of IG for contracts.

The matters requiring management attention include:

- Developing a holistic register of third party contracts in order to identify third parties with IG requirements.
- Formally requiring departments to check IG training for temporary staff, and offering PHW IG training if necessary.
- Establishing contract management procedure and ensuring an annual check for suppliers to re-confirm IG compliance.

Other recommendations / advisory points are within the detail of the report.

Further matters arising concerning the areas for refinement and further development are noted in Appendix A.

## Report Opinion



Some matters require management attention in control design or compliance.

**Low to moderate impact** on residual risk exposure until resolved

## Assurance summary<sup>1</sup>

Objectives	Assurance
1 Data protection and IG contracts and agreements	Reasonable
2 Contracts and agreements are documented	Reasonable
3 A review process is in place	Limited

<sup>1</sup>The objectives and associated assurance ratings are not necessarily given equal weighting when formulating the overall audit opinion.

## Key Matters Arising

	Objective	Control Design or Operation	Recommendation Priority
1	Contract Management	Design	High
2	No centralised record of third party providers	Operational	Medium

---

3	IG Training	2	Design	Medium
---	-------------	---	--------	--------

---

## 1. Introduction

- 1.1 In line with the 2022/23 Internal Audit Plan for Public Health Wales NHS Trust ('PHW' or 'the Trust') we have reviewed the arrangements in place for the management of Information Governance (IG) requirements within the contracts management process.
- 1.2 The IG Toolkit for Health Boards and Trusts includes a section with requirements for the management of contracts, in addition under UK GDPR, data controllers need to ensure appropriate contracts are in place when engaging the services of data processors. The specific requirements around contracts and liabilities are set out in Article 28 of the UK GDPR.
- 1.3 Data processors are generally third-party organisations – that is, they are external organisations that work for or on behalf of data controllers. However, GDPR defines 'third party' as 'a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data'.
- 1.4 As part of our audit work, we sampled seven contracts for examination, with a targeted focus on those with an underlying risk to IG.
- 1.5 The risk considered as part of this audit relates to the non-compliance with key information governance legislation.

## 2. Detailed Audit Findings

### **Objective 1: Data protection and IG contracts and agreements are in place with suppliers, contractors, third parties and staff, who have access to / process personal data, which include data protection /IG requirements.**

- 2.1 There is a process for requiring that data protection impact assessments (DPIA) are undertaken for activities involving the use of data and following that, that data processor agreements (DPA) are put in place with the parties using the data. Our testing and review of DPIA documents confirmed that this process ensures that Caldicott Guardianship is in place within the Trust. This ensures that personal confidential data is managed, stored, and transmitted securely, whether in electronic or paper form, and that personal confidential data is only shared for lawful and appropriate purposes.
- 2.2 Any third party processing PHW data, or accessing a system for maintenance purposes, needs a data processing contract or agreement. This requirement is set out within the DPIA procedure.
- 2.3 Payments for goods and services are made via the financial system, with the purchasing module used to request orders for payments. For orders over £25,000 a formal contract for supply is established, and for those less than £25,000 a quote process is used.
- 2.4 For contracts over £25,000, clauses regarding Information Governance (IG) are incorporated into the contract tender document and form part of the awarded

contract. This process is overseen by the NHS Wales Shared Services Partnership (NWSSP) Procurement department and as such a list of third parties engaged with the Trust is collated. Our testing confirmed that tender requests / contracts over £25,000 have an IG section in the tender and no contract is awarded unless the suppliers agrees to the IG and data protection impact assessments (DPIA) clause within the contract terms.

- 2.5 For orders under £25,000, the requester within PHW relies on the purchasing system which states *'This order is subject to the NHS Standard General Conditions of contract (a copy of which may be obtained on application to the Ordering Authority)'*. The clause is a 'catch-all' and offers the supplier an opportunity to request a full copy of the terms and condition which covers IG awareness, although we note that this itself would not be sufficient to comply with GDPR for contracts for processing data. We note that the requester (the Trust or NWSSP) does not obtain confirmation from the supplier that IG compliance is in force.
- 2.6 We note that there is no PHW procedure or guidance for requesting contracts or services that set out the expected requirements for checks and notifications for requesting departments. This leads to a risk that contracts (in particular for under £25,000) may be established without a GDPR compliant contract being in place in the event that the requesting department has not notified IG or completed a DPIA.

### **Matter Arising 1**

#### **Conclusion:**

- 2.7 There is a process for undertaking DPIAs and ensuring that data processing agreements are in place for contracts which involve third party processors. IG is incorporated in relevant contracts with IG being included within the contracting documentation, and as a clause within the purchasing system. We note that the lack of formal PHW guidance leads to a risk that contracts may be established without full IG involvement. Accordingly, we have provided reasonable assurance over this objective.

### **Objective 2: Contracts and agreements are documented to allow easier assessment of current contracts/agreements already in place and due diligence checks are carried out on potential suppliers, contractors, data processors and third parties.**

- 2.8 The IG department holds some information on third parties which is captured on the Information Asset Register (IAR). However, the IAR may not be fully up to date, with the IG department being reliant on information provided to them. There is inconsistency between the fields of information recorded in the DPIA log and the information recorded in the IAR which make cross referencing difficult, and no company information is recorded in either.
- 2.9 There is a lack of clarity within the Trust over the contracts and agreements in place with third party providers, with no department in PHW has a record of all third party suppliers. We note that NWSSP has a log of awarded contracts over £25,000, and uses a register of requests for quote (RFQ) for those between £5000-£25,000, although this is a high-level register. Our fieldwork identified that the

Trust's IG department were aware of the over £25,000 register but not aware of the register of requests for quote and therefore do not have a list of live contracts under £25,000. **Matter Arising 2**

- 2.10 For contracts over £25k, the tendering process requires that contractors respond regarding their IG processes and provide evidence of IG. This process is led by Shared Services Procurement, who hold the documentation. Without this assurance, Shared Services are unable to award contracts. Our testing confirmed that appropriate IG evidence was provided by suppliers. For example, one supplier provided a company handbook outlining the responsibility of the employed staff with regards to IG compliance.
- 2.11 Contracts and orders with a value under £25,000 are requested by the local department within PHW, who rely on a standard clause which is incorporated in the Oracle purchasing system. The requester does not receive confirmation from the supplier that IG process are on place, which, as noted previously would not be sufficient to comply with GDPR for contracts for processing data.
- 2.12 As noted above, there is no PHW procedure relating to contracting. As such there is nothing that requires requesting departments to notify the IG department of potential contracts, and as such the department may not request and review the appropriate IG related documentation from suppliers. **Matter Arising 1**
- 2.13 We note that not all contracts under £25,000 require IG compliance to be checked as not all contracts were related to employing third party staff or need access to Trust data. Contracts under £25,000 are subject to the standard clauses in the Oracle purchasing system which contains a clause stating, *'This order is subject to the NHS Standard General Conditions of contract (a copy of which may be obtained on application to the Ordering Authority)'*, which covers IG requirements. Generally, only contacts where temporary / agency staff are employed or third parties need to access data for processing or systems for maintenance purposes need IG to be considered separately.
- 2.14 The Trust use temporary staff provided via contracts. Our testing showed that there was limited evidence that third party agency staff working at the Trust had received IG awareness training, with PHW training records not separately identifying temporary staff. As we note in the example above, a supplier may provide a handbook which outlines IG compliance, but there is no evidence staff have read the handbook. There is an assumption that the supplier follows good IG practices.
- 2.15 We note that there was variation across PHW over departmental checking of the IG training status of third party staff working at the Trust. Some departments ask the staff if they have had IG awareness training, but this is not always the case, so there is a risk that temporary staff may not be aware of their IG responsibilities. **Matter Arising 3**
- 2.16 Furthermore, there was variation within PHW regarding the level of departmental provision of IG training for third party staff. Some departments offer induction to

temporary / agency staff, which includes IG, but this is not always the case, with reliance placed on the supplier having provided this. **Matter Arising 3**

- 2.17 We note that IG related documentation and training is available by the Trust's IG department, and has been provided to temporary staff when requested. However, this is not mandated for temporary staff. IG training compliance figures collated by the IG department do not include temporary staff, as the department has no knowledge of where temporary staff are used within the organisation. **Matter Arising 4**

**Conclusion:**

- 2.18 There are contract agreement documents in place and suppliers are made aware of the Trust's policy in respect to IG, through either the tender process or via the purchasing process. The contracting process run by NWSSP ensures that suppliers confirm, with evidence, that their IG process comply with GDPR / NHS requirements, however we note that the lack of procedures mean that these documents may not be fully evaluated within PHW. We also note there is no record of contracts within PHW that could be used to identify those that require IG compliance. In addition, there is no formal process to ensure that departments confirm that temporary staff have had IG training. Accordingly, we have provided reasonable assurance over this objective, although we note that significant reliance is being placed on the processes within NWSSP.

**Objective 3: A review process is in place to ensure that contracts and agreements are monitored and regularly reviewed to ensure that IG controls are being adhered to, to resolve problems or unforeseen events, and changes are communicated appropriately.**

- 2.19 Once the contract is awarded no further checks are conducted by Shared Services to ensure IG compliance has been conveyed to staff working for the supplier, or potential temporary / agency staff being provided to PHW. Reliance is placed on the supplier continuing to comply with the IG processes set out within the original tender document.
- 2.20 As previously noted, that there is no Trust procedure for contracting, or for managing ongoing contracts that sets out the requirements for the Trust. As such, there is nothing that requires annual / ongoing checks of IG compliance.
- 2.21 When a contract is either amended, extended or up for renewal the IG clause is re-iterated in the contract. However, until such time there is no scheduled review process for existing contracts which would require suppliers to confirm that the IG processes are still in place.
- 2.22 We did not see evidence of existing contracts being reviewed for IG compliance, or long standing contracts being reviewed on a regular basis. Contracts awarded in 2017 had not been reviewed to date. **Matter Arising 1**
- 2.23 We note that there is a process for reporting IG incidents, and following this, to investigate and identify actions for improvement. The outcomes from investigations are reported at Audit Committee.



Conclusion:

2.24 When contracts are renewed IG is considered, however there is no process in place for regular review of the IG compliance status of contractors and third party providers. Accordingly, we have provided limited assurance over this objective.

## Appendix A: Management Action Plan

Matter Arising 1: Contract management (Design)	Impact
<p>There is no procedure within PHW that sets out the requirements and processes for requesting contracts. This means that there are gaps in the processes:</p> <ul style="list-style-type: none"> <li>- Staff requesting items may not inform IG, or undertake a DPIA which could result in a lack of DPA for processing, leading to a lack of a GDPR compliant contract.</li> <li>- Staff requesting contracts may not review, assess properly the tender response and documentation relating to IG.</li> <li>- there is no scheduled review process for existing contracts which would request suppliers to confirm that their IG processes are still in place. We did not see evidence of this review, and it was evident that long standing contracts were not reviewed on a regular basis. We note contracts awarded in 2017 had not been reviewed to date.</li> </ul>	<p>Potential risk of:</p> <ul style="list-style-type: none"> <li>• Non-compliance with key information governance legislation</li> </ul>
Recommendations	Priority
<p>1.1 A procedure for contracting and managing ongoing contracts for PHW should be developed. This should include:</p> <ul style="list-style-type: none"> <li>- Notification of the intent to IG.</li> <li>- Review of IG related tender documentation</li> <li>- An annual review process should be established that requests all suppliers to confirm adherence to IG requirements.</li> </ul>	<p><b>High</b></p>

Agreed Management Action	Target Date	Responsible Officer
1.1 For contracts with a value of over £25k there is an organisation wide process in place which is managed by Shared Services Procurement There is currently no organisation wide process or procedure for contracts with a value of under £25k and each Directorate manages its own contracts. Public Health Wales will review current arrangements and develop an organisational procedure for the management of contracts under £25k and will also consider the option of placing such contracts under the management of Shared Services Procurement. Procedures will include the appropriate information governance requirements.	September 2023	Angela Williams/ Stuart Silcox

<b>Matter Arising 2: Record of third party providers (Operation)</b>		<b>Impact</b>	
<p>There is a lack of clarity within PHW over the contracts and agreements in place with third party providers. While we note that Shared Services maintain a log of contracts over £25,000 and have a requests for quote (RFQ) register for contracts between £5,000 and £25,000, there is no central record of contracts and agreements within the Trust, and no record within the IG department apart from the IAR, which is not fully up to date.</p>		<p>Potential risk of:</p> <ul style="list-style-type: none"> <li>Non-compliance with key information governance legislation</li> </ul>	
<b>Recommendations</b>		<b>Priority</b>	
2.1	The contract and RFQ record should be shared with the IG department and a record of third party providers maintained within PHW.	<b>Medium</b>	
<b>Agreed Management Action</b>		<b>Target Date</b>	<b>Responsible Officer</b>
2.1	As per the Management Action at 1.1, Public Health Wales will review its contract management process and procedures to include the provision of an appropriate contracts register which will be maintained either by Shared Services Procurement or Public Health Wales, dependant upon the outcome of the review. Again, the register will be shared with information governance colleagues along with the RFQ records.	Sept 2023	A Williams/ Stuart Silcox





<b>Matter Arising 3: IG training (Design)</b>		<b>Impact</b>	
There was variation across the Trust over the departmental checking of the IG training status of third party staff, and the provision of IG induction and training to these staff.		Potential risk of: <ul style="list-style-type: none"> <li>• Non-compliance with key information governance legislation</li> </ul>	
<b>Recommendations</b>		<b>Priority</b>	
3.1	Departments within the Trust should be informed that when third party staff are used, their IG training status should be established, and IG training provided if necessary.	<b>Medium</b>	
<b>Agreed Management Action</b>		<b>Target Date</b>	<b>Responsible Officer</b>
3.1	A Procedure will be developed to cover the appointment and on-boarding of agency and other third party staff.	Sept 2023	Neil Lewis / Stuart Silcox

<b>Matter Arising 4: IG training compliance (Operation)</b>		<b>Impact</b>	
The IG training compliance figures provided by the IG department do not include temporary staff, as the department has no knowledge of where temporary staff are used within the organisation.		Potential risk of: <ul style="list-style-type: none"> <li>Temporary staff are not aware of key information governance requirements.</li> </ul>	
<b>Recommendations</b>		<b>Priority</b>	
4.1	The IG department should consider including third party staff within the compliance figures.	<b>Low</b>	
<b>Agreed Management Action</b>		<b>Target Date</b>	<b>Responsible Officer</b>
4.1	IG Training compliance figures provided to the IG Service will be updated to include training for third party staff, and these will then be incorporated into the IG Performance Report	Sept 2023	Neil Lewis / Stuart Silcox

## Appendix B: Assurance opinion and action plan risk rating

### Audit Assurance Ratings

We define the following levels of assurance that governance, risk management and internal control within the area under review are suitable designed and applied effectively:

	<b>Substantial assurance</b>	Few matters require attention and are compliance or advisory in nature. <b>Low impact</b> on residual risk exposure.
	<b>Reasonable assurance</b>	Some matters require management attention in control design or compliance. <b>Low to moderate impact</b> on residual risk exposure until resolved.
	<b>Limited assurance</b>	More significant matters require management attention. <b>Moderate impact</b> on residual risk exposure until resolved.
	<b>No assurance</b>	Action is required to address the whole control framework in this area. <b>High impact</b> on residual risk exposure until resolved.
	<b>Assurance not applicable</b>	Given to reviews and support provided to management which form part of the internal audit plan, to which the assurance definitions are not appropriate. These reviews are still relevant to the evidence base upon which the overall opinion is formed.

### Prioritisation of Recommendations

We categorise our recommendations according to their level of priority as follows:

Priority level	Explanation	Management action
High	Poor system design OR widespread non-compliance. Significant risk to achievement of a system objective OR evidence present of material loss, error or misstatement.	Immediate*
Medium	Minor weakness in system design OR limited non-compliance. Some risk to achievement of a system objective.	Within one month*
Low	Potential to enhance system design to improve efficiency or effectiveness of controls. Generally issues of good practice for management consideration.	Within three months*

\* Unless a more appropriate timescale is identified/agreed at the assignment.



GIG  
CYMRU  
NHS  
WALES

Partneriaeth  
Cydwasaethau  
Gwasanaethau Archwilio a Sicrwydd  
Shared Services  
Partnership  
Audit and Assurance Services

NHS Wales Shared Services Partnership  
4-5 Charnwood Court  
Heol Billingsley  
Parc Nantgarw  
Cardiff  
CF15 7QZ

Website: [Audit & Assurance Services - NHS Wales Shared Services Partnership](#)