

Stephen Brown (Chief Officer)

Orkney Health and Care

01856873535 extension: 2601

OHACfeedback@orkney.gov.uk



Agenda Item: 9.

Integration Joint Board – Audit Committee.

Date of Meeting: 16 March 2022.

Subject: Internal Audit – Information Governance and Data Sharing.

1. Purpose

1.1. To present the Information Governance and Data Sharing Audit Report for members' scrutiny.

2. Recommendations

The Integration Joint Board – Audit Committee is invited to:

2.1. Scrutinise and seek assurance on the Information Governance and Data Sharing Audit Report, attached as Appendix 1 to this report.

3. Background

3.1. The Integration Joint Board is a data controller for any personal data it holds and is required to comply with data protection law and any data sharing protocols in place.

3.2. The objective of this audit was to review the processes in place and to ensure that the Integration Joint Board complies with the seven key principles of the UK General Data Protection Regulations and data sharing agreements with partner organisations.

4. Audit Findings

4.1. The audit provides substantial assurance that the processes and procedures relating to Information Governance and Data Sharing are well controlled and managed.

4.2. The internal audit report, attached as Appendix 1 to this report, includes one medium and two low priority recommendations within the action plan. There are no high-level recommendations made as a result of this audit.

5. Contribution to quality

Please indicate which of the Orkney Community Plan 2021 to 2023 visions are supported in this report adding Yes or No to the relevant area(s):

Resilience: To support and promote our strong communities.	No.
Enterprise: To tackle crosscutting issues such as digital connectivity, transport, housing and fuel poverty.	No.
Equality: To encourage services to provide equal opportunities for everyone.	No.
Fairness: To make sure socio-economic and social factors are balanced.	No.
Innovation: To overcome issues more effectively through partnership working.	No.
Leadership: To involve partners such as community councils, community groups, voluntary groups and individuals in the process.	No.
Sustainability: To make sure economic and environmental factors are balanced.	No.

6. Resource and financial implications

6.1. There are no resource or financial implications associated directly with this report.

7. Risk and equality implications

7.1. There are no risk or equality implications associated directly with this report.

8. Direction required

Please indicate if this report requires a direction to be passed to:

NHS Orkney.	No.
Orkney Islands Council.	No.

9. Escalation required

Please indicate if this report requires escalated to:

NHS Orkney.	No.
Orkney Islands Council.	No.

10. Authors and contact information

10.1. Stephen Brown (Chief Officer), Integration Joint Board. Email: stephen.brown3@nhs.scot, telephone: 01856873535 extension 2601.

10.2. Andrew Paterson (Chief Internal Auditor), Integration Joint Board. Email: andrew.paterson@orkney.gov.uk, telephone 01856873535 extension 2107.

11. Supporting documents

11.1. Appendix 1: Information Governance and Data Sharing Audit Report.



Internal Audit

Audit report

IJB Information Governance and Data Sharing

Draft issue date: 04 February 2022

Final issue date: 11 February 2022

Distribution list:	IJB Chief Officer IJB Chief Finance Officer Data Protection Officer
---------------------------	--

Contents

Audit Opinion	1
Executive Summary	1
Introduction	2
Audit Scope.....	2
Background.....	2
Audit Findings	3
Action Plan.....	6
Key to Opinion and Priorities.....	7

Audit Opinion

Based on our findings in this review we have given the following audit opinion.

Substantial

The framework of governance, risk management and control were found to be comprehensive and effective.

A key to our audit opinions and level of recommendations is shown at the end of this report.

Executive Summary

Our audit provides adequate assurance that the information governance and data sharing processes of the Orkney Integration Joint Board (IJB) are controlled and managed with some areas of good practice being evident, including:

- A formal Information Sharing Protocol, and Memorandum of Understanding signed by Orkney Islands Council (OIC) and National Health Service Orkney (NHSO).
- A Records Management Plan which has been approved by the Keeper of Records in Scotland.

The IJB, in its role of commissioning board, only holds personal data relating to its two Officers.

In practice, the two Officers of the IJB will view and hold some personal data when supporting service delivery.

The IJB's strategic role in the commissioning of service delivery provided by its partners can also, in practice, become intertwined with service delivery. In delivering the service, partners will need to share personal data. Any risk to the timeous sharing of personal data could risk efficient delivery of service, which in turn poses a strategic risk to delivery of service, and reputational risk, to the IJB.

Our review is limited only to information governance and data sharing processes of the IJB in performing its own role.

However, the IJB may need to understand and consider information governance and data sharing processes amongst partners, should the method of service delivery evolve in future.

The report includes 3 recommendations which have arisen from the audit. The number and priority of the recommendations are set out in the table below. The priority headings assist management in assessing the significance of the issues raised.

Responsible officers will be required to update progress on the agreed actions via Pentana Risk.

Total	High	Medium	Low
3	0	1	2

The assistance provided by Officers contacted during this audit is gratefully acknowledged.

Introduction

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018.

It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018 to reflect the UK's status outside the EU.

The UK GDPR is the UK's General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights, and obligations for most processing of personal data in the UK.

Should the IJB have collected any personal or sensitive personal data it should be using a risk-based approach to justify how and why it uses this data.

Should the IJB share data with any of its partners, or other bodies, this should be in conformance with legislative obligations, its Data Sharing Protocol, and Data Sharing Agreements in place.

This review was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Audit Scope

The scope of this audit included a review of the IJB's processes and controls, in particular its compliance to the seven key principles of the UK GDPR, these are:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability.

Background

The IJB's activity, being a commissioning agent, does not require it to handle any personal or sensitive data relating to service users. The only personal data handled by the Integration Joint Board, for its purpose, relates to its two members of staff, the Chief Officer and the Chief Finance Officer.

Nevertheless, the IJB is considered a data controller for the limited personal data it may hold and is required to comply with data protection law.

The IJB has taken the following steps with regards to compliance with legislative requirements:

- On 1 December 2016, the IJB was registered as a controller with the Information Commissioner's Office (ICO) (Registration reference: ZA207653).
- On 25 March 2018, the IJB's Chief Officer nominated the Council's Data Protection Officer and Head of Legal Services, to become the Board's Data Protection Officer, with the appointment being formalised at a Meeting of the IJB Board on 27 June 2018.
- On 25 June 2019, the Integration Joint Board adopted its Records Management Plan, which, inter alia states that, "because the only special category information that the Board is likely to handle relates to members of staff who are employees of the Council [at the time of this report], the Board has decided to adopt and follow the Council's Data Protection Policy and Data Protection Procedure. As employees of the Council [now of its partners], the Board's staff are already required by their employment contracts to comply with the Council's Data Protection Policy and Procedure."

The Orkney Integration Scheme agreement between Orkney Islands Council and NHS Orkney set out the requirement for the IJB to agree an Information Sharing Protocol to include, inter alia, the procedure for the sharing of information between parties.

The Information Sharing Protocol provides a high-level focus on the purposes underlying the sharing of specific information. It provides high level guidance to:

- The processes for sharing information.
- The specific purposes served.
- The people it impacts upon.
- The relevant legislative powers.
- What data is to be shared.
- The consent processes involved.
- Any required operational procedures and processes for review.

It is the responsibility of the IJB's Chief Officer that appropriate arrangements are in place in respect of information governance and the requirements of the Scottish Information Commissioner's Office.

Audit Findings

1.0 Data Protection Officer

- 1.1 A specific requirement from legislation is that the IJB board must publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.
- 1.2 The contact details of the IJB's Data Protection Officer could not be found from a simple internet search.
- 1.3 It is recommended that the contact details of the IJB's Data Protection Officer should be more prominent on the partners respective websites.

Recommendation 1

- 1.4 It is good practice, in situations where the Data Protection Officer is not under a contract of employment with the organisation to have a formal engagement agreement in place for the performance of this role. Currently the Data Protection Officer does not have a formal

engagement agreement with the IJB, largely because the IJB handles very little personal data.

- 1.5 However, it is recommended that a simple agreement be drawn up between the IJB and its Data Protection Officer.

Recommendation 2

2.0 Records Management Plan

- 2.1 The most recent version of the IJB's Records Management Plan which has received the approval of the Keeper of Records of Scotland, was approved by the IJB on 9 December 2020 and submitted to the Keeper of Records of Scotland on 14 January 2021.
- 2.2 The IJB's Record Management Plan was endorsed by the Keeper of Records for Scotland on 5 February 2021. The summary being that "Elements 1-15 that the Keeper considers should be in a public authority records management plan have been properly considered by (the) Orkney Integration Joint Board. Policies and governance structures are in place to implement the actions required by the plan."
- 2.3 The Keeper formally agreed to the IJB's Record Management Plan and recommended "that Orkney Integration Joint Board should publish its agreed Records Management Plan as an example of good practice within the authority and the sector".
- 2.4 Applying a RAG system, the Keeper graded eleven elements of the plan as green (noting his agreement), three elements as amber (noting his agreement to the element as an "improvement model"), and one element as not applicable due to the fact that the IJB does not share records with third parties to carry out functions of the IJB.
- 2.5 The three elements, rated as amber, relate to the following:
 - Audit Trail – in tracking the location and movement of documents.
 - Business Classification – The Keeper commended the IJB's self-recognition that IJB staff may hold documents in personal drives and personal e-mail accounts.
 - Destruction Arrangements – the Keeper again commended the self-identified gap in provision of this element and that it is working towards closing this gap.
- 2.6 A report reviewing the progress on the implementation of the records management plan, and progress in improvement to the three elements agreed as an improvement model is due to be presented to the IJB at its meeting of 22 March 2022.

3.0 Information Sharing Protocols

- 3.1 The Information Sharing Protocol (ISP) for Orkney Health and Care, NHS Orkney, Orkney Islands Council, GPs and its voluntary sector partners is supplementary to the Scottish Accord on the Sharing of Personal Information (SASPI) and has been agreed between the participating partner organisations. The agreement was intentionally prepared to be a high-level agreement.
- 3.2 A Memorandum of Understanding document was agreed, in July 2020, between the OIC and NHSO in relation to the sharing of information for the purposes of the provision of integrated Health and Social Care services in Orkney. The document being signed by the respective Senior Information Risk Owners of both organisations. This document, in part, supersedes the Information Sharing Protocol referred to at 3.1.

- 3.3 A code of practice document for information sharing, confidentiality and consent, entitled growing up in Orkney 3, and relating to getting it right for every child (GIRFEC) has been developed and is currently awaiting signatures to the agreement. This document is scheduled for review on 1 April 2022 where it is planned to incorporate the Independent GP sharing agreement.
- 3.4 The most recent Information Sharing Agreement between the IJB, OIC, NHSO and Public Health Scotland was signed by the partners in July 2021. This agreement provides the IJB access to health and social care planning and performance analytics to help with its own planning and performance activity.
- 3.5 Partners to the IJB also engage in various other data sharing agreements. Examples of these are those between OIC Assessment Teams and NHS Orkney via the SDS Single Shared Assessment and between OIC, NHSO, the Northern Constabulary and Voluntary Action Orkney.
- 3.6 The absence of a data sharing agreement should not prevent the sharing of information where there is a legal obligation to do so.
- 3.7 However, for good practice it is recommended that the IJB maintains a register of its data sharing agreements, memorandums of understanding, or any other relevant documents, together with their respective due dates of review, to control the ongoing administration of these documents.

Recommendation 3

Action Plan

Recommendation	Priority	Management Comments	Responsible Officer	Agreed Completion Date
1) The contact details of the IJB's Data Protection Officer should be more prominent on the partners respective websites.	Low	Agreed - The digital communications officers at each of the respective organisations will be contacted to update this information on the partners websites.	Chief Officer	28 Feb 2022
2) A service agreement should be put in place between the IJB and its Data Protection Officer.	Low	Agreed – A service agreement will be established between the Chief Officer and the Data Protection Officer.	Chief Officer	28 Feb 2022
3) The IJB should maintain a register of its data sharing agreements, memorandums of understanding, or any other relevant documents, together with their respective due dates of review.	Medium	Agreed – This task will be carried out by the information governance champions within OHAC.	Chief Officer	28 Feb 2022

Key to Opinion and Priorities

Audit Opinion

Opinion	Definition
Substantial	The framework of governance, risk management and control were found to be comprehensive and effective.
Adequate	Some improvements are required to enhance the effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Recommendations

Priority	Definition	Action Required
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.