ABERDEEN CITY COUNCIL

| | |
|---|---|
| **COMMITTEE** | Audit, Risk and Scrutiny Committee |
| **DATE** | 23 March 2023 |
| **EXEMPT** | No |
| **CONFIDENTIAL** | No |
| **REPORT TITLE** | Internal Audit Report AC2302 – IJB Data Sharing |
| **REPORT NUMBER** | IA/AC2302 |
| **DIRECTOR** | N/A |
| **REPORT AUTHOR** | Jamie Dale |
| **TERMS OF REFERENCE** | 2.2 |

## 1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on IJB Data Sharing

## 2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

## 3. CURRENT SITUATION

3.1 Internal Audit has completed the attached report which relates to an audit of IJB Data Sharing

## 4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

## 5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

## 6. ENVIRONMENTAL IMPLICATIONS

6.1 There are no direct environmental implications arising from the recommendations of this report.

## 7. RISK

7.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are detailed in the resultant Internal Audit reports. Recommendations, consistent with the Council's Risk Appetite Statement, are made to address the identified risks and Internal Audit follows up progress with implementing those that are agreed with management. Those not implemented by their agreed due date are detailed in the attached appendices.

## 8. OUTCOMES

8.1 The proposals in this report have no impact on the Council Delivery Plan.

8.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

## 9. IMPACT ASSESSMENTS

| Assessment | Outcome |
|---|---|
| **Impact Assessment** | An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics. |
| **Privacy Impact Assessment** | Not required |

## 10. BACKGROUND PAPERS

10.1 There are no relevant background papers related directly to this report.

## 11. APPENDICES

11.1 Internal Audit Report AC2302 – IJB Data Sharing

## 12. REPORT AUTHOR CONTACT DETAILS


| | |
|---|---|
| **Name** | Jamie Dale |
| **Title** | Chief Internal Auditor |
| **Email Address** | Jamie.Dale@aberdeenshire.gov.uk |
| **Tel** | (01467) 530 988 |

# Internal Audit

# Assurance Review of IJB Data Sharing

**Status:** Final
**Date:** 5 December 2022
**Risk Level:** Function

**Report No:** AC2302
**Assurance Year:** 2022-23

| Net Risk Rating | Description | Assurance Assessment |
|---|---|---|
| **Moderate** | The framework of governance, risk management and control provides reasonable assurance over the achievement of objectives. Net risks to objectives are moderate in relation to the IJB's activities and processes. | **Reasonable** |

| Report Tracking | Planned Date | Actual Date |
|---|---|---|
| **Scope issued** | 08/07/2022 | 08/07/2022 |
| **Scope agreed** | 15/07/2022 | 18/07/2022 |
| **Fieldwork commenced** | 01/08/2022 | 06/07/2022 |
| **Fieldwork completed** | 29/08/2022 | 26/08/2022 |
| **Draft report issued** | 19/09/2022 | 21/10/2022 |
| **Process owner response** | 09/10/2022 | 08/11/2022 |
| **Director response** | 17/10/2022 | 05/12/2022 |
| **Final report issued** | 24/10/2022 | 05/12/2022 |
| **Audit Committee** | 28/02/23 | |

| Distribution | |
|---|---|
| **Document type** | Assurance Report |
| **Director** | Sandra MacLeod, Chief Officer (ACHSCP) |
| **Process Owner** | Martin Allan, Business and Resilience Manager (ACHSCP) |
| **Stakeholder** | Fraser Bell, Chief Operating Officer (ACHSCP) |
| | Paul Mitchell, Chief Finance Officer (ACHSCP) |
| | Helen Cannings, Data Protection Officer (ACC) |
| ***Final only** | Alan Bell, Data Protection Officer (NHS Grampian) |
| | Nick Fluck, Medical Director (NHS Grampian)* |
| | Vikki Cuthbert, Interim Chief Officer – Governance (ACC)* |
| | Ronnie McKean, Corporate Risk Lead (ACC)* |
| | External Audit* |
| **Lead auditor** | Jamie Dale, Chief Internal Auditor |

# Contents

# 1 Introduction

## 1.1 Area subject to review

The General Data Protection Regulation (GDPR) and most of the provisions of the Data Protection Act 2018 (the 2018 Act) came into force on 25 May 2018. Upon the UK's exit from the European Union the EU GDPR was replaced domestically by the UK GDPR; the key principles, rights and obligations remain the same.

The GDPR regulates the processing of personal data which amongst other things includes its use, transmission, and dissemination. Within this, 'data sharing' is critical to the delivery of effective health and social care services, without which an integrated approach to service delivery could not be achieved. This could lead to a reduction in the quality of care and increase the risk of harm to individuals because the different Partners and agencies involved in providing services may be unaware of the needs of the individual and the actions of others.

As 'Data Controllers' the IJB, Aberdeen City Council and NHS Grampian (NHSG) have a responsibility to comply with data protection law. Different systems and reporting tools assist the IJB in making strategic decisions to steer the integration and provision of health and social care services. Data within these systems is ultimately used at an operational level where the IJB directs its Partners (Aberdeen City Council and NHSG operating as the Aberdeen City Health and Social Care Partnership – ACHSCP) to deliver services intended to achieve positive health and wellbeing outcomes, increase individuals' resilience, and provide personalised care where and when it is required. This operational element will not be a specific focus of this review, instead the audit is being carried out at the more strategic 'Data Controllers' level.

The objective of this audit is to ensure that the IJB has appropriate assurance over the arrangements / procedures for data sharing between the Partners themselves, (Aberdeen City Council and NHS Grampian) and other agencies responsible for delivering health and social care arrangements in respect of delegated functions and in line with the IJB's strategic directions. In general, one of the delegated partners will fill the role of Data Controller for the function, noting that the IJB itself acts as Data Controller for a limited subset of data it manages directly.

## 1.2 Rationale for the review

The audit will be a joint review in conjunction with NHS Grampian and Moray Council (following conclusion of a similar review for Aberdeenshire in 2021) and provides an opportunity to determine where practice can be standardised across the organisations and broader assurance gained.

Data sharing and GDPR compliance within the Aberdeen City IJB and for the delivery of Aberdeen City Health & Social Care Partnership services and functions has not been audited previously.

Whilst the data controlled by the IJB itself is restricted to Committee Papers, the data that the Partners (Aberdeen City Council and NHS Grampian) control is largely highly sensitive personal information. This data is also shared with care providers which are appointed to meet individuals' care needs. Any failure to comply with data protection law and to adequately mitigate information risk could result in ICO investigation, financial penalties and civil claims and would have an impact on customers and on the reputation of the IJB and the Partners. As the IJB directs the Partners to deliver the services delegated under the Integration Scheme, and the integration and transformation of their activities and data, it has an interest and therefore requires assurance over delivery, including data protection.

Information Risk is identified in the risk registers of both Aberdeen City Council and NHS Grampian. Work is currently ongoing to ensure the implications of the risk of information sharing associated with the revised IJB Strategic Plan is being incorporated in the ACHSCP Risk Register and Board Escalation and Assurance Framework.

## 1.3 How to use this report

This report has several sections and is designed for different stakeholders. The executive summary (section 2) is designed for senior staff and is cross referenced to the more detailed narrative in later sections (3 onwards) of the report should the reader require it. Section 3 contains the detailed narrative for risks and issues we identified in our work.

# 2 Executive Summary

## 2.1 Overall opinion

The full chart of net risk and assurance assessment definitions can be found in Appendix 1 – Assurance Scope and Terms. We have assessed the net risk (risk arising after controls and risk mitigation actions have been applied) as:

| Net Risk Rating | Description | Assurance Assessment |
|---|---|---|
| **Moderate** | The framework of governance, risk management and control provides reasonable assurance over the achievement of objectives. Net risks to objectives are moderate in relation to the IJB's activities and processes. | **Reasonable** |

The organisational risk level at which this risk assessment applies is:

| Risk Level | Definition |
|---|---|
| **Function** | This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of policy within a given function. |

## 2.2 Assurance assessment

The level of net risk is assessed as **MODERATE**, with the control framework deemed to provide **REASONABLE** assurance over the IJB's approach to data sharing.

Information, when used lawfully, held securely and is reliable in terms of its availability and accuracy, facilitates the Aberdeen City Health and Social Care Partnership in providing high quality, safe and effective services which meet service user needs. Data ultimately facilitates the IJB and Partnership management's decision making in order for integration and transformation intentions to be realised, performance targets to be met, and strategic objectives delivered.

Data Protection and other information legislation requires the Partners within the Aberdeen City Health & Social Care Partnership (Aberdeen City Council and NHS Grampian) and the IJB to be aware of the consequences of inadequate information risk management. Accordingly appropriate resources, robust policies and procedures, and a clear governance framework must be in place to ensure data is appropriately managed in an information risk environment which the Aberdeen City Health & Social Care Partnership and the IJB itself understands.

Information risk is increased where data is shared between organisations, hence the Information Commissioner's Office (ICO) Data Sharing Code of Practice recommends that organisations have a data sharing agreement. A data sharing agreement between NHSG and the Aberdeen City, Aberdeenshire, and Moray Councils was drafted and issued in 2022 but has not yet been signed by all parties. However the Policy, Procedure and Governance framework in place within each Partner organisation should ensure their staff are adequately trained in data protection to operate in a risk environment where their responsibility is clear.

Records Management plans are in place in accordance with legislation, but how these and other procedural documents and the key staff involved fit into the overall information governance framework for the IJB is not clearly documented. The types of information, how this is shared, the systems used, and the individuals responsible for ensuring its quality, security, safe passage, and the authority required, should be clearly mapped out. Where appropriate, there may be scope for the harmonisation of procedures, potentially with the other IJB's that NHS Grampian serves.

Assurance over information compliance can be drawn from the Partners' Risk Boards and records of training, data protection impact assessments, and information breaches, all of which are reported

internally. The Chief Officer of the IJB is also a member of NHS Grampian's Chief Executive Team and similar with Aberdeen City Council. The Business and Resilience Manager is responsible for providing the IJB with this assurance: more comprehensive regular assurance reporting to the Risk, Audit and Performance Committee, based on such sources, would be beneficial for the IJB.

The original intention of this review was for the assurance providers of the three organisations to work together and where individual reports would be produced, also include a covering report providing details of the assurance gained from all areas of work. As there is currently limited assurance being provided directly to the IJB on this aspect of its business, Internal Audit sought assurance from the Partners over their data protection governance arrangements, and how these are applied in respect of services delegated to the IJB.

Comprehensive data was available on the arrangements put in place by Aberdeen City Council. However, due to other commitments (a regulatory audit from the ICO) NHS Grampian has not been able to facilitate such a review and their auditors instead plan to carry out the work later in the year. The IJB will still require assurance over this aspect of its governance arrangements, and recommendations have been made in this report as to the type and extent of assurance required. The intention is still to carry out analysis of all three pieces of work and create an overarching summary, however this will not be available until later in the financial year. Where we have been unable to confirm arrangements or gain assurance over elements of the control framework managed by NHS Grampian, this has been highlighted in the report and Management should seek to gain assurance over these areas where they feel it is needed. However, assurance can be taken from the results of the ICO audit, and from the engagement of NHS Grampian in the finalisation of this report.

## Severe or major issues / risks

Issues and risks identified are categorised according to their impact on the Board. The following are summaries of higher rated issues / risks that have been identified as part of this review:

| Ref | Severe or Major Issues / Risks | Risk Agreed | Risk Rating | Page No. |
|---|---|---|---|---|
| 1.1 | **Governance** – A review of the current governance arrangements put in place by the Board highlighted:<br>• No Data Sharing Agreement is currently in place for the Aberdeen City IJB. A data sharing agreement between NHSG and the Aberdeen City, Aberdeenshire, and Moray Councils was drafted and issued in 2022 but has not yet been signed by Aberdeen City Council.<br>• The IJB Strategic Risk Register did not recognise information sharing and management as a risk.<br>• Governance arrangements appear to be appropriate but could be mapped out in order that the Business and Resilience Manager and IJB members can see the sources that provide assurance in respect of ACHSCP Partners' compliance with information sharing and data protection legislation.<br>There is a risk that the current governance arrangements may not facilitate effective data | Yes | **Major** | 10 |

| Ref | Severe or Major Issues / Risks | Risk Agreed | Risk Rating | Page No. |
|---|---|---|---|---|
| | sharing and provide effective overarching control. | | | |

## 2.3 Management response

*Management welcome the audit and its recommendations. The audit will help to provide assurance to the Partnership's Senior Leadership Team as well as the IJB. The Business and Resilience Manager post can provide assurance to the Senior Leadership Team around data sharing and the IJB's Data Protection officer can provide assurance to the Board. The mapping of this assurance from the IJB's partners (NHS Grampian and Aberdeen City Council) helps to provide clarity as well as assurance and the mapping process can assist in outlining the roles and responsibilities of the Business and Resilience Manager and Data Protection officer posts in relation to data sharing matters for the IJB.*

*The remit and agency of the IJB over data protection governance is relatively limited – as it is data controller for only a limited amount of information. It will need to rely on Partners to the Integration Scheme (NHSG and Aberdeen City Council) which are data controllers in their own right, and have their own governance and reporting arrangements, in respect of appropriate processing of personal data in the joint activities Directed by the IJB; and in addressing the implications of any data breaches. Training has been provided by the DPO in this regard in previous years. However, it is acknowledged that a review of the assurance required by and provided to the IJB could be beneficial.*

*A pan-Grampian data sharing agreement was drafted in 2022 and shared with relevant partners. There has been positive feedback and it is awaiting conclusion of the relevant partners' internal governance arrangements before it can be fully implemented.*

# 3 Issues / Risks, Recommendations, and Management Response

## 3.1 Issues / Risks, recommendations, and management response

| Ref | Description | Risk Rating | Major |
|---|---|---|---|
| 1.1 | **Governance** – Appropriate governance, incorporating agreements, risk management and resources, is imperative to ensure an effective framework of control for information management and data sharing. A review of the current arrangements put in place by the Board highlighted:<br>• No overarching Data Sharing Agreement (which is deemed good practice by the ICO) is currently in place for the Aberdeen City IJB. A data sharing agreement between NHSG and the Aberdeen City, Aberdeenshire, and Moray Councils has been drafted and issued, but has yet to be signed Aberdeen City Council. There are however information sharing agreements covering specific projects / activities.<br>• The IJB Strategic Risk Register did not clearly recognise information sharing and management as a risk. The IJB's strategic risk register does now reference IG as a risk to transformation. This was discussed at an IJB workshop in August and has been reported through the IJB in October 2022<br>• Governance arrangements appear to be appropriate but could be mapped out in order that the Business and Resilience Manager and IJB members can see the sources (e.g. Risk Boards) that provide assurance in respect of ACHSCP Partners' compliance with information sharing and data protection legislation.<br>• DPIAs are being completed and logged in individual Partners' registers for activities to demonstrate that information sharing risks have been given due consideration.<br>• Data Protection officers are in place within each Partner, and the DPO for NHSG has also been appointed as the DPO for the IJB.<br>There is a risk that the current governance arrangements may not facilitate effective data sharing and provide effective overarching control. | | |
| | **IA Recommended Mitigating Actions**<br>With regards to the above issues, it is recommended that Management should:<br>• Establish a Data Sharing Agreement between the Partners which gives due consideration to any data sharing beyond the Partners themselves.<br>• Map the sources of assurance ACHSCP draws on from within the Partners and elsewhere to provide assurance to the IJB that information management and sharing is adequately governed.<br>• Ensure assurance is obtained that Data Protection Impact Assessments are completed where appropriate and that a register of these is held by each Data Controller.<br>• Consider whether data protection resources available to the IJB are sufficient to ensure the IJB is compliant and well informed concerning data legislation compliance and practice. | | |

| Ref | Description | Risk Rating | Major |
|---|---|---|---|
| | **Management Actions to Address Issues/Risks**<br>*Data Sharing arrangements will be reviewed in conjunction with the IJB Data Protection Officer to establish whether and to what extent an agreement between the Partners is required, and a timeline for its development. Consideration will also be given to pan-Grampian harmonisation of the arrangements as recommended at 1.3 below.*<br><br>*The IJB DPO has previously outlined the relevant governance and information flows for IJB data protection training. This can be refreshed, and ACHSCP will map the sources of assurance as above.*<br><br>*DPIA's are being done for projects reported to IJB. All functions delivered on behalf of the IJB will be subject to a Direction, which is included on a tracker which is regularly monitored and reported to the IJB. It will be explored whether this can be expanded to identify and record assurance in instances where data is required to be shared.*<br><br>*Following conclusion of the assurance mapping process, management will consider whether data protection resources and reporting available to IJB are sufficient.* | | |

| Risk Agreed | Person(s) | Due Date |
|---|---|---|
| Yes | Business and Resilience Manager | April 2023 (Data Sharing Agreement plans)<br><br>April 2023 (DPIA assurance)<br><br>September 2023 (Assurance mapping)<br><br>September 2023 (Resource review) |

| Ref | Description | Risk Rating | Moderate |
|---|---|---|---|
| 1.2 | **Staff Training and Responsibilities** – All staff have responsibility for protecting the data their organisation holds but some have particular responsibility to monitor and maintain the information control environment and to report and address control issues or incidents via various channels which ultimately provide the IJB with assurance over information management and sharing.<br><br>Accordingly, all staff should receive up to date Data Protection training and be familiar with the latest Information Management and Record Management Plans, Policies and Procedures which are in place. Where adequate, this can help ensure that data held is accurate, used lawfully, adequately protected and only shared by appropriate means when approved.<br><br>The IJB Data Protection Officer and HSCP Business and Resilience Manager should receive updates from the Partners regarding information management, and provide the Risk, Audit and Performance Committee and ultimately the IJB with assurance regarding information management and data sharing control. Risk Boards would be one source of information / assurance.<br><br>The review identified the following:<br><br>• Roles and responsibilities of key staff who confirm and provide assurance over information sharing, records management, and data protection, such as the data | | |

| Ref | Description | Risk Rating | Moderate |
|---|---|---|---|

protection officers, the Business and Resilience Manager (ACHSCP), the Medical Director (NHSG), the Chief Operating Officer (ACHSCP), Risk Board members and identified information systems owners within the Partner organisations, are relatively clear but not in terms of how they align with the governance and reporting structure.

- The process for, the sources of and reporting of information management and data sharing assurance to the IJB, from ACC and NHSG Boards is unclear.
- Training resources in ACC are sufficient to ensure Board Members and staff are aware of data protection responsibilities. Whilst there are registers providing assurance that staff have received up to date data protection training in respect of specific systems (e.g. D365), further assurance over Partners' training may be required.

Shortcomings in training or practice could compromise the information management environment, impact on service user and staff safety, and affect delivery of operational and strategic plans. Financial penalties and reputational damage could result from breaches of data legislation and poor information sharing practice.

**IA Recommended Mitigating Actions**

With regards to the above issues, it is recommended that Management should:

- Identify Key staff roles in the Governance mapping recommended at 1.1 above.
- Establish reporting mechanisms which ensure the Business and Resilience Manager receives assurance regarding information sharing and provides this assurance to the IJB.
- Establish mechanisms which provide assurance that data protection training is up to date.

**Management Actions to Address Issues/Risks**

*Staff roles and reporting lines will form part of the assurance mapping to be implemented in response to 1.1 above. Training records are also a source of assurance.*

*The Business and Resilience Manager will liaise with ACC and NHSG on the training of those staff who report to the IJB and IJB Board members.*

| Risk Agreed | Person(s) | Due Date |
|---|---|---|
| Yes | Business and Resilience Manager | September 2023 |

| Ref | Description | Risk Rating | Moderate |
|---|---|---|---|
| 1.3 | **Data Management** – Managing Data requires robust policies, procedures and an acute awareness of the information systems used, the processes and controls involved, and the nature of the data held across these systems. Data controllers are subject to higher risk where they share data with other organisations. Data protection policy, procedure, training, and data sharing agreements must be robust, but organisational culture and compliance may vary between the organisations involved.<br><br>Data sharing may entail one-off disclosures or regular sharing which is necessary for routine service delivery. Regardless of any variances between the organisations, it is essential that the IJB has assurance that data sharing is done in a manner which is agreed by all of the organisations and ensures legislative compliance in terms of collection, handling, use, accuracy, and security of the data the partners control. | | |

| Ref | Description | Risk Rating | Moderate |
|---|---|---|---|

An understanding of the cause, extent, and frequency of any data breaches can provide insight into service delivery, systems, procedures, and practice. This can inform operational and strategic decision making and give direction in terms of the delivery of integration, transformation, and strategic objectives.

In respect of data management and sharing, the following matters were observed:

- The policy and procedure of ACC provides a robust framework for information control within which data sharing can be undertaken. The arrangements in NHSG will be subject to their own audit and are currently being reviewed by the ICO, over which assurance will be taken. Given it serves the Aberdeen City, Aberdeenshire, and Moray IJB's, harmonised standards and policies across the local authorities could facilitate data sharing for NHSG and increase assurance that data is managed appropriately.
- A full understanding of the information being shared between the Partners and others, the systems being used, and the individuals responsible for ensuring the controls within these are adequate to ensure accuracy and availability of data whilst preventing loss or data breaches is not evident.
- The Business and Resilience Manager does not receive a regular report of data breaches from each Partner which could be pertinent to strategic and operational decision making.

There is an increased risk of data being compromised where the data and systems involved are not clear and policy and procedure governing these varies between partners. A breach of data legislation could result in reputational damage and financial penalties. Strategic Plan and service delivery could be impacted where the HSCP Business and Resilience Manager is not advised of relevant data-related incidents.

**IA Recommended Mitigating Actions**

With regards to the above issues, it is recommended that Management should:

- Ensure the IJB receives periodic assurance that policy and procedure for data sharing is robust within each Partner.
- Consider and investigate whether there is scope for harmonisation of data protection procedures and policies with the Aberdeenshire and Moray Health and Social Care Partnerships.
- Map out the information sharing environment so that the data sources, types of data, information systems involved, their owners and controls across the Partners are clear and can be given due consideration where new projects or other operational changes are intended.
- Ensure the Business and Resilience Manager is made aware of data breaches relevant to the IJB, including the activities delivered by Partners on its behalf, which could be pertinent to strategic and operational decision making.

**Management Actions to Address Issues/Risks**

*Agreed reporting timescales will be built in to the assurance mapping and reporting exercise agreed at 1.1.*

*As agreed at 1.1 Data Sharing arrangements will be reviewed in conjunction with the IJB Data Protection Officer to establish whether and to what extent an agreement between the Partners is required, and a timeline for its development. Consideration will be given to pan-Grampian harmonisation of the arrangements, and a timeline for development of such an approach.*

*As part of the assurance mapping exercise, the supporting detail and assurance over data sources and processing will also be considered.*

| Ref | Description | Risk Rating | Moderate |
|---|---|---|---|
| | *Data controllers need to resolve any breaches in the first instance, and these are typically addressed, and shared where necessary, at the Senior Information Risk Owner (SIRO) level. The Business and Resilience Manager has previously been informed where potential data risks have been identified by Partners. The process will be reviewed to ensure this takes place as required.* | | |

| Risk Agreed | Person(s) | Due Date |
|---|---|---|
| Yes | Business and Resilience Manager | September 2023 (Assurance mapping and supporting detail)<br><br>April 2023 (Data Sharing harmonisation options)<br><br>April 2023 (Data breach process) |

# 4 Appendix 1 – Assurance Terms and Rating Scales

## 4.1 Overall report level and net risk rating definitions

The following levels and ratings will be used to assess the risk in this report:

| Risk level | Definition |
|---|---|
| Corporate | This issue / risk level impacts the IJB as a whole. Mitigating actions should be taken at the Senior Leadership level. |
| Function | This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of policy within a given function. |
| Cluster | This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer. |
| Programme and Project | This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned. |

| Net Risk Rating | Description | Assurance Assessment |
|---|---|---|
| Minor | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. | Substantial |
| Moderate | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited. | Reasonable |
| Major | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. | Limited |
| Severe | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. | Minimal |

| Individual Issue / Risk Rating | Definitions |
|---|---|
| Minor | Although the element of internal control is satisfactory there is scope for improvement. Addressing this issue is considered desirable and should result in enhanced control or better value for money. Action should be taken within a 12 month period. |
| Moderate | An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on the audited area's adequacy and effectiveness. Action should be taken within a six month period. |
| Major | The absence of, or failure to comply with, an appropriate internal control, which could result in, for example, a material financial loss. Action should be taken within three months. |
| Severe | This is an issue / risk that could significantly affect the achievement of one or many of the IJB's objectives or could impact the effectiveness or efficiency of the IJB's activities or processes. Action is considered imperative to ensure that the IJB is not exposed to severe risks and should be taken immediately. |

# 5 Appendix 2 – Assurance Scope and Terms of Reference

## 5.1 Area subject to review

The General Data Protection Regulation (GDPR) and most of the provisions of the Data Protection Act 2018 (the 2018 Act) came into force on 25 May 2018. Upon the UK's exit from the European Union the EU GDPR was replaced domestically by the UK GDPR; the key principles, rights and obligations remain the same).

The GDPR regulates the processing of personal data which amongst other things includes its use, transmission, and dissemination. This 'data sharing' is critical to the delivery of effective health and social care services, without which an integrated approach to service delivery could not be achieved. This would lead to a reduction in the quality of care and increase the risk of harm to individuals because different the different Partners and agencies involved in providing services may be unaware of the needs of the individual and the actions of others.

As 'Data Controllers' the IJB, Aberdeen City Council and NHS Grampian have a responsibility to adhere to sound data sharing practice. Different systems and reporting tools assist the IJB in making strategic decisions to steer the integration and provision of health and social care services. Data within these systems is ultimately used at an operational level where the IJB seeks through its partners to achieve positive health and wellbeing outcomes, increase individuals' resilience, and provide personalised care where and when it is required. This operational element will not be a specific focus of this review, instead out audit being carried out at the more strategic 'Data Controllers' level.

The objective of this audit is to provide assurance that the IJB has implemented appropriate arrangements / procedures for data sharing between the Partners themselves, (Aberdeen City Council and NHS Grampian) and other agencies responsible for delivering health and social care arrangements and complies with these.

## 5.2 Rationale for review

The audit will be a joint review in conjunction with NHS Grampian and Moray Council and provides an opportunity to determine where practice can be standardised across the organisations and broader assurance gained. Data sharing and GDPR compliance within the Aberdeen City IJB and the Aberdeen City Health & Social Care Partnership has not been audited previously. Whilst the data controlled by the IJB itself is restricted to Committee Papers, the data that the Partners (Aberdeen City Council and NHS Grampian) control is largely highly sensitive personal information. This data is also shared with care providers which are appointed meet individuals' care needs. Any failure to adequately mitigate information risk could result in ICO investigation and financial penalties and would have an impact on customers and on the reputation of the IJB and the Partners. Information Risk is identified in the risk registers of both Aberdeen City Council and NHS Grampian. The Aberdeen City Health and Social Care Partnership also has its own risk register which recognises data sharing.

## 5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the Function level.
- Individual **net risk** ratings for findings.

Please see Appendix 1 – Assurance Terms and Rating Scales for details of our risk level and net risk rating definitions.

### 5.3.1 Detailed scope areas

**As a risk-based review this scope is not limited by the specific areas of activity listed below. Where related and other issues / risks are identified in the undertaking of this review these will be reported, as considered appropriate by IA, within the resulting report.**

The specific areas to be covered by this review are:

- Data Protection Governance and Accountability
- Staff Data Protection Training and Awareness
- Security of Personal Data
- Information Sharing and the Co-ordinated Partnership Approach
- Records Management.

## 5.4 Methodology

This review will be undertaken through interviews with key staff involved in the process(es) under review and analysis and review of supporting data, documentation, and paperwork. To support our work, we will review relevant legislation, codes of practice, policies, procedures, guidance.

The audit will be a joint review in conjunction with NHS Grampian and Moray Council and as such an element of reliance may be placed on the work of other assurance providers

Due to the ongoing impacts of COVID-19, this review will be undertaken remotely. We remain flexible in the face of the rapidly changing risk environment. Where our resourcing or access to the client is impacted further by COVID-19, we will adapt our audit methodology to balance the risks and assurance output and will work in co-operation with key contacts to understand the impact of the situation as it evolves.

## 5.5 IA outputs

The IA outputs from this review will be:

- A risk-based report with the results of the review, to be shared with the following:
  - IJB Key Contacts (see 5.7 below)
  - Audit, Risk and Scrutiny Committee (final only)
  - Risk, Audit and Performance Committee (final only)
  - External Audit (final only)

## 5.6 IA staff

The IA staff assigned to this review are:

- Phil Smith, Auditor **(audit lead)**
- Colin Harvey, Audit Team Manager
- Jamie Dale, Chief Internal Auditor **(oversight only)**

## 5.7 IJB key contacts

The key contacts for this review across the IJB / HSCP are:

- Sandra MacLeod, Chief Officer (ACHSCP)
- Fraser Bell, Chief Operating Officer (ACC)
- Paul Mitchell, Chief Finance Officer (ACHSCP)
- Martin Allan, Business Manager (ACHSCP) **(Process Owner)**
- Helen Cannings, Data Protection Officer (ACC)
- Nick Fluck, Medical Director (NHS Grampian)
- Alan Bell, Data Protection Officer (NHS Grampian)

## 5.8 Delivery plan and milestones

The key delivery plan and milestones are:

| Milestone | Planned date |
|---|---|
| Scope issued | 08/07/2022 |
| Scope agreed | 15/07/2022 |

| Milestone | Planned date |
|---|---|
| Fieldwork commences | 01/08/2022 |
| Fieldwork completed | 29/08/2022 |
| Draft report issued | 19/09/2022 |
| Process owner response | 09/10/2022 |
| Director response | 17/10/2022 |
| Final report issued | 24/10/2022 |