Appendix 2

AUDIT REPORT 23'009

INFORMATION MANAGEMENT

Executive Summary

The annual audit plan for 2022/23 provides for an audit review of the systems and procedures in the management and security of adult social care information, including the transfer of information between the Council to NHS Grampian and other care providers. This review should also complement the recent audit undertaken regarding the Council's compliance with the UK General Data Protection Regulation.

Effective information controls within adult social care are particularly important due to the sensitive nature of information held concerning service users. In addition, the Council has duties under data protection regulations, and breaches of these regulations can result in substantial financial penalties being levied by the Information Commissioner's Office.

In recent years, discussions have been held with the internal audit providers for NHS Grampian, Aberdeen City and Aberdeenshire Councils. The intention has been to develop closer working relationships to better coordinate the audit planning process within social care. An audit of Information Management was agreed as the first step within this process. This has progressed well with a joint approach undertaken, especially within the Internal Audit Services of Aberdeen City, Aberdeenshire and Moray Councils. However, further to a recent communication, it has not proved possible for the NHS Grampian Internal Audit Provider to participate as a review by the Information Commissioner has taken precedence.

The audit was carried out in accordance with Public Sector Internal Audit Standards (PSIAS).

The review has highlighted the following areas for consideration:-

- The Information Commissioner considers it is good practice to have a data sharing agreement when information is shared between two organisations. Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards, and help organisations involved in sharing to be clear about their roles and responsibilities. It was found that the data sharing arrangements for patient/ service user information between the Council and NHS Grampian are still based on a Memorandum of Understanding from 2011. Consideration should be given to agreeing on a Data Sharing Agreement between the Council and NHS Grampian to reflect the updated Data Protection Legislation.

- A Data Protection Impact Assessment (DPIA) is an essential part of the Council's accountability obligations under the UK General Data Protection Regulation (GDPR). A DPIA is a process to help identify and minimise data protection risks. Information regarding adult social care service users are shared with approximately 80 care providers. However, it was found that only one DPIA had been completed regarding these data sharing arrangements.

- The Council uses a software application to schedule visits for care workers to service users. Details held within this software include personal information concerning individuals receiving care. The software application is administered through desktop computers but with a facility to download information to a mobile device used by carers. Access controls were found to have been installed within the mobile devices; however no individual user login or password was required to access the desktop computers used for administering the software application.

Recommendations

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
Key Control: Arrangements are in place for secure handling of personal data.						
5.01	Data Protection Impact Assessments (DPIAs) should be undertaken to determine whether additional safeguards need to be implemented where information concerning service users is shared with care providers.	High	Yes	DPIAs are to be carried out on all processes, including for new contracts where data sharing is required with partners.	Records and Heritage Manager, and, Data Protection Officer/ Commissioning Manager	31/12/2023
5.02	Assurances should be obtained that appropriate data protection training has been undertaken by NHS Grampian employed officers requiring access to Council administered databases.	Medium	Yes	Arrangements to be put in place to confirm that Data Protection training has been received by NHS staff prior to being given access	Information Systems Officer	31/03/2023

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
				to Council systems.		
5.03	Access to the Staffplan Software Application used to schedule visits by Care Workers to service users should require individual user login and password controls.	Medium	Yes	Password Protection facility to be utilised for Staffplan office based access.	Provider Services Manager	31/03/2023
5.04	Regular reviews should be undertaken to confirm the access requirement to the Occupational Therapy Stores Management System by NHS Grampian employed officers.	Medium	Yes	Develop procedure for confirming current NHS staff access requirements to Council systems.	Information Systems Officer	31/03/2023

Appendix 2

Risk Ratings for Recommendations						
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	Medium	Less critically important controls absent, not being operated as designed or could be improved.		Low	Lower level controls absent, not being operated as designed or could be improved.
No.	**Audit Recommendation**	**Priority**	**Accepted (Yes/ No)**	**Comments**	**Responsible Officer**	**Timescale for Implementation**
Key Control: Appropriate security controls operate within Information sharing arrangements						
5.05	The Council and NHS Grampian should agree on an updated Data Sharing Agreement (DSA) for operational information concerning service users that includes the requirements of the current data protection regulations.	Medium	Yes	Overarching Information Sharing Protocol with NHS Grampian to be updated and signed. Dedicated DSAs then to be completed for individual processes.	Records and Heritage Manager, and, Data Protection Officer/ Commissioning Manager	31/06/2023
5.06	Contract compliance visits to care providers should include a review that appropriate systems are being followed to manage and ensure the security of service user information.	Medium	Yes	Contract Monitoring checklist for external providers updated to include Information Management.	Commissioning Manager	Implemented