Regional Health and Social Care Information Sharing Agreement

Schedule B – Qualifying Standard (Policy)

Contents

Visit www.regisa.uk for the latest versions of Schedules

Schedule B - Qualifying Standard

This schedule to the Regional Health and Social Care Information Sharing Agreement sets out the qualifying standard for organisations to access and process data shared under the Regional Health and Social Care Information Sharing Agreement.

Audit and quality

1. Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the auditors and the data subject on request.
2. The use of computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access.
3. Procedures are in place to ensure the accuracy of service user (data subject) information on all systems that support the provision of care.

Confidentiality

4. All transfers of personal and sensitive information are conducted in a secure and confidential manner.
5. Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected.
6. Where sharing of personal information is required beyond the boundaries of the data controller organisation, protocols governing the sharing are agreed with other organisations.
7. The confidentiality of service user information that is not involved in the process of providing direct care is protected through anonymisation techniques where appropriate

Contracts

8. All contracts with staff, contractors and third parties contain clauses that clearly identify information governance responsibilities.

Disclosure

9. Individuals are informed about the proposed uses of their personal information.

Governance

10. All new processes, services and systems are implemented in a controlled manner.
11. Background checks are carried out for staff, contractors and third parties given access to confidential and sensitive information.
12. Processes and technical measures including but not limited to role based access controls are in place to ensure that only those staff, contractors and third parties with a lawful purpose to access confidential data are able to do so.
13. Responsibility for Information Governance and for the scrutiny and approval of all Information Governance matters including but not limited to information sharing protocols and information risk management policies has been assigned to an appropriate member, or members, of staff.
14. There are approved and comprehensive Information Governance policies with associated strategies and/or improvement plans.
15. There are documented Information Governance incident management and reporting procedures.

Security

16. All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.
17. All new processes, services and systems are developed and implemented in a secure manner.
18. Operating and application information systems that store and process confidential and sensitive information that are used by the organisation to support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
19. Policy and procedures are in place to ensure that information technology networks operate securely.
20. The requirements of the Data Security and Protection Toolkit (DSPT) are satisfied.
21. Unauthorised access to the premises, equipment, records and other assets is prevented.

Training

22. All staff members are provided with appropriate training on information governance requirements.
23. Staff members are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.

Statement of Compliance

In respect of the organisation's membership of the Regional Health and Social Care Information Sharing Agreement by signing the master agreement the organisation asserts and confirms its satisfactory compliance with the qualifying standard criteria set out in paragraphs 1 to 23 of this schedule above and with the requirements of the General Data Protection Regulation ("GDPR") and associated enabling legislation including but not limited to the Data Protection Act 2018 as amended.

End of Schedule B