Regional Health and Social Care Information Sharing Agreement

Qualifying Standard – Supplementary Assurance Requirements

Information Governance Steering Group 13th February 2024

Contents

Visit www.regisa.uk

Qualifying Standard Supplementary Assurance Requirements

This document supports the Regional Health and Social Care Information Sharing Agreement (Regional ISA) Qualifying Standard (https://www.regisa.uk/documents/scheduleb.pdf) and the related policy for assessing compliance with the Qualifying Standard's Data Security and Protection Toolkit (DSPT) requirement (https://regisa.uk/documents/AcceptableDSPTstatusPolicy.pdf).

In particular, this document sets out the supplementary assurance information requirements for membership of the Regional ISA where membership is associated with access to the Thames Valley and Surrey (TVS) Shared Care Record and analytics capabilities.

The information requested as part of this document supports the assertions made by Regional ISA applicant organisations in their related Qualifying Standard submission.

These supplementary requirements have been mandated by the Information Governance Steering Group (IGSG) that oversees the Regional ISA (https://www.regisa.uk/documents/annex1.pdf).

Where answers to assurance requests do not apply to the entirety of an organisation's operations the assurance provided can be made specific to the health and care activity that your organisation will be involved in and to the part of your organisation, staff and suppliers that directy relate to your participation in the Regional ISA.

This document takes effect from 12th March 2024 and expires on the 30th April 2028.

Version 1 (draft).

Next Steps

Please complete this checklist and, where possible, supply evidence to support statements made. This evidence may include copies of or hyperlinks to documents. When completing the checklist:

- For simple requests and closed questions such as "*Registered name of the legal entity*", "*1. Does the organisation have an in date Cyber Essentials/Cyber Essentials Plus compliance certificate?*" and "*8. Is the organisation registered for the DSPT with a submission covering the current DSPT timeframe?*" please just add your response directly after question itself.
- Where requests are likely to require more detailed information in your response the question/request is accompanied by an expandable box that will allow longer answers and that can be used to supply attachments.

The completed checklist should be sent to the person or team that is managing your sign up to the Regional ISA.

Once your application has been approved, Regional ISA schedules will be issued to your authorised signatory my means of the Adobe Sign system.

Privacy

When completing the checklist, please note that:

1. The purpose of the request is to allow the Regional ISA Administrator to manage your organisation's application to join (or renewal of its membership of) the Regional ISA;
    a. The personal information that is requested as part of the "General" section of this document is only used for the above purpose
    b. If your organisation is or becomes a member of the Regional ISA, then section 18.5 of the Regional ISA master agreement requires your organisation to "*ensure that the Administrator is made aware of the details of and any changes to the individuals holding the roles and their respective contact information*"
    c. Questions regarding personal data captured as part of the above purpose are to be addressed to the Regional ISA Administrator; and
2. Where supporting attachments provided by you include the names of individuals this information is kept confidential to the sign-up and renewal processes and is deleted when the lead controller for the arrangements has either:
    a. Confirmed that the organisation adequately satisfies the Qualifying Standard, or
    b. Determined (together with IGSG) that the organisation cannot be signed-up to, or existing membership of the Regional ISA cannot be renewed.

General

Registered name of the legal entity:

Trading name if different to the above:

Registered address:

NHS Organisation Data Service (ODS) registration number:
Company registration number if a limited company:
Charity registration number if a registered charity:

IG Contact Details

Senior Information Risk Owner (SIRO)

Name:
Role within the organisation:
Email address:

Caldicott Guardian (or equivalent data subject representative)

Name:
Role within the organisation:
Email address:

Data Protection Officer (DPO) or equivalent

Name:
Role within the organisation:
Email address:

Head of Information Governance

Name:
Role within the organisation:
Email address:

Authorised signatory for Information Governance matters

Name:
Role within the organisation:
Email address (this cannot be a generic mailbox):

Assurances

Registration and Certification

Cyber Essentials/Cyber Essentials Plus

1. Does the organisation have an in date Cyber Essentials/Cyber Essentials Plus compliance certificate?
    a. If yes, what is the certificate number:
    b. If yes, please provide a copy of the current certificate:

Information Commissioner's Office (ICO)

2. ICO Registration Number:
3. ICO registration expiry date:
4. Is the registered organisation or any affiliate or subsidiary organisations covered by this registration currently under ICO investigation?
    a. If so, please provide details below:

5. Have the registered organisation or any affiliate or subsidiary organisations covered by this registration previously been the subject of ICO enforcement action?
    a. If so, please provide details below:

ISO27001

6. If applicable, does the organisation have an in date ISO27001 certificate?
7. If yes, does the certificate cover your organisation's activities that are relevant to this request?
    a. If yes, what is the certificate number:
    b. If yes, please provide a copy of the current certificate:

NHS Data Security and Protection Toolkit (DSPT) Compliance

8. Is the organisation registered for the DSPT with a submission covering the current DSPT timeframe?
    a. If yes, what is the organisation's latest DSPT status and the date it was achieved:

    b. Is the organisation subject to a mandatory external audit of the organisation's DSPT submission?
    c. If yes, please provide details of the external auditor and audit outcome:

9. Does the organisation have a current DSPT status of "Standards Met" or above?
10. Does the organisation have a current DSPT status of "Approaching Standards"?
    a. If yes, please provide us with a copy of the plan to achieve "Standards Met" that was agreed with NHS England:

11. Does the organisation have a current DSPT status of "Standards Not Met"? …
    a. If yes, please provide us with details of all DSPT criteria where the organisation did not achieve a satisfactory status:

    b. If yes, please also provide a copy of the organisation's plan to achieve "Standards Met":

12. If the organisation is not registered or does not have a submission covering the current DSPT timeframe please provide:
    a. a copy of the organisation's plan to register for DSPT and achieve "Standards Met"

b. please also set out the areas of DSPT that the organisation sees difficulty in demonstrating compliance with:

Further guidance is available at: https://www.dsptoolkit.nhs.uk/help .

13. Where organisations have a current DSPT status of 'Approaching Standards' please can they provide a copy of their DSPT Action Plan and confirmation of whether this has been approved by NHS Digital:

Ministry of Defence Secure Data Network Compliance

14. If applicable, does the organisation have a valid and in date MOD Secure Data Network compliance certificate?
15. If yes, does the assessment cover your organisation's activities that are relevant to this request?

Public Services Network (PSN) Compliance

16. Does the organisation have a valid and in date PSN connection compliance certificate?
17. If yes, does the certificate cover your organisation's activities that are relevant to this request?
18. If yes, what is the certification number:
19. If yes, please provide a copy of the current certificate:

Qualifying Standard Assurances

Please provide supporting evidence for the Qualifying Standard (https://www.regisa.uk/documents/scheduleb.pdf) topics set out below. Examples of the sort of documents that would satisfy the requirement are listed under each topic.

Where a criterion is covered by your organisation's Cyber Essentials, ISO and PSN certification please note this in your response. Additional evidence is not needed for these items.

Where supporting documentation relates to multiple criteria it only needs to be provided once and then it can be referenced against individual criteria that the documentation supports.

Where documentation and certification evidence does not exist, please provide a written assurance statement setting out how your organisation complies with the criterion concerned.

Audit and Quality Assurances

20. Staff access to confidential personal information is monitored and audited:

21. Procedures are in place to ensure the accuracy of service user (data subject) information on all systems that support the provision of care:

Examples of evidence:

- Audit Policy
- Confidentiality and Data Protection Policy or equivalent
- Data Quality Policy
- Extract from independent audit report

Confidentiality Assurances

22. All transfers of personal and sensitive information are conducted in a secure and confidential manner:

23. 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:

24. Where sharing of personal information is required beyond the boundaries of the data controller organisation, protocols governing the sharing are agreed with other organisations:

25. The confidentiality of service user information that is not involved in the process of providing direct care is protected through anonymisation techniques where appropriate:

Examples of evidence:

- Confidentiality and Data Protection Policy or equivalent
- Examples of information / data sharing agreements / DPIAs
- Link to Privacy Notice(s)
- Procedures / staff guidance for data sharing
- Procedures / staff guidance for handling information rights related requests
- Procedures / staff guidance for secure data transfer

Contracts

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

27. Do all staff, contractors and third parties have contracts containing confidentiality clauses?
28. Information governance and data protection responsibilities are outlined within employment contracts:

Examples of evidence:

- Extract from contracts with suppliers that process personal data
- Extract from staff contract of employment
- Relevant policies / audit reports

Disclosure

29. Individuals are informed about the proposed uses of their personal information and how they can exercise their rights:
    a. Please provide brief details of how you inform data subjects of their rights:

    b. Please supply link to your organisation's main Privacy Notice and to any Privacy Notice that covers the specific area of your business that this request relates to:

Governance

30. All new processes, services and systems are implemented in a controlled manner:

31. Background checks are carried out for staff, contractors and third parties given access to confidential and sensitive information:

32. 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:

33. 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:

34. There are approved and comprehensive Information Governance policies with associated strategies and/or improvement plans:

35. There are documented Information Governance incident management and reporting procedures:

Examples of evidence:

- Extract from relevant audit report
- Procedures for accreditation of activities
- Procedures for handling IG incidents
- Procedures for vetting of staff
- Relevant Policies
- Role Based Access Control Profiles
- Staff guidance

Security

36. All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures:

37. All new processes, services and systems are developed and implemented in a secure manner:

38. Operating and application information systems that store and process confidential and sensitive information that are used by the organisation have appropriate access control functionality, and documented and managed access rights are in place for all users of these systems:

39. The use of computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access:

40. Policies and procedures are in place to ensure that information technology networks operate securely:

41. Unauthorised access to the premises, equipment, records and other assets is prevented:

Examples include:

- Audit policy / procedures
- Audit report examples
- Bring Your Own Device (BYOD) Policy if applicable and if devices will be used to process shared data
- Cyber Essentials / Cyber Essentials Plus / ISO27001 Certificates
- Extract from relevant audit report
- Information and Cyber Security Policy or equivalent
- Network Security Policy or equivalent
- Procedures for accreditation of activities
- Procedures relating to network security
- Relevant Policies
- System level security policies

Training

42. All staff members are provided with appropriate training on information governance requirements:

43. Staff members are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users:

Examples include:

- Audit reports
- Details of IG training provided
- Relevant Policies
- Staff guidance