Wiltshire Single View

Information Sharing Agreement

Tier 1 Framework

DOCUMENT VERSION CONTROL			
Version	**Issue Date**	**Author / Organisation**	**Status / Amendment Summary**
0.1	15/12/2015	Debbie Mason-Smith Information Assurance Wiltshire Council	First Draft
0.2	March 2016	Debbie Mason-Smith Information Assurance Wiltshire Council	Final Draft with amendments to multiple sections following review and comment
1.0	May 2016	Debbie Mason-Smith Information Assurance Wiltshire Council	Section 4: Broader description of gateways to sharing decisions added. Decisions will be in consultation with IG Partners made clearer. Section 5: Data Controller, IG Lead, Head of IT roles, responsibilities and Information Management operating model updated. FOI handling statement added. Section 6: Information Security Design Assurance – change stored data statement. Appendix C: Tier 2 Template updated Issued for Approval Sign Off
Document Approval Body(ies): Single View Information Governance Board Single View Programme Board			
Document Review Date: December 2017			

Contents

1. Parties to Wiltshire Single View Tier 1 Information Sharing Agreement

This Tier 1 Information Sharing Framework Agreement is between:

Wiltshire Council Local Government Authority County Hall, Wiltshire Council, Bythesea Road, Trowbridge BA14 8JN	
DPA Registration No. Z1668953	Date of expiry/re-registration: Constantly renewed

Great Western Hospitals NHS Foundation Trust Great Western Hospital, Marlborough Road, Swindon SN3 6BB	
DPA Registration No. Z4953683	Date of expiry/re-registration: Constantly renewed

Royal United Hospitals Bath NHS Foundation Trust Combe Park, Bath BA1 3NG	
DPA Registration No. Z8889967	Date of expiry/re-registration: Constantly renewed

Salisbury NHS Foundation Trust Odstock Rd, Salisbury, Wiltshire SP2 8BJ	
DPA Registration No. Z6613850	Date of expiry/re-registration: Constantly renewed

Avon and Wiltshire Mental Health Partnership Jenner House, Langley Park Est, Chippenham, Wiltshire SN15 1GG	
DPA Registration No. Z6995243	Date of expiry/re-registration: Constantly renewed

South West Ambulance Service NHS Foundation Trust Bathwick St, Bath, Bath and North East Somerset BA2 6PU	
DPA Registration No. Z2767936	Date of expiry/re-registration: Constantly renewed

Wiltshire Clinical Commissioning Group Southgate House, Pans Lane, Devizes, SN10 5EQ	
DPA Registration No. Z3620444	Date of expiry/re-registration: Constantly renewed

Wiltshire Police London Road, Devizes, SN10 2DN	
DPA Registration No. Z4894491	Date of expiry/re-registration: Constantly renewed

Dorset & Wiltshire Fire and Rescue Authority Five Rivers Health and Wellbeing Centre, Hulse Road, Salisbury SP1 3NR	
DPA Registration No. ZA17 1812	Date of expiry/re-registration: Constantly renewed

For the latest DPA Date of expiry/re-registration, go to; ICO - Data Protection Public Register

Commencement of agreement
This agreement will commence on 1st July 2016.

Length of Agreement and Reviews
This Tier 1 Framework Agreement will remain in place as long as Single View Programme information sharing continues. The agreement will be reviewed every two years, or sooner, if significant changes to Information Legislation arise.

Tier 2 Information Sharing Agreements reflecting each instance of information sharing will be subject to Single View Information Governance Board Change Requests and Change Control in the event amendments are sought

2. Introduction and Purpose - Information Sharing Framework Agreement

Wiltshire Council is working in collaboration with Health partners, Police, Ambulance, and Fire to develop a new approach to electronic sharing data which will be known as Single View (SV). In essence, the patient, the customer and the resident are all one and the same and the opportunity to rationalise data systems and share information securely and collaboratively will provide secure data views to:

- Plan more effectively for the scale and type of public services required in Wiltshire
- Provide clinical continuity and improving health and wellbeing (The Better Care Plan)
- Save lives and protect the vulnerable (Police Service Delivery Plan)
- Improving the customer journey by providing efficient and effective services (Wiltshire Council Business Plan)

This Tier 1 document records the agreement of processes, procedures and obligations between all members of the Single View Governance Boards for the review and operation of Wiltshire Single View Product Case Data Sets. These Information Governance principles, processes and procedures have been designed to ensure robust considerations are given to fair and lawful, safe sharing of data in accordance with the Data Protection Act 1998 and all other legislation and guidance affecting the sharing and disclosure of personal information.

Individual information sharing request cases submitted under the Single View Programme, to support particular purposes, will be reviewed by the Single View Information Governance Board. These will be subject to change control. Where cases are agreed, the approval will be recorded in the Single View Information Sharing Register and full details will be documented in 'Tier 2' Information Sharing Agreement Appendices to this document.
A Tier 2 Information Sharing Agreement template can be referenced in Appendix C of this document.

3. Governance and Common Principles for the Sharing of Information

A Single View Information Governance Board (SVIGB) has been established to develop, implement and apply processes which will facilitate decisions for proposed Single View Product Cases to ensure fair and lawful sharing of information between partner organisations. In addition the SVIGB will assure suitable organisational processes and systems solutions for effective and secure handling of shared information, referencing HSCIC Information Governance Toolkit and ISO 27001. The SVIGB will inform the Single View Programme Board of decisions, issues and risks.

The agreed processes and responsibilities are documented in this Tier 1 Single View Information Sharing Framework Agreement. This will be supplemented by Tier 2 Single View Information Sharing Appendices which reflect specific arrangements for individual Product Cases.

Caldicott Guardians and Designated Officers

All statutory Health and Social Care organisations must have a Caldicott Guardian who, for the purposes of information sharing, will be the Designated Officer. Other organisations must nominate a Designated Officer.

Data Controller Responsibilities

Each partner organisation to this Tier 1 Single View Framework Agreement must fulfil Data Controller responsibilities to fully comply with Data Protection Act principles for the information they process as part of their business as usual operations.

The Data Protection Act recognises a 'Joint Data Controller' model of information sharing. "Joint" covers the situation where the determination is exercised by Data Controllers acting together, typically with written agreements setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied.

Single View Product Cases which are approved for specific purposes will be documented in individual Tier 2 Information Sharing Agreements which will set out the nature of the data to be shared, the legal basis for sharing, the security measures that will be in place and the storage methodology for that data. Some references may be made to common Tier 1 Agreement principles. This includes, but is not limited to:-

- Data Controllers together with their Single View Information Governance Board representatives must satisfy themselves that a lawful basis exists to share information when considering any product case requests for data held by their organisation as a deliverable to the Single View Programme and it's product case data sets.
- Onward Transmission of Personal Data: The disclosing organisation has responsibility to obtain assurance that the recipient organisation has adequate information governance controls in place. The disclosing organisation retains ownership of the data and any recipient may have a duty of confidence and must not disclose it without the consent of the disclosing organisation and service user, or use it for a secondary purpose.
- Organisations will ensure there is appropriate security for the safe and secure transportation or transmission of information, and will comply with, or move their practices towards alignment with, ISO/IEC 27001 Information Security Management systems.
- Health and Social Care organisations will comply with the relevant Caldicott requirements.
- Data quality assurance for data which may be shared and matched with that of other partners. Issues and Risks are to be raised as part of Product Case development and Information Governance review
- Staff Vetting arrangements for those handling confidential / sensitive data proportionate to protective marking classification for each Product Case

- Briefing staff about expectations set out in Tiers 1 and 2 of Single View Information Sharing Framework Agreements
- Training provision for information management and security best practice for staff granted access to Single View data sets
- Assessing Information Governance and Management maturity against recognised control framework (HSCIC IG Toolkit, ISO 27000 series) and driving improvements
- Maintain oversight of Third Party data processors information management and security practices based on contractual services agreements.
- Ensuring shared information disclosed under this framework agreement is not printed or copied, or shared with third parties or abused and is solely used for purposes defined in product case proposals.
- Data Controllers sharing personal data their organisation holds, about data subjects, for the purpose of the Single View Programme, will be responsible for their own or their employee's actions and will be liable for any breach of the Data Protection Act 1998.
- In the event that the disclosure of information between any of the Partners under this agreement is challenged by a person or organisation other than the Partners, any liability arising from any such challenge will be the responsibility of the Partner Organisation which disclosed the information. Staff Contracts of Employment and supporting Organisational Information Policies should clearly state the possibility of disciplinary action as a result of offences, non-compliance and poor handling of sensitive information.

4. Legal Principles and Powers applicable to Information Sharing

Each Product Case presented to the Single View Information Governance Board will be reviewed to examine its purpose and the extent to which Data Protection Act 1998 principles, Common Law and relevant Codes are met. Privacy Impact Assessments will be undertaken for each Product Case proposal, in consultation with Information Governance partners, to identify risks and mitigations, prior to approval from IG Programme Board to proceed with information sharing.

Tier 2 Information Sharing Agreements will set out the legal considerations and basis upon which decisions to share have been made.

Where the decision to share information is agreed, a record of the decision will be made in the Single View Information Sharing Agreement Register. A Tier 2 Information Sharing Agreement will be created detailing the specific information items, parties, sharing purpose, access and management arrangements. Measures will be put in place and monitored to ensure ongoing information management is robust and secure.

Fair Processing and Consent - Sharing Personal or Sensitive Personal Data
Existing Privacy Notices and nature of Data Subject Consent will be reviewed for data sources. Where existing arrangements are not adequate, the options include but may not be limited to:-

i) Identify an alternative statutory basis for sharing of information, for the specified purpose, between proposed parties. It may be possible to disclose personal information without consent if sharing is justified by application of other suitable criteria, (such as 'to protect vital interests of data subjects' or 'in substantial Public Interests') within the Data Protection Act and relevant Schedules, Examples include:

- Administration of justice
- Maintaining of public safety
- Apprehension of offenders
- Prevention of crime and disorder
- Detection of crime
- Protection of vulnerable members of the community

When judging the public interest, it is necessary to consider:

- Is the intended disclosure proportionate to the intended aim?
- What is the vulnerability of those who are at risk?
- What is the impact of disclosure likely to be on the individual to whom the shared information pertains?
- Is there another equally effective means of achieving the same aim?
- Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
- Is it necessary to disclose the information, to protect others?

The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject: Privacy Notices and Consent arrangements will reflect this.

Or

ii) Obtain explicit informed consent from data subjects to share their information for proposed purposes, to stated organisations, via a targeted communications exercise. The option of 'opt out' should be provided for data subjects unwilling to give consent and their records must be marked accordingly.

5. Information Management Arrangements

Access to Information – Data Subject Access Requests
Wiltshire Single View partners will adhere to Principle Six of the Data Protection Act which provides Data Subjects the right to access their processed information.
There are a number of exemptions to the normal rule of law. Under the provisions of Section 29(1) two exemptions exist: for the first principle of fairness and lawfulness, and to the data subjects right to access their personal data if to do so would prejudice the prevention & detection of crime, the apprehension or prosecution of offenders or the assessment and collection of any tax or duty. If these apply, there is no obligation even to inform the data subject of the processing. However, all processing must still be justified by reference to schedules 2 & 3 as appropriate. If it cannot, then the data cannot be processed lawfully irrespective of this exemption.
Section 29(3) and 35 may also dis-apply the non-disclosure provisions and enable data to be shared in appropriate circumstances. Relevant advice should be sought from Data Controller's subject matter experts before relying upon such exemptions.

In the event Single View partner organisations receive a Subject Access Request query for personal information held, each Partner Data Controller is responsible for responding appropriately to requests addressed to them and for providing information to the data subject to enable them to make appropriate requests to other Partners where appropriate. Information Governance procedures will be in place and followed at each partner organisation to correct any factual inaccuracies that may have been made processed information.

Freedom of information – Requests for Information
Single View partner organisations will have in place procedures to address Requests for Information in keeping with Freedom of Information Act 2000. Each partner will confirm and supply held information requested. If information is not held this will be confirmed to the applicant: a general statement informing him or her that the information requested may be held by another public authority is optional. Due to the transient nature of Single View product case information, formal Transfer of Requests between partner organisations is not considered appropriate.

Complaints relating to Disclosure of information
Single View partner organisations will have in place procedures to address complaints relating to the disclosure of information to Third Parties. Any complaints relating to the disclosure of information facilitated by Wiltshire Single View Programme will be reported to the Single View Information Governance Board.

Retention & Disposal of Information
Source data, (belonging to the partner organisations that originally collected it from data subjects), will be stored in individual source systems in line with their organisational Records Retention schedule.

Retention and Archive Disposition Dates for data collated and audit logs in the Single View System Solutions will be agreed between partner organisations in accordance with their retention schedules.

In the event a Product Case data set is no longer needed, this must be reported to the Single View Information Governance Board who will instruct IT Support to securely delete this content and cease refresh presentation to the Single View portal or cease other technical solutions implemented to share information.

Information Security Breaches - Incident Handling

Information Incident Definition
The following events are all considered to be information security incidents:

- Unauthorised access, or attempted unauthorised access, to systems or data;
- Deliberate and unauthorised denial of access to any system to authorised users;
- Theft or attempted theft of assets;
- Accidental or deliberate unauthorised disclosure, modification or destruction of information;
- Misuse of data;
- Misplacement of equipment, data, reports or media containing data;
- Compromise of cryptographic keys / materials;
- Introduction of unauthorised hardware or software to any systems in use by the Single View Programme.

Responsibilities and Information Incident Reporting
All partner staff handling Wiltshire Single View information have a personal responsibility to ensure the security of the information that the Programme processes in the conduct of its business activities. This relates not only to the systems that hold the information, devices used to access the information and personnel granted access but also the premises where information is stored and processed.

The Single View System will incorporate protective monitoring to deter, detect and support post incident event forensic investigations. In the event a partner identifies an information security incident or potential security incident / potential Single View system / process weakness that might lead to a security incident, it must be reported in writing to Wiltshire Council's Data Controller and member of the Single View Information Governance Board.

For instances of unauthorised or unlawful processing, loss, damage or destruction of Single View Product Case information reporting as soon as is practicable, in any case within one working day of identification. If it is judged the incident has the potential to cause risk to anyone's safety, financial loss or reputational damage to partner organisations, an initial and immediate verbal notification may be necessary. If the nature of the weakness, potential or actual incident is system related it may also be appropriate to inform Wiltshire Council's ICT Service Desk on 01225 718 718, who process Single View data, in order that appropriate technical steps can be taken immediately to help contain the incident.

The expectation on partners is that 'near miss incidents' will also be reported.

Wiltshire Council's Data Controller will ensure all information security breaches and incidents are raised with relevant members of the SV Information Governance Board.

Incident Response and Management
Where possible, partners will take immediate reasonable steps locally to contain any information incident impact that has arisen to support the overall management effort.

Wiltshire Council's Data Controller and Information Governance Lead will work in conjunction with partner organisations Information Governance Leads and Wiltshire Council Head of IT, as necessary, to co-ordinate the initial response to any information security incident from Single View. An initial assessment of the incident will be made to determine a management plan for the incident, including

- Identification of members for incident response 'team';
- Risk Assessment
- Containment and recovery actions
- Escalation / Notification to stakeholder parties of incident proportionate to the severity and risk of the incident
- Mobilisation of any necessary incident response 'team'.

The Incident Management Plan will be a bespoke response to the security incident and shall in addition to the above considerations include an assessment of whether there needs to be an investigation on a criminal basis. This will be documented as a record of actions taken and will be updated as effectiveness of actions are completed and evaluated. The record will be a source for post-incident written reports and recommendations of any remedial action for policy or process improvement.

Staff from all Single View partner organisations will be expected to provide relevant information to assist with any investigation that may follow a reported information security incident: in some instances they may be required to lead and undertake aspects of the investigation.

Where a crime is suspected, then it should be reported to the Police and any investigative action undertaken must not compromise formal investigative procedures.

Staff disciplinary investigations will be undertaken in relation to information security incidents where necessary and these investigations will involve HR and Legal services of affected partner organisations as appropriate.

Communications protocols and a coordinated communications plan for the security incident will be put in place resulting from collaboration between stakeholders, for example business partners, third parties, police, media and communications support.

Following risk assessment, significant information security incidents will be reported to the Information Commissioners Office. If the information security incident compromises health data a report will also be submitted to HSCIC using the SIRI Online Reporting Tool.

Identified risks arising from reported security incidents will be reflected in the SV Risk Register and suitable mitigation actions identified and implemented.

6. Information Security Design Assurance

Technical Design and System Level Security documents will be produced by the Programme Technical Work stream of the Single View Programme and made available for information assurance. The Single View Systems will be developed and tested based on Security Policy Framework, Standards and Good Practice Guides published by UK Government. Based on the Confidentiality, Integrity and Availability Impact Assessments, protection of Information will be designed into all components of the Single View Systems to prevent inappropriate access, modification, manipulation or deletion of data.

The partnership IG board proposes that we treat all product cases as containing personal sensitive data and treat it in line with guidance for such, ie, data will not be transmitted electronically unless it is protected by strong symmetric key cryptography: the recognised standard of Advanced Encryption Standard 256-bit will be applied commensurate with an Official-Sensitive data classification as defined in UK Government Classification Scheme of April 2014.

The Single View Systems Solution Design will wherever possible make use of trusted networks such as N3 and PSN to transfer data between partners and secure services to the cloud hosted platform with appropriate security. Where trusted network links are unavailable data transfers will be encrypted to AES256 encryption strength.

Single View Systems Hosting / Processing
Information held and processed by the Single View Systems will remain within the UK. Any proposed change to hosting / processing of information outside of the European Economic Area must be presented to SVIGB for risk and mitigating control assessment. This will ensure appropriate information safeguards are in place to satisfy the provision of the eighth principle of the Data Protection Act.

Stored Data
Data at rest will be stored in a location which provides controls which are commensurate with the information sensitivity and Business Impact Level, currently expected to not exceed Business Impact Level 3 / Official.

Data Flow
Data Flows will be determined for each individual Product Case and information assurance for the technical solution will be stated in Tier 2 Information Sharing Agreements. This will cover data extraction, secure data transport, data storage and audit trails for protective monitoring.

Systems Logical Access Control to Shared Data
To protect the confidentiality of data, access to product case data sets will only be granted to authorised users. The user names and roles will be notified via Information Governance representatives from the partner organisations.

A system login will be required where users must identify and authenticate themselves by use of a unique user identifier and strong password. Periodic password changes will be enforced together with lockout following a defined number of invalid login attempts. Additional means of authentication may be used in some instances, such as tokens. This will be determined within Technical Design and System Level Security applicable for specific product cases which will also take account of device types and internet browsers in use.

Following successful identification and authentication login, access to user account management and data sets, (as authorised for read, add, amend, delete), will be managed by Single View System roles and logical access controls. Information Security and Caldicott principles are to be observed, ie, the minimum necessary information will be shared, on a justified 'need to know' basis, consistent with the purpose for sharing.

The data and user details for individual Single View Product Cases will be covered within Tier 2 Information Sharing Agreements.

Protective Monitoring – Audit Logs
The Single View Systems will ensure forensic readiness is built into its design to minimize risks to integrity of data.

Key systems activities will be gathered and preserved: Data Extract, Transform and Load jobs, Additions, amendments and deletions to Organisations, User Accounts and Roles will be captured and recorded. The system will also record both successful and unsuccessful login attempts. In addition viewing, additions, amendments and deletions to Product Case Data Sets will be recorded.

The protective monitoring data will be available for IT to detect and deter information crime before it occurs and will be available to support any post-event Information Security Incident investigation by Information Governance.

Disaster Recovery / Business Continuity
The Single View Systems solution design will provide resilience and Disaster Recovery provision to ensure High Service Availability for delivery of the portal service to partners. The Single View Data Controllers, Information Governance Leads and Data Processor will work together to agree Business Continuity arrangements to ensure that services reliant on Single View Product Case data can continue to operate as normally as possible in the event of disruption or disaster.

All Business Continuity Plans shall be reviewed periodically and any impacting changes reported to the Single View Information Governance Board.

Second level Information Sharing Agreement
This Tier 1 Framework Agreement is not intended to stand alone as the only procedural document necessary to facilitate appropriate information sharing. A Tier 2 Information Sharing Agreement for individual projects will be incorporated into Product Case Specific Agreements where the sharing of personal data is a key element. These will be used to cover specific data flows where these would help identify the reason for the sharing, the legal basis, the methodology and security being applied, amongst other details.

7. Appendix A

Signatories: Single View Tier 1 Information Sharing Framework Agreement

By signing below, I agree on behalf of the organisation I represent to adhere to the principles and practices of this agreement in a manner compliant with my statutory responsibilities.
I understand that my organisation may withdraw from being a partner and signatory to this Agreement upon giving written notice to Head of Single View Programme, Wiltshire Council.

Please arrange **signature of this page and completion of Organisational Compliance Statement. Scan and return via email to:** Singleview.Programme@wiltshire.gov.uk.

Wiltshire Council Local Government Authority County Hall, Wiltshire Council, Bythesea Road, Trowbridge BA14 8JN
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Great Western Hospitals NHS Foundation Trust Great Western Hospital, Marlborough Road, Swindon SN3 6BB
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Royal United Hospitals Bath NHS Foundation Trust Combe Park, Bath BA1 3NG
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Salisbury NHS Foundation Trust Odstock Rd, Salisbury, Wiltshire SP2 8BJ
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Signatories to the Single View Tier 1 Information Sharing Framework Agreement *continued:*

Avon and Wiltshire Mental Health Partnership Jenner House, Langley Park Est, Chippenham, Wiltshire SN15 1GG
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

South West Ambulance Service NHS Foundation Trust Bathwick St, Bath, Bath and North East Somerset BA2 6PU
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Wiltshire Clinical Commissioning Group Southgate House, Pans Lane, Devizes, SN10 5EQ
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:
Date:

Wiltshire Police London Road, Devizes, SN10 2DN
Name of signatory (CEO, SIRO or delegated lead): ACO Zoe Durrant
Position: Assistant Chief Officer - SIRO
Signature:
Date:

Dorset & Wiltshire Fire and Rescue Authority Five Rivers Health and Wellbeing Centre, Hulse Road, Salisbury SP1 3NR
Name of signatory (CEO, SIRO or delegated lead):
Position:
Signature:

8. Appendix B

Signatories: Organisational Compliance Statement
Single View Tier 1 Information Sharing Framework Agreement

Please indicate the status of Policies, Processes and Procedures for your Organisation in relation to this Information Sharing Agreement and the associated activities.

This signed Compliance Statement must be completed, signed, scanned and returned via email with the Single View Information Sharing Framework Agreement Signatory Page. Each signatory must store a copy of their own statement and be able to provide it to another signatory on request.

Organisational responsibilities:

Organisation Name & Postal Address:	
Activity area	**Comments: In Place? / In Progress - target implementation date?**
Keeping Data Subjects informed	
▪ Active provision of information to patients/service users of the purposes to which information about them may be put and to whom it may be disclosed.	
▪ Publicise and implement processes to provide access to records to Data Subjects on request.	
Provide choice for Data Subjects	
▪ Have policy covering consent to use information and respond to any specific requests made by subjects with regard to handling their information.	
Protect information	
▪ Have documented policy and processes to check the accuracy and clarity of data both with the subject and on information systems.	
▪ Protect the confidentiality and security of data in any form, during collection, storage and sharing with appropriate security arrangements (moving to general compliance with ISO27000 Information Security Management standard) – via relevant policy, process and staff guidance on handling information. ▪ Have adequate facilities to encrypt data sent via email, placed on removable media, or stored on mobile devices.	
▪ Documented policy and process relating to retention and disposal of information.	
▪ Ensure contractual arrangements with staff (employment terms), contractors and other suppliers/individuals handling identifiable information contain reference to confidentiality / non-disclosure.	

▪ Provide education and training to all staff on the safe handling of personal data including sharing/disclosing information. ▪ Control access to shared information on the 'need to know basis'. Ensure timely notification of leavers with access to Single View Product Case Data Sets to Wiltshire Council's Data Controller and representative at Single View Information Governance Board for account deletion instructions to Head of IT.	
▪ Complete and maintain a Data Protection notification detailing all sources, subjects, purposes and disclosures relevant to their function and partnerships under any agreement.	
Monitoring	
• Have incident and risk reporting arrangements that incorporate information related issues. • Audit & assess security of information flows and information systems. • Perform regular (at least annual) assessments and audits of organisational compliance with legislation and regulation on processing personal information.	

I the undersigned certify that the personal data being received will not be disclosed to unauthorised persons. The data and their purposes of use are notified under the Data Protection Act 1998 and my organisation/company is committed to compliance with the Data Protection Principles through applying the activities stated in the Tier 1 Information Sharing Agreement and above.

Authorised Signatory Name	
Position	
Signature	
Date	

9. Appendix C:Tier 2 Single View Information Sharing Agreement Template

10. Appendix D: Glossary of terms used

Tier 1 Information Sharing Agreement: a tier 1 agreement is an overarching document designed to establish common purposes, commitments and general principles for sharing information, and for complying with the Data Protection Act 1998.

Tier 2 Information Sharing agreement: aims to set out the purposes and principles for a specific information sharing instance associated with a specific project and with defined fields of the information to be shared and will list parties to whom it is intended to share information.

Data Controller: a person fulfilling an organisation's role who, (either alone or jointly or in common with other persons), determines the purposes for which and directs the manner in which any personal data are, or are to be, processed.

Data Processor: In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors are not directly subject to the Data Protection Act, but the Information Commissioner recommends that organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing and a written contract (detailing the information governance requirements) must be in place to ensure compliance with principle 7 of the Data Protection Act.

Data Processing: obtaining, recording or holding information or carrying out any operation or set of operations on that data.

Third Party: Third parties are those individuals or organisations other than the members of the Single View Information Sharing Agreement.

Caldicott Guardian: A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to professionals and staff.

Data Subject: An individual to whom data information relates.

Personal Data / Information: is defined within the Data Protection Act 1998 and means information which relate to a living individual who can be identified;

From those data, or From those data and other information which is in the possession of, or is likely to come into the possession, of the data controller

Sensitive Personal Data / Information: Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual.

Common Law Duty of Confidentiality: Common Law is the law of precedent. It is not written down and relies on the application of the findings in previous Court cases decided by judges. The Common Law Duty of Confidentiality therefore means that it has been established that, when there is an expectation of confidentiality between two parties (when information is more than just trivial or unimportant), in this case between the Health Professional and the Patient that confidence will not generally be broken without the explicit consent of the patient. In practice all patient information, whether held on paper, computer, video or audio tape, or even when it is simply held in the memory of a Health Professional, must not normally be disclosed to a third party without the consent of the patient.

Specified 'Purpose': The Data Protection Act stipulates that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Consent: The Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defines consent as "…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". For consent to be valid, it must be voluntary and informed, and the person consenting must have the capacity to make the decision

Implied Consent: Implied consent is given when an individual takes some action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, e.g. nodding their head. The consent must also be informed, the data subject must know, in other words, what are the proposed uses or disclosures of personal data, to whom it is being disclosed and that they have the right to object.

Explicit Consent: Explicit consent is given by a patient agreeing actively, usually orally or in writing, to a particular use or disclosure of information. The person consenting should be clear on the purposes of the processing and with whom the information will be shared. The consent must also be informed, the data subject must know, in other words, what are the proposed uses or disclosures of personal data, to whom it is being disclosed and that they have the right to object.

Anonymised data: is Data rendered into a form which it is not possible to identify an individual.

Pseudonymised data: is Data which has been given a unique identifier, which does not reveal a person's 'real world' identity. It is still considered 'personal data' within the definition of the Data Protection Act 1998, but appropriate management of the 'key' to reverse the pseudonymisation, means that disclosure should not breach the 'common law duty of confidentiality', where the recipient party does not and will not have the key to reverse the pseudonym.

Subject Access: the individual's right to obtain a copy of information held about them.

HSCIC Information Governance Toolkit: The IG Toolkit is an online system which allows NHS organisations, and other organisations processing health data to assess themselves against Department of Health Information Governance policies and standards. It also provides a score viewing facility to allow others to see the capability maturity in information governance for all subscribing organisations.

ISO 270001: ISO 27001:2013 is an information security standard that was published in September 2013 by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). It is a specification for an Information Security Management System (ISMS).