TVS SDE Glossary

Terms and plain English definitions

About the TVS SDE

Secure Data Environment (SDE)	A secure setting where approved users can access and analyse health and care data for approved purposes. Data remains protected within the environment and cannot be freely downloaded or copied.
TVS SDE	The Thames Valley and Surrey Secure Data Environment provides secure access to health and care data for approved research, planning and innovation projects.
Data Access Request Form (DARF)	The application form used to request access to data within the TVS SDE. Applicants provide details about their project, data requirements, approvals, and expected benefits.
Dataset Menu	A catalogue that helps applicants identify and specify the types of data they need for their proposed work.
Data Use Register	A publicly available record of projects approved to use data through the TVS SDE. It supports transparency about how health and care data is being used.
Analysis Environment	The secure workspace within the TVS SDE where approved users analyse data.
Processing Environment	The secure area where data can be prepared, linked or transformed before it is made available for analysis.

Data and Technical

Aggregated data	Data that has been grouped or summarised so that the information relates to groups of people rather than individual records.
Record-level data (or row-level data)	Information held as individual records rather than grouped summaries. Access is only provided where appropriate approvals and safeguards are in place.
Identifiable data	Data that includes details which directly identify a person, such as their name, address, date of birth or NHS number, or that could readily be combined with other information to identify them
Deidentified data	Data from which the details that directly identify a person, such as name, address and NHS number, have been removed before the data is made available in the TVS SDE.
Free-text data	Information written in narrative form, such as clinical notes, letters and reports, rather than information held in structured fields or codes.
Coded and numeric data	Information recorded using standard codes, categories, dates or numbers, rather than narrative text.

Medical imaging data	Clinical images such as X-rays, CT scans, MRI scans and ultrasound images.
Metadata	Information that describes a dataset, rather than the data itself. For example, metadata may explain what the dataset contains, where it came from, when it was last updated, what fields are included, and any rules or restrictions for using it.
Data linkage	The secure process of combining information from different datasets that relates to the same person, service or event.
Data refresh	An update to a dataset so that it includes newer or additional information.
Reidentification	The process of connecting deidentified data back to an identifiable person. This is prohibited under the Data Access Agreement, and the TVS SDE's controls (no access to identifying details, no downloading of data, and checking of all outputs) are designed to prevent it.
Data Minimisation	An important data protection principle that means only the data needed for an approved project should be made available in the TVS SDE. This helps reduce privacy risks by avoiding unnecessary use of personal information.
Data asset	A set of data that is managed as a resource and can be used for approved purposes, such as research, planning or service improvement.
Virtual machine (VM)	A secure, software-based computer provided within the SDE for approved users to carry out their work.
Natural Language Processing (NLP)	A type of computing that can analyse and interpret written language, such as information in clinical notes or reports.
Data ingress	The controlled transfer of data into the secure environment.
Data egress	The controlled release of approved data or results from the secure environment.
Data transformation	Changing data into a different structure, format or standard so that it can be used for an approved purpose.
Data specification	A detailed description of the data needed for a project, including the required fields, population, time period and any inclusion or exclusion criteria.

Research and approvals

Research database	A structured collection of data that has been reviewed and given ethical approval as a research database by a Research Ethics Committee (REC) or another independent ethics body. It may be used for future approved research, subject to the conditions of that approval and any relevant governance, legal and ethical requirements.
Patient and Public Involvement and Engagement (PPIE)	Activities that involve patients and members of the public in shaping, reviewing or informing projects that use health and care data.
Research Ethics Committee (REC)	An independent committee that reviews research proposals to consider whether they are ethically appropriate.

Health Research Authority (HRA)	The organisation that helps protect and promote the interests of patients and the public in health and social care research in England.
Confidentiality Advisory Group (CAG)	An independent group that provides expert advice to the Health Research Authority (HRA) and The Secretary of State for Health and Social Care on the use of confidential patient information in specific circumstances.

Governance

Five Safes Framework	A framework used to assess whether data can be accessed and used safely. It considers Safe People, Safe Projects, Safe Data, Safe Settings and Safe Outputs.
Safe People	Approved users, working for an approved User Organisation, who have the appropriate identity checks, training, skills and authority to access data. The approval of organisations and users is managed within the Network Registration Service.
Safe Projects	Projects with a clear purpose, expected public benefit and appropriate legal and ethical approvals.
Safe Data	Data that has been prepared and protected to reduce privacy risks while remaining useful for the approved purpose.
Safe Settings	Secure technical and organisational arrangements that control how data can be accessed and used.
Safe Outputs	Results that are checked before leaving the secure environment to make sure they do not disclose information about individuals.
Information Governance (IG)	The rules, responsibilities and processes used to ensure that information is handled lawfully, securely and appropriately.
Legal basis	The lawful reason that allows personal data to be processed for a particular purpose.
Common law duty of confidentiality	The legal duty to protect information given in confidence and only use or disclose it where there is an appropriate justification.
Section 251	Section 251 of the NHS Act 2006 allows confidential patient information to be used without individual consent for approved purposes, where seeking consent is not practicable and strict safeguards are in place. Applications are reviewed by the Confidentiality Advisory Group (CAG) and approved by the Health Research Authority on behalf of the Secretary of State. The TVS SDE holds Section 251 support for flow of confidential patient information into the SDE for linkage and application of the National Data Opt-Out, prior to de-identification and provision of deidentified data to Users
National Data Opt-Out	A choice that allows people in England to opt out of their confidential patient information being used for purposes beyond their individual care, such as research and planning. Where it applies, the TVS SDE must check and respect this choice before data is used.
TVS SDE Local Opt-Out	A choice that allows people in the Thames Valley and Surrey area to tell us if they do not want their confidential patient information to be used through the TVS SDE for purposes such as research, planning or service improvement.

	Where this applies, we will respect that choice before data is made available in the SDE.
Data controller	The organisation that decides why and how personal data is processed.
Data processor	An organisation that processes personal data on behalf of a data controller and under the controller's instructions.
Data Provider/Partner	An NHS organisation that contributes data to the TVS SDE. Data providers remain responsible for their data and take part in approving how it is used.
Joint Controller	Joint controllership means two or more organisations jointly decide why personal data is used and how it is processed. The key distinction is shared decision-making, rather than simply sharing data or working together. A processor acts on a controller's instructions; joint controllers jointly determine the purposes and means of the processing
Service and data Access Review Committee (SARC)	The committee that reviews every application to use data in the TVS SDE against the Five Safes and the public benefit test before access is granted. It includes [public / data provider / IG] members.
Data Access Agreement (DAA)	A formal agreement setting out the responsibilities, conditions and controls that apply when data is accessed through the TVS SDE.
Data Access Framework Agreement (DAFA)	An overarching agreement between the TVS SDE and an organisation that expects to carry out several projects. It sets out the standard legal terms once, so that each project then needs only a project-specific Statement of Work. Project-level approval via SARC is still required.
Host Organisation	Oxford University Hospitals NHS Foundation Trust, which runs the TVS SDE on behalf of the partner NHS organisations and employs the team. The TVS SDE isn't a separate legal entity, so OUH signs the DAA or DAFA with a User Organisation.
User Organisation	The organisation that is responsible for the individual researchers accessing data in the SDE. They would sign the DAA and accept this responsibility through the terms included in this.
Approved Users	A named person who works for, or on behalf of, an organisation that has signed a Data Access Agreement with the TVS SDE. The organisation decides which of its people may access the data, and only for the approved project. Each person must accept the Terms of Use before they are given access.
Network Registration Service	A process for registering and checking users and their organisations against common requirements across the NHS SDE Network, designed to avoid repeating the same checks for different SDEs.

Quick acronym list

AE	Analysis Environment
AI	Artificial Intelligence
CAG	Confidentiality Advisory Group
DAA	Data Access Agreement
DARF	Data Access Request Form
DPIA	Data Protection Impact Assessment
DSA	Data Sharing Agreement
EPR	Electronic Patient Record
FDP	Federated Data Platform
HRA	Health Research Authority
IG	Information Governance
ISMS	Information Security Management System
KYC	Know Your Customer
MFA	Multi-Factor Authentication
NDOO	National Data Opt-Out
NLP	Natural Language Processing
OMOP	Observational Medical Outcomes Partnership
PE	Processing Environment
PPIE	Patient and Public Involvement and Engagement
REC	Research Ethics Committee
SARC	Services and data Access Review Committee
SATRE	Standardised Architecture for Trusted Research
SDE	Secure Data Environment
SOP	Standard Operating Procedure
TRE	Trusted Research Environment
TVS	Thames Valley and Surrey
VM	Virtual Machine