Reference: FOI.ICB-2526/404

Subject: Secure Data Environment Software Platforms and Systems

I can confirm that the ICB does hold the information requested; please see responses below:

QUESTION	RESPONSE
I would be grateful if you could provide information regarding the software platforms and systems currently used by your Secure Data Environment for health data analysis and research.	
1. Analytical Platforms and Tools What software platforms or tools does your organisation currently use for: • Creating dashboards and data visualisation • Analytics and reporting (including business intelligence tools) • Statistical and analytical environments (e.g., R, Python, or similar) • Advanced analytics including machine learning or AI applications For each platform/tool identified, please provide: • Platform/tool name • Primary use case	**Creating dashboards and data visualisation/ Analytics and reporting (including business intelligence tools)** The South West Secure Data Environment (SWSDE) does not currently provide dashboarding or data visualisation for operational or business intelligence purposes. The environment is designed exclusively for research and analytical use within secure research workspaces rather than organisational performance reporting. SWSDE is hosted on a separate local cloud tenancy (see next section) to all other ICB functions. **Platform/tool name:** Not applicable as a core SWSDE function Note as part of monthly programme reporting SWSDE are required to submit a report in a Microsoft Excel Template with information gathered from MS Lists.

• Approximate year of adoption	**Statistical and analytical environments (e.g., R, Python, or similar)** Researchers access SWSDE via a secure Azure Virtual Desktop hosted within a local Microsoft Azure tenant to conduct analysis. Tooling within each workspace is provisioned based on research requirements, with open-source tools available as standard. **Platform/tool name**: Azure Virtual Desktop (within standalone Azure tenant), R, GitHub, other open-source analytical tooling (on request on a project by project basis) **Primary use case**: Secure statistical analysis and research computing within isolated Trusted Research Environment (TRE) workspaces **Approximate year of adoption**: 2025. **Advanced analytics including machine learning or AI applications** Advanced analytics capabilities are enabled through azure native tooling supporting large-scale data processing and data science within the SWSDE. These are only stepped up as and when a project requires it. . **Platform/tool name:** Azure Databricks, Native Microsoft Azure modules such as Azure ML. **Primary use case:** Data processing, cataloguing, advanced analytics and machine learning experimentation in a secure research environment. **Approximate year of adoption:** 2025

2. Research Data Environments What systems or platforms does your organisation use to provide: • Secure data environments (SDEs) or Trusted Research Environments (TREs) for approved research • Access to health data for researchers • Computational resources for data analysis For each system/platform, please specify: • System/platform name • Whether provided centrally or distributed across multiple sites • Cloud infrastructure provider if applicable (e.g., AWS, Azure, Google Cloud, other, or on-premise)	BNSSG ICB hosts SWSDE. This operates within a dedicated local Microsoft Azure tenant and enables researchers to access and analyse data within controlled, isolated research workspaces. **Secure data environments / trusted research environments** A Secure data environment (SDE) for approved research **System/platform name**: South West Secure Data Environment (SWSDE), configured to the DARE UK SATRE (standard architecture for trusted research environment) standards, aligning to the Azure Trusted Research Environment (TRE) model. **Provision model**: The platform that is jointly controlled by regional NHS organisations, but hosted in a single NHS organisation. The All components within the segmented management, SDE and TRE domains are deployed using secure baseline configurations. Azure-native services, such as Key Vault, Storage Accounts, SQL Databases, Databricks, and Azure Kubernetes clusters. Management of infrastructure is handled ensuring version-controlled, automated deployments through GitHub Actions and Azure DevOps, preventing configuration drift. **Cloud infrastructure provide**r: Microsoft Azure. **Provision model**: Hosted in on organisation. **Infrastructure**: Physically based in a Microsoft UK South data centres. **Access to health data for researchers** **System/platform name:** Azure virtual Desktop **Provision model**: Hosted in a single organisation, project approval

	managed via regional data access committee. **Cloud infrastructure provider:** Microsoft Azure **Computational resources for data analysis** **System/platform name:** Flexible compute and virtual machines via Azure, configured based on project requirements to control cost.
3. Data Processing and Linkage What software or systems does your organisation use for: • Data extraction, transformation, and loading (ETL) from source systems • Linking datasets from different sources • Data quality checks and curation Please specify: • System/platform name • Primary function • Whether provided in-house or by external supplier	The SWSDE operates a structured cloud-native data pipeline to support secure ingestion, transformation, linkage and curation of research datasets. All processing takes place within the controlled SDE architecture. **Data extraction, transformation, and loading (ETL) from source systems** **System/platform name**: Azure Data Factory with Self Hosted Integration Runtime, supported by Azure Databricks **Primary function:** Orchestrated data ingestion from source systems, manual transformation of raw data into structured research-ready datasets, and movement of data across controlled storage zones. **Provision model:** Core platform capability delivered within the SWSDE environment hosted by BNSSG, implemented with regional SDE partners. **Linking datasets from different sources** **System/platform name**: As above. **Primary function**: Secure linkage and transformation of datasets within the Safe Haven zone, including pseudonymisation and

	project-specific dataset preparation in line with governance controls **Provision model**: Core platform capability delivered within the SWSDE Azure environment. **Data quality checks and curation** **System/platform name:** As above. Platform separation layers including Raw, Cleansed, Conformed and Curated zones in Azure. **Primary function**: Data validation, quality assurance, transformation, standardisation and curation to create analysis-ready research datasets **Provision model:** Core platform capability delivered within the SWSDE Azure environment, implemented in partnership with core SWSDE partners (University of Exeter, Bristol) an external delivery suppliers where additional capacity is required (Simpsons Associates) for technical expertise. Processing activities are undertaken within a standalone Microsoft Azure tenant and aligned to Secure Data Environment. The environment is designed exclusively for research use and incorporates audit logging, access controls and policy-driven data movement throughout the pipeline.
4. Privacy Protection and Data Security What software or systems does your organisation use for: • Privacy-enhancing technologies or privacy protection of research data • Anonymisation or pseudonymisation	The SWSDE is designed around the Five Safes framework and incorporates layered technical and procedural controls to protect research data, prevent unauthorised disclosure and manage re-identification risk. **Privacy-enhancing technologies or privacy protection of**

• Detection and prevention of re-identification risks or data leakage Please specify: • Technology/platform name or type • Primary use case (e.g., data at rest, data in transit, output checking) • Whether automated, manual, or combination	**research data** **Technology/platform name or type:** Microsoft Azure native security controls including Azure Firewall, Azure log monitoring, EntraID, Key Vault, Private Endpoints, Role Based Access Control, encryption at rest and in transit, and secure network segmentation within the SWSDE architecture **Primary use case**: Protection of data at rest and in transit, strict access control, network isolation, and prevention of unauthorised ingress or egress from Trusted Research Environments **Automation type:** Combination of automated enforcement through platform controls and manual governance oversight **Anonymisation or pseudonymisation** **Technology/platform name or type:** Azure Databricks transformation pipelines within Azure Safe Haven and TRE zones. **Primary use case:** Pseudonymisation, de-identification, and preparation of research-ready datasets prior to researcher access **Automation type:** Combination of automated transformation processes and manual governance approval aligned to data access approvals. **Detection and prevention of re-identification risks or data leakage** **Technology/platform name or type:** Controlled airlock mechanisms, output checking processes, audit logging and monitoring via Azure Log Analytics. **Primary use case:** Prevention of unauthorised data extraction, review and approval of researcher outputs prior to release, and monitoring of user activity within the

	TRE **Automation type:** Combination, automated logging and monitoring with mandatory manual output checking and disclosure control prior to data release.

The information provided in this response is accurate as of 6 March 2026 and has been approved for release by Seb Habibi, Interim Chief Transformation and Digital Officer for NHS Bristol, North Somerset and South Gloucestershire ICB.