NSW Health

Minimum requirements for Secure Access Environments

## CONTENTS

# 1. BACKGROUND

**An improved approach to sharing NSW Health Unit Record Data that contains health information for a secondary purpose:**

- **Enhancing safe data sharing:** NSW Health is introducing changes that increase the use of Secure Access Environments (SAEs) for sharing specific data outside of the NSW Health domain.
- **Adapting to a changing landscape:** In Australia, cyber and privacy risks are on the rise, particularly in the context of health data. In response, NSW Health is adopting SAEs as an additional safeguard for sensitive information and patient privacy, while enabling analytics, innovation, and collaboration.
- **Embracing collaboration:** We invite all platforms to provide supporting documentation demonstrating adherence to the NSW Health minimum requirements for Secure Access Environments.

## 1.1. About this document

This document is for those seeking guidance on Secure Access Environments, including when to use them and which environments are suitable. It also provides details on NSW Health's Minimum Requirements and the process for submitting a document addressing those requirements.

This document supports and clarifies what is acceptable secure storage in the following policy directives: PD2015_037: “Disclosure of Unit Record Data for Research or Management of Health Services” [1] and PD2018_001: “Disclosure of unit record data by Local Health Districts for research or contractor services” [2].

## 1.2. Key definitions

| | |
|---|---|
| **Secondary Purpose** | Secondary purpose or use[1] of data refers to any application of data beyond the reason for which they were first collected (known as the primary use or purpose). For example, the primary use of data collected to treat a patient in a hospital is to provide the patient with the care they need in that hospital episode; a secondary use could be to aggregate patients’ data to compare hospital performance across Australia. |
| **Secure Access Environment (SAE)** | Secure Access Environments (SAEs) provide a single location to store, access and analyse health datasets. The data and analytical tools are all in one place, a ‘one stop shop’ for data access and analysis in a securely managed environment. SAEs help streamline access to data and allow multiple people to work on a single project, while increasing the confidence of patients |

[1] https://www.aihw.gov.au/getmedia/57ed4b65-5919-43ce-bb21-933ea9a8b012/aihw-aus-221-chapter-2-5.pdf.aspx

| | |
|---|---|
| | and data custodians that data will be kept safe. Use of SAEs helps ensure health data and information is accessible to those who need it, and the data is stored and used safely. |
| **Unit Record Data** | Electronic records of information that relate to the health of an individual. |

# 2. WHEN ARE SECURE ACCESS ENVIRONMENTS REQUIRED

NSW Health Approved Secure Access Environments will need to be used when:

- **Who**: People not employed by NSW Health (such as researchers, consultants, system partners) or NSW Health employees for which the purpose is not directly related to their role, require access to,
- **What**: NSW Health Unit Record Data that contains health information (meaning files with patient data e.g., spreadsheets, databases, SAS files, EMR records),
- **Why**: For a 'secondary purpose' (e.g., research, health service evaluation and planning). Excluding: secure transfers for mandatory reporting and data submissions (e.g., State, National and statutory reporting or submissions, GIPAA requests, Minimum Data Set submissions), directly related secondary purposes, primary purposes (e.g. providing care, transferring care, referrals), the provision of data to NSW Health,
- **Where**: Outside of NSW Health technology, information systems and assets.

# 3. CONTEXT AND RATIONALE

NSW Health routinely discloses data to authorised people for approved purposes, such as researchers, consultants, and system partners. For example, the CHeReL alone released over 2.85 billion records for more than 100 projects in 2021–22 [3].

When data is disclosed externally, it is often not possible to ensure where it goes, who can access it, what it is used for and whether it is destroyed after use. Historically, this has been managed through agreements, de-identification, and trust; however, the changing risk landscape means additional controls are required.

## 3.1. A changing landscape

- Cyber and privacy risks such as data breaches are increasing, with health data a prime target ( [4], [5], [6], [7], [8], [9], [10], [11] ).
- The growing ease by which “de-identified data” can be re-identified is a concern ( [12], [13], [14], [15], [16], [17] ).
- The consequences, such as damage to personal privacy, reputation and trust, and the associated costs of data breach response and applicable penalties are also increasing ( [18], [19], [20], [21], [22] ).

- These risks have sometimes resulted in a hesitancy to share data [23], and prompted legislation change, such as the introduction of a Mandatory Notification of Data Breach Scheme [24], and the international adoption across government and research of the Five Safes Risk Management Framework for data sharing ( [25], [15], [26], [27], [28], [29], [30], [31], [32], [33], [34] ) and the associated proliferation of Secure Access Environments, and wide recognition of the need for secure systems to project personal information [35], .

The threat landscape is constantly changing, and we need to change with it to ensure that data can continue to be shared safely.

### 3.1.1. Enabling and streamlining data sharing

It is important that data sharing and associated benefits, such as health service improvement, innovation and research continue despite the increasing risks. Accordingly, the Five Safes Risk Management Framework supports data custodians to decide if it is safe to share data and manage the associated risks. Under this framework, data sharing risks are managed independently and collectively across five dimensions:

- Safe Projects (ensuring the project is ethically and legally sound, authorised, and appropriate),
- Safe People (restricting access to authorised and trained individuals),
- Safe Data (anonymising or protecting data to prevent reidentification),
- Safe Settings (providing secure environments for data storage and use), and,
- Safe Outputs (ensuring that data outputs do not risk reidentification).

These safeguards collectively aim to balance data utility with privacy protection, allowing valuable research while minimizing the risk of compromising sensitive information. Secure Access Environments enable both the Safe Settings and Safe Outputs domains. It is important to note however that Secure Access Environment use does not negate the responsibility for, or change any of the associated processes or requirements for data sharing, such as data custodian authorisation and ethics approvals, which remain the same.

## 3.2. Safe settings: Appropriately safe and secure environments

Per the Five Safes, NSW Government agencies need to ensure data will only be accessed and used within an appropriately safe and secure environment [25]. This document was created to provide advice regarding what constitute an appropriate environment for both storage and analysis of sensitive data in the context of NSW Health data disclosures.

### 3.2.1. Defining a Secure Access Environment

In Australia, there isn't a standard definition or set of requirements for Secure Access Environments. Because there are many different environments, each with different technologies and uses, NSW Health has developed a set of Principles and Minimum Requirements to determine whether a Secure Access Environment is appropriately safe and secure. Principles based frameworks are used internationally for both Secure Access Environments and Information Security ( [36], [37] ) particularly the:

- Health Data Research UK Trusted Research Environment approach [38], and,
- Principles for data access within trusted research environments [39],

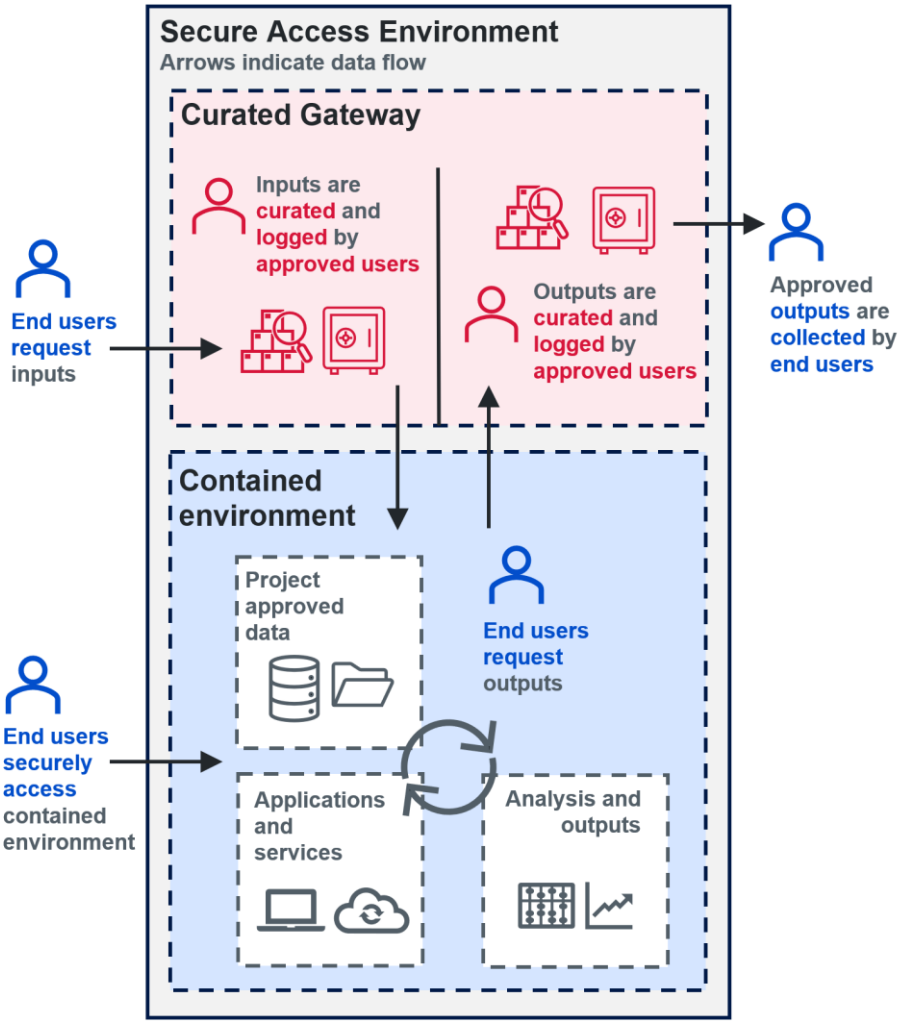
Internationally, Secure Access Environments are also known as Data Safe Havens, Secure Data Environments, Trusted Research Environments (TREs), clean rooms and Digital Research Environments (DREs). NSW Health adopted the term Secure Access Environments, which aligns with the AIHW [40].

The requirements were designed to be comprehensive and sensible yet generic enough to be applied to many types of SAEs and updated as needed to keep up with changing demands. It's important to note that these principles apply to the secure access environment itself and not necessarily to the organization that operates it.

### 3.2.2. Key principles of a Secure Access Environment

The five NSW Health principles of a Secure Access Environment are listed and illustrated in a simplified diagram below:

1. **Curated gateway**: a checkpoint for data and files moving in and out of the environment,
2. **Contained environment**: project data, tools and software are kept in a single space, separated by project (like a secure hotel with secure rooms)
3. **Secure platform**: the environment meets best-practice security standards,
4. **Analytics enabled**: the environment provides all the tools and resources analysts need,
5. **Platform governance**: the environment is well governed with clear roles and responsibilities.


Secure Access Environment
Arrows indicate data flow
Curated Gateway
Inputs are curated and logged by approved users
Outputs are curated and logged by approved users
End users request inputs
Approved outputs are collected by end users
Contained environment
Project approved data
End users request outputs
End users securely access contained environment
Applications and services
Analysis and outputs

## 3.3. Safe outputs: curation and review

A key component of a Secure Access Environment is a Curated Gateway, which provides a mechanism for facilitating "Safe Outputs". The aim is to ensure that any outputs approved for release are non-disclosive i.e., that reidentification cannot occur. Overlapping aspects of curation include ( [41], [42], [15] ):

- Statistical knowledge (e.g., checking for sufficient aggregation and disclosure control)
- Technical knowledge (e.g., checking for intentional or accidental data exfiltration)
- Domain knowledge (e.g., checking for sensitive data, such as vulnerable cohorts and communities, and ensuring expectations are met in reporting)
- Administrative (e.g., the outputs directly relate to the project approval and purpose).

Currently it is not possible to automate the curation process ( [43], [44] ).

### 3.3.1. Curation Models

Historically, curation by the data custodian or the Secure Access Environment has been the typical approach, however nominated user curation models (i.e. an authorised person in the project team curates the project outputs) to address the time and resource constraints with other curation models [45]. With a nominated user curation model there is the risk of data egress, however this is compensated by the audit functionality of the gateway.

*Curation models / levels*

| Curation Level | Key Benefit | Role Responsible | Approximate Risk Mitigation | Resources Required |
|---|---|---|---|---|
| 3. Custodian Curation | Greatest control | Data custodian(s) or their delegate(s), e.g., data stewards | Med - High | Staff (for curation) |
| 2.5 Hybrid Curation | Custodian(s) control can cease at an appropriate time | Custodian(s) and nominated project user(s) | Med - High | Staff (for curation) |
| 2. Trusted Independent Curation | Frees internal resources | Trusted independent curator(s), e.g., SAE platform staff | Med - High | Costs for curation services |
| 1. Nominated User Curation | Required for scale | Nominated project user(s) e.g., lead investigator | Low - Med | Staff (for audits) |
| 0. No Curation | No Resourcing | No curation is required after release e.g., Open Data | None | None |

# 4. IMPLEMENTATION CONSIDERATIONS

## 4.1. Community expectations

There is support and uptake from research institutions for Secure Access Environments. The Digital Health Cooperative Research Centre states the need for “Standardised methodologies and technologies that support secure research environments that preserve privacy and confidentiality” [46]. The ARDC SeRP project is a multi-institutional initiative that aims to deliver access to secure environments for data custodians and research users nationally [47].

## 4.2. Adapting to change

Parties that have typically had data disclosed directly to them in the past will need to factor in the cost of Secure Access Environments. Changes will be reflected in policy in early to mid-2024. In the interim, many Data Custodians will be implementing changes to ensure the benefits occur as soon as possible.

The use of Secure Access Environments is becoming the norm for many projects. End users will need to plan for the cost of the environment, including any requirements for long term archiving in their grant proposals or project budget. Each environment has its own pricing structure which depends on a multitude of factors, such as the number of users, performance required and software available. This means projects can pay for what they need. The cost of utilising these environments is far lower than the costs of a data breach: financial, reputational, and to patient privacy. Contact an approved environment to discuss pricing options.

# 5. ADDRESSING THE REQUIREMENTS

When a Secure Access Environment has provided sufficient evidence of adherence to the minimum requirements, they will be listed on the NSW Health website (which is anticipated to go live in Dec 2023): https://www.health.nsw.gov.au/data/sharing/Pages/secure-access-environments.aspx

To address the requirements, an authorised person from the organization operating the Secure Access Environment needs to complete the template (provided on the website above), clearly addressing how the environment meets or exceeds the minimum requirements detailed in the next section.

Any supporting documentation should be attached and addressed to the NSW Health Data Governance Reform Program: moh-datagovernance@health.nsw.gov.au

The submission will be appraised, and clarification sought if required. Comprehensive answers will facilitate a faster response.

## 5.1. NSW Health Data Governance Reform Contact Details

To submit a document addressing the minimum requirements, or for any general questions or comments, please email: moh-datagovernance@health.nsw.gov.au

# 6. THE MINIMUM REQUIREMENTS IN DETAIL

## 6.1. 1. Curated Gateway

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| a. All data and file movements (ingress and egress) occur via a curated gateway | A gateway is a checkpoint for file movements that helps prevent unauthorised ingress and egress and enables review and logging. In a curated gateway, there's a special area that only approved users can access, and they have permission to transfer files between the user and the external world. | Even authorised users can make mistakes or act maliciously. To reduce these risks, training and raising awareness about the importance of reviewing and curating outputs and conducting background checks can be beneficial. |
| b. Curation is facilitated by approved users and processes | Curation involves making decisions about what is allowed in or out of the Secure Access Environment. For outputs, this means checking for statistical disclosure control, ensuring alignment with approved purposes, checking for data exfiltration (unauthorised removal of data, e.g., through covert methods), and conducting context-specific checks. For inputs, it involves making sure no harmful files or unauthorized data is uploaded.<br>Approved users can be data custodians or stewards from NSW Health, system administrators or staff from the environment, or a nominated user within a project. The parties responsible for approving the data sharing activity (data custodian, ethics committee) determine who qualifies as an approved user. | Each Secure Access Environment has different methods for performing curation, and it is up to the approved users to understand their responsibilities and procedures. |
| c. The gateway supports multiple curation models (**Optional**) | Environments that offer different curation levels or models enable data custodians to apply varying degrees of control in line with the Five Safes framework. | Not all environments support multiple curation models, so it's an optional but desirable feature. |
| d. Gateway actions and approved files are immutably captured and logged | Files captured in the gateway must be immutable, meaning no user can modify or delete them, or their related log data, including information like dates, times, user details, comments, and decisions (like approval or denial) must also remain intact. It's crucial to preserve all gateway data for a specified period, even after the project concludes. | It's important to understand that while logging and auditing can't stop data breaches from happening, they do enable a response when a breach occurs. |

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| e. Curation occurs in a timely and transparent manner | Platform curators must minimise unreasonable delays when curating outputs, especially for short-term projects. Timely processing is essential for stakeholder satisfaction, particularly when rapid feedback is needed to progress a project. Processing time can vary depending on the level of curation required. Multiple curation models can help with scaling but should be balanced against the project risks. Transparency involves documenting the decision to approve or deny a request. | End user training in Statistical Disclosure Control and raising awareness about responsibilities means users are more equipped to request outputs that are likely to be approved the first time and produce outputs that require minimal effort to check. |

## 6.2. 2. Contained Environment

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| a. Data and files are contained within project workspaces for storage and analysis | All project data is kept and analysed exclusively within the Secure Access Environment. Additionally, access to data and files is divided or isolated in workspaces by project, like secure rooms in a secure hotel, each designated for a specific purpose. | Different curation models could allow end users take files out of the contained environment via the gateway. The fact that all outputs are recorded for auditing purposes provides a stronger incentive for users to follow the usage rules. |
| b. Project and role-based access controls are implemented | Only authorized users can access specific project workspaces and data. This is achieved by using control mechanisms like Active Directory groups to grant users access only to the roles and projects they are approved for. It's crucial to prevent users with access to multiple projects from moving data between projects or users. Role separation should be enforced, meaning if a user is given permissions to manage a project, those permissions should not automatically apply to other projects unless they have specific approval for those projects as well. | It's important to consider how permissions are managed for individuals with multiple roles and responsibilities. |
| c. Transparent platform architecture allowing the requirements to be verified | Provide technical documentation that explains how the environment is set up so that it can be checked to ensure it meets the necessary standards. This documentation should include a diagram that shows all the important parts of the system, making it clear that it meets the requirements. | There might be concerns about sharing detailed information due to intellectual property issues. In such cases, the provided documentation should still offer enough detail for assessment without revealing sensitive intellectual property. |

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| d. Cut, copy, and paste to or from the environment is prevented | The ability to cut, copy, and paste data in and out of the environment is blocked. This makes sure that data can only be transferred through the gateway. | Screenshots cannot be prevented however the volume of data that can be captured in this way is limited. |

## 6.3. 3. Secure Environment

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| a. Demonstrated adherence to a recognised information security and technology standard | Demonstrate adherence to at least one recognized industry information security and technology standard, such as those deemed suitable for an ONDC Accredited Data Service Provider application or eHealth NSW, including:<br>• eHealth NSW Privacy Security Assurance Framework (PSAF)<br>• Information Security Registered Assessor Program Assessment (IRAP)<br>• Information Security Management System (ISMS)<br>• Essential Eight Maturity Assessment<br>• Protective Security Policy Framework<br>• ISO27001:2013 Information Security Management<br>• NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organisations. | Accreditation and standards are not guarantees of security because configurations, environments, and threat models can change. For example, the discovery of new security vulnerabilities (zero-day exploits) can alter the security landscape. Regardless, adherence to these standards indicates that security is being well-managed.<br>Evidence of independent certification by an accredited certification body is provided, or, detailed supporting documentation of adherence can be considered on a case-by-case basis. |
| b. Security audits, testing, updates, and backups occur regularly; backups must not contravene the requirements | There's no exact definition of what "regular" means, but penetration testing, and audits should happen at least once a year. You should be able to provide evidence of these tests upon request, which should include any recommendations and actions taken as a result.<br>For Secure Access Environments, it's important to conduct two-way penetration testing. This means ensuring that data can't get out of the system is just as vital as preventing it from getting in.<br>Backups need to be planned cautiously so that they don't contravene any of these requirements, such as to prevent situations like | It's crucial to remember that security is an ongoing process, and regular audits, testing, and updates are key components of achieving it. |

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| | using a third-party service located overseas to handle backups.<br>Regular updates, including updating the software used by end users, are essential for maintaining security and offering users the latest features, and so that users do not need to do this themselves. | |
| c. Network access to and from the environment is prevented (except to provide required functionality) | The enclosed environment should be isolated from any communication or computer networks, which means it shouldn't have any connections to the internet or local networks. This is done to prevent unauthorized data transfers and reduce the potential for cyberattacks.<br>However, there's an exception for the curated gateway and any other essential functions needed for the Secure Access Environment. Any whitelisted addresses should be documented, with a strong reason for why they are allowed, and these permissions should be regularly reviewed for any changes. | It's important to note that the environment still needs internet connectivity for users to access the service and transfer files through the curated gateway. The objective of this requirement is to ensure that users can only move data in and out of the environment through the gateway, and to reduce the risk of external threats by limiting potential points of attack. |
| d. Hosted in Australia (whether physical or cloud infrastructure) | All the data, technology systems, and the services that handle the data, including backup copies, should be kept within Australia to ensure data sovereignty. There can be cases where it's okay for someone to access the Secure Access Environment from a location outside of Australia, but there should be clear guidelines for regulating such access. The goal is to avoid using applications or services that send data overseas. | There are situations where certain new cloud services and applications might not be accessible within Australian regions. In these cases, you'll have to find suitable alternatives to use instead. |
| e. Users are authenticated using best practices | To ensure robust security measures, such as detailed logging and strict access controls, user authentication should be designed to reduce the risk of actions like sharing login credentials or attempting brute force attacks. | It's also important for Secure Access Environments (SAEs) to think about the possibility of integrating data passport technology into their systems in the future and plan for interoperability. |
| f. Encryption at rest and in transit for all data and files, including uploads to the gateway | Encrypting data at rest and in transit helps reduce the harm caused by successful attacks. To do this, it's important to use strong and trusted encryption methods, carefully manage encryption keys, and stay up to date by reviewing and improving encryption techniques to stay ahead of evolving threats and vulnerabilities. | Depending on the specific approach used, encryption might affect system performance. |

## 6.4. 4. Analytics Enabled

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| a. Economically sustainable and offers flexible resources | To cater for projects of different sizes and durations, environments need to provide affordable solutions for different computing and resource needs. This might involve offering a selection of virtual machines with graphics processing units (GPUs), storage space, memory, and processors, so users can choose resources suited to their project. Giving users the option to choose their software packages or bring their own licenses can save them money by letting them pay only for the licenses they require. It's also important for these resources to be flexible to match the different stages of a project. The environments should be sustainable for both the people using them and operating them to ensure long-term support. | End users should know that the expenses needed to run a Secure Access Environment will be included in the overall cost. However, it's important to understand that the cost of dealing with a data breach and its aftermath is much, much higher than the cost of using a Secure Access Requirement in the first place. In other words, it's more cost-effective to invest in security upfront to prevent a breach than to deal with the financial consequences of a breach later. |
| b. Performant environment that can support big data and complex analytics | Environments should be capable of handling a variety of analytical tasks, such as artificial intelligence, machine learning, natural language processing, and big data. They should provide the necessary resources like computing power, storage, processing capabilities, tools, and software to support both current and future analytical needs. In other words, they should be prepared for emerging requirements. | If a project needs a lot of resources, it can get expensive. So, when you're planning your project, you should think about your approach and estimate the costs involved. This way, you can better anticipate and budget accordingly. |
| c. Common tools, software and packages are provided as standard | Environments should provide a set of common tools and software as standard. These typically include analytical software and languages, word processing and spreadsheet software, database functionality, code editing software, version control software, business intelligence tools, and other software as deemed suitable by the environment owner. | Licensed software might be included as standard or come at an extra cost. Depending on the environment not all software or services may be available. It is the responsibility of the end user to verify which tools, software, and packages are available. |
| d. Non-standard software can be deployed at the discretion of the SAE (**Optional**) | At times, users may require access to specific, tools and software. To accommodate this, some environments allow non-standard software in contained environments without compromising the platform's security. Whether this option is available depends on various factors, including the technical feasibility, security needs and policies. Documentation of applicable policy or processes should be provided. | Any software or tools brought into the environment must undergo a thorough review to ensure they won't pose risks, such as relying on internet access, which could potentially expose the environment to security threats. |

## 6.5. 5. Platform Governance

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| a. Roles, responsibilities, governance policies, service expectations and liabilities are clearly defined | The environment should have well-defined roles and responsibilities for all types of users, including end users, environment administrators, and data custodians, with clear consequences for users who don't follow the rules.<br>The environment needs to establish clear service expectations and responsibilities, especially when it comes to data breaches. To ensure proper data governance and handling of data breaches, there should be a clear reporting structure from the Secure Access Environment to the data custodian. Policies and procedures should support this connection because reporting at the project level is not sufficient to address mandatory breach reporting obligations.<br>Environments should also provide relevant documents, such as data governance frameworks and policies as supporting evidence. | Each platform may have its own unique processes and policies. Therefore, it should be as easy as possible for end users and data custodians to find information specific to their environment. |
| b. Clear policies and efficient processes for user management | New users should have their accounts and workspaces set up promptly. Access for end users should have a specific time frame, aligned with their authorization and the duration of their project. This can be automated or managed manually. It's essential to regularly check that users are still part of the project team, working with the lead investigator or their designated institution, holding the same role, or if they've moved overseas. There should be a well-defined policy for handling access for international collaborators, and when multiple custodians or agencies are involved.<br>Follow the principle of giving users the least amount of access they need. To move files through the gateway, users need special permissions. They should only be allowed to manage projects they have approval for, which helps prevent data leaks. | There are many different scenarios when it comes to users, roles, and responsibilities, and established platforms should have processes in place to address these variations. |

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| c. Data retention and disposal policies are enforced - differentiated for project, archive, and gateway / audit data | Projects can be of varying duration, sometimes spanning several years. To manage this, it's important to have policies and procedures in place for handling data retention and disposal, which can vary based on the project.<br>Policies should be set up in a way that allows the deletion of project-specific data without erasing the associated gateway audit trail until a specific future time. Some research projects require archives, and many Secure Access Environments have arrangements for archiving. It's crucial to ensure that access to archives is concordant with project access. Additionally, there should be a policy for how long backups are retained and when they should be disposed of. This retention policy should be clearly documented. | Researchers need to include archiving costs in their project budgets and plans. |
| d. Training and support for users and custodians is available | End users and data custodians have access to training and support that is tailored to their specific roles. This training covers topics related to the environment, how it works, and the various procedures, such as workflow management. | Training on statistical and analytical methods, including statistical disclosure control, is not a part of this requirement, though it can be helpful to have. |
| e. Processes for NSW Health to respond to data breaches, conduct audits and curate outputs | NSW Health Data Custodians, the Cybersecurity Team, and other relevant staff should have clear and quick access to the Secure Access Environment for purposes such as responding to data breaches, conducting audits and curating / reviewing outputs. The procedure for granting access must be well-documented. Rapid access to respond to a breach is of critical importance and supports the requirements for mandatory breach reporting. When there is reasonable suspicion of a potential data breach, an assessment must be carried out within 30 days. All these processes should be documented, and Memorandums of Understanding (MOUs) should be developed. | Each environment will have different processes and protocols for handling these requirements. |
| f. Processes for SAE reporting on projects with NSW Health Data, including breaches | Environments need to be capable of creating a list of projects that use NSW Health Data and keeping track of how many projects are ongoing. They should also be able to provide information about the users who have access to these projects. This helps in responding effectively in case of a data breach and for regular auditing purposes.<br>If a data breach is identified or if an end user violates the terms of use, reports should be shared with the appropriate contacts as soon as possible to enable a swift response. | Each environment will have different processes and protocols for handling these requirements. |

| Requirement Description | Rationale and Context | Limitations and Mitigations |
|---|---|---|
| | These processes should be documented, and Memorandums of Understanding (MOUs) should be established. | |
| g. Data Custodians, their delegates or trusted platform administrators load data to the environment directly | It is extremely important to ensure that end users cannot access the data outside of the Secure Access Environment because doing so would defeat the entire purpose of having such a secure system.<br>Custodians or trusted delegates should have the ability to directly input data into a project workspace using a Secure Access Environment gateway, to reduce the number of interactions and potential risks. | Some environments do not allow custodians to load data directly, and instead require their own administrative staff to do so. In this scenario, the secure transfer of data is important to maintain. |
| h. Compliance with relevant legislation | Relevant legislation depends on the data that will be stored and analysed within the SAE, for example, the Health Records and Information Privacy Act 2002 (NSW) [48]. Compliance with the SOCI Act [49] may be required for certain projects.<br>The onus is on the Secure Access Environment to ensure and demonstrate ongoing compliance with applicable legislation and changes. | Some environments may not be able to host certain projects. |

# 7. REVISION HISTORY

As this document evolves to meet emerging needs and changes, version history and significant changes will be documented below.

| Version | Changes |
|---|---|
| 2024-01-25 - Current | • Updated the term “Self-curation” to “Nominated user curation” to clarify the meaning and simplified the curation levels table.<br>• Added clarification around certification in requirement 3.a. (Demonstrated adherence to a recognised information security and technology standard).<br>• Replaced examples in requirement 4.c. (Common tools, software and packages are provided as standard) with generic categories.<br>• Removed draft status and added change log. |
| 2023-11-23 | Original draft released. |

## 8. REFERENCES

[1] NSW Health, "Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services," [Online]. Available: https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2015_037.pdf.

[2] NSW Health, "Disclosure of unit record data by Local Health Districts for research or contractor services," [Online]. Available: https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2018_001.pdf.

[3] PHRN, "Annual Review 2021-2022," [Online]. Available: https://www.phrn.org.au/media/82500/phrn_report-2021-2022_28april2023_web.pdf.

[4] Austrade, "Australia’s A$7 billion cyber security opportunity," [Online]. Available: https://www.austrade.gov.au/en/news-and-analysis/analysis/australias-a-7-billion-cyber-security-opportunity.html.

[5] Australian Government, "Nation's largest ever investment in cyber security," [Online]. Available: https://www.minister.defence.gov.au/media-releases/2020-06-30/nations-largest-ever-investment-cyber-security.

[6] ABC News, [Online]. Available: https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586.

[7] Bitdefender , "New Bitdefender Survey Reveals Top Cybersecurity Challenges and Concerns for Businesses Globally," [Online]. Available: https://www.bitdefender.com/news/new-bitdefender-survey-reveals-top-cybersecurity-challenges-and-concerns-for-businesses-globally.html.

[8] OAIC, "Notifiable data breaches report July to December 2022," [Online]. Available: https://www.oaic.gov.au/__data/assets/pdf_file/0026/39068/OAIC-Notifiable-data-breaches-report-July-December-2022.pdf.

[9] Australian Signals Directorate, "ASD's ACSC Annual Cyber Threat Report, July 2021 to June 2022," [Online]. Available: https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022.

[10] UNSW, "Secure data analysis environments," [Online]. Available: https://ipdln.org/sites/default/files/2018ConcurrentSessions/210/Sept-12-1515-C12-Room210-Jorm.pdf.

[11] CRN, "MSSPs dish on why Australian universities are so attractive to hackers," [Online]. Available: https://www.crn.com.au/news/mssps-dish-on-why-australian-universities-are-so-attractive-to-hackers-584213.

[12] ABC News, "See your identity pieced together from stolen data," [Online]. Available: https://www.abc.net.au/news/2023-05-18/data-breaches-your-identity-interactive/102175688.

[13] University of Melbourne, "THE SIMPLE PROCESS OF RE-IDENTIFYING PATIENTS IN PUBLIC HEALTH RECORDS," [Online]. Available: https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records.

[14] Wikipedia, "ε-differential privacy," [Online]. Available: https://en.wikipedia.org/wiki/Differential_privacy#%CE%B5-differential_privacy.

[15] NIST, "De-Identifying Government Datasets: Techniques and Governance," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-188.pdf.

[16] M. e. A. Chamikara, "OptimShare: A Unified Framework for Privacy Preserving Data Sharing -- Towards the Practical Utility of Data with Privacy," [Online]. Available: https://www.researchgate.net/publication/371347369_OptimShare_A_Unified_Framework_for_Privacy_Preserving_Data_Sharing_--_Towards_the_Practical_Utility_of_Data_with_Privacy.

[17] Salinger Privacy, "To fix the Privacy Act, we need one extra sentence," [Online]. Available: https://www.salingerprivacy.com.au/2023/04/19/one-extra-sentence/.

[18] Parliament of Australia, "Chapter 1 - PwC: A calculated breach of trust," [Online]. Available: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/Consultingservices/PwC_Report/Chapter_1_-_PwC_A_calculated_breach_of_trust.

[19] Attorney-General, "Parliament approves Government’s privacy penalty bill," [Online]. Available: https://ministers.ag.gov.au/media-centre/parliament-approves-governments-privacy-penalty-bill-28-11-2022.

[20] Reuters, "Australia regulator tells Medibank to set aside $167 million after data breach," [Online]. Available: https://www.reuters.com/business/finance/australia-regulator-asks-medibank-set-aside-167-mln-after-data-breach-2023-06-26/.

[21] Financial Review, "Inside the Optus hack that woke up Australia," [Online]. Available: https://www.afr.com/technology/inside-the-optus-hack-that-woke-up-australia-20221123-p5c0lm .

[22] ASIC, "Guidance for consumers impacted by the Optus data breach," [Online]. Available: https://asic.gov.au/about-asic/news-centre/news-items/guidance-for-consumers-impacted-by-the-optus-data-breach/.

[23] NSW Health, "As one system," [Online]. Available: https://www.health.nsw.gov.au/Infectious/covid-19/evidence-hub/Publications/as-one-report.PDF.

[24] ICP, "Mandatory Notification of Data Breach Scheme," [Online]. Available: https://www.ipc.nsw.gov.au/privacy/MNDB-scheme .

[25] NSW Government, "Data Sharing Principles," [Online]. Available: https://data.nsw.gov.au/data-sharing-principles.

[26] UWE Bristol, "Five Safes: designing data access for research," [Online]. Available: https://www.researchgate.net/profile/Felix-Ritchie/publication/292975549_Five_Safes_designing_data_access_for_research/links/56b31cc908ae56d7b06d15fb/Five-Safes-designing-data-access-for-research.pdf.

[27] CADRE, "Cadre 5 Safes," [Online]. Available: https://cadre5safes.org.au/about/outreach/.

[28] AIHW, "The Five Safes framework," [Online]. Available: https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework.

[29] F. Ritchie, "Secure access to confidential microdata," [Online]. Available: https://link.springer.com/content/pdf/10.1057/elmr.2008.73.pdf?pdf=inline%20link.

[30] UK Data Service, "What is the Five Safes framework?," [Online]. Available: https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/.

[31] Stats NZ, "How we keep integrated data safe," [Online]. Available: https://www.stats.govt.nz/integrated-data/how-we-keep-integrated-data-safe/.

[32] ONDC, "Share Data," [Online]. Available: https://www.datacommissioner.gov.au/share-data.

[33] FACSIAR, "Human Services Dataset De-Identification and Five Safes Framework Policy," [Online]. Available: https://www.facs.nsw.gov.au/__data/assets/pdf_file/0007/813634/Human-Services-Dataset-De-Identification-and-Five-Safes-Framework-Policy.pdf.

[34] ABS, "Five Safes framework," [Online]. Available: https://www.abs.gov.au/about/data-services/data-confidentiality-guide/five-safes-framework.

[35] Australian Government, "National Health Reform Agreement (2020-2025)," [Online]. Available: https://federalfinancialrelations.gov.au/sites/federalfinancialrelations.gov.au/files/2021-07/NHRA_2020-25_Addendum_consolidated.pdf.

[36] Australian Signals Directorate, "Essential Eight," [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained.

[37] Australian Signals Directorate, "The cyber security principles," [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles.

[38] HDRUK, "New principles published to improve public confidence in access and use of data for health research through Trusted Research Environments," [Online]. Available: https://www.hdruk.ac.uk/news/new-principles-published-to-improve-public-confidence-in-access-and-use-of-data-for-health-research-through-trusted-research-environments/.

[39] R. e. A. Brophy, "Towards a standardised cross-sectoral data access agreement template forresearch: a core set of principles for data access within trusted research environments," [Online]. Available: https://ijpds.org/article/view/2169/4941.

[40] AIHW, "Data Governance Framework," [Online]. Available: https://www.aihw.gov.au/getmedia/c3e00f60-c40d-4989-ad22-de1be3ab5380/Data-Governance-Framework-2021.pdf.aspx.

[41] NSW Health, "Privacy issues and the reporting of small numbers," [Online]. Available: https://www.health.nsw.gov.au/hsnsw/Publications/privacy-small-numbers.pdf.

[42] ABS, "Treating aggregate data," [Online]. Available: https://www.abs.gov.au/about/data-services/data-confidentiality-guide/treating-aggregate-data.

[43] Bennett Institute, "The Opensafely Output Checking Service," [Online]. Available: https://www.bennett.ox.ac.uk/blog/2023/05/the-opensafely-output-checking-service/.

[44] AiLECSlab, "The Data Airlock - Infrastructure for restricted data informatics," [Online]. Available: https://ailecs.org/wp-content/uploads/2022/03/TR22_03-AirlockV1-Technical-Report.pdf.

[45] NSW Cancer Institute, "CanDLe User Protocol," [Online]. Available: https://www.cancer.nsw.gov.au/getmedia/36d5cb1b-df31-4bca-a31e-fc7c7a7d90a6/CanDLe-User-Protocol.

[46] Digital Health CRC, "Digital Transformation Of Healthcare In Australia Constrained - A Call To Action For A National Data Governance Framework," [Online]. Available: https://digitalhealthcrc.com/wp-content/uploads/2023/02/DHCRC-Call-to-Action-for-a-National-Data-Governance-Framework_Feb-2023_FINALDESIGNED.pdf.

[47] ARDC, "Sensitive Data Platforms Australia," [Online]. Available: https://www.sensitivedataplatforms.org/collaborators.

[48] NSW Government, "Health Records and Information Privacy Act 2002 No 71," [Online]. Available: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-071.

[49] Australian Government, "Security of Critical Infrastructure Act 2018," [Online]. Available: https://www.legislation.gov.au/Details/C2022C00160.