UK Research and Innovation

HDRUK Health Data Research UK

ADR UK Data-driven change

DARE UK – Early Thinking

Access and Accreditation

Stakeholder workshop, Wednesday 23 March 2022

Access and Accreditation

The requirements discussed in this theme focus on two main aspects of accessing a standardised trusted research environment (TRE) for access and processing of sensitive data.

One of the biggest challenges for researchers from both industry and academia is the time that it takes to apply for data access and have all approvals, checks and safeguards in place to do the analysis.

For the purpose of our recommendations:

- Access is split in two parts
  - Requesting access to sensitive data from data custodians – Data Access Request
  - Requesting access to a TRE to process previously approved data (i.e. user authentication/ accreditation)
- Accreditation
  - This covers the definition of a TRE and conformity of TREs to be able inter-operate with each other

Technical Glossary

- **Trusted research environment (TRE)** – A secure data centre that holds sensitive data with secure access policies, processes, and analysis capability managed by governance/information protection professionals
- **User Authentication** – Process by which a user logs into a service/website
- **User Accreditation** – Process by which a user obtains the correct training to handle sensitive data
- **Identity Federation** – Process by which different identity providers (institutions) can mutually recognise each other’s users
- **Identity Brokerage** – Process by which an identity token is negotiated to obtain another identity token to access services. Think of using your drivers licence to prove age to gain entry into a pub
- **TRE Accreditation** – Process by which conformance/compliance of a TRE facility to a standard is evaluated and maintained
- **Privacy Evaluation Framework** – Process by which the privacy risk of a dataset(s) is evaluated aligned to legal and regulatory requirements

First Draft Recommendations (1 of 5)

AA1: Provide a unifying user authentication capability to access services

- AA1a. Leverage existing identity federations to develop identity brokerage services
- AA1b. Leverage existing industry & community standards as the basis to allow for maximum interoperability nationally and internationally
- AA1c. Pilot a test case of identity federation and authentication nationally and internationally

Your thoughts and feedback

Provide a unifying user authentication capability to access services

- Prerequisite for all forms of federation to occur – mostly a hearts and minds challenge
- This will allow the creation of an interoperable 'research passport' – link to Health Research Authority
- The identity will be held in the passport, which can be used to track all access licenses as 'visas'
- Like the idea of identity federation to improve trustworthiness; but need to consider how organisations will trust each other's users
- Need to have a three tiered approach – identity, authentication (SSO) and authorisation (passport/visa)
- Need identity verification levels – going beyond email address
- Need to explore how international identity federations are facilitated or withdrawn
- Test case for identity federation is great idea – DiRAC (Distributed Research Utilising Advanced Computing) infrastructure may be a good test case
- Need logging and auditing system wide – distributed ledger may be an option
- Leverage existing standards – for example, Global Alliance for Genomics and Health (GA4GH) passports; AAI (Authentication and Authorisation Infrastructure)
- Ensure industry and other non-academic stakeholders (e.g. NHS) are also part of federation

First Draft Recommendations (2 of 5)

AA2: Develop a UK-wide and legally conformant user accreditation standard

- AA2a. Leverage existing work from regulatory authorities and TREs to institute a federated approach to user accreditation
- AA2b. Develop consistent guidance for stakeholders to undertake user accreditation
- AA2c. Develop user accreditation online training modules that can be delivered at a UK-wide scale with on-site drop-ins to scale the delivery and maintenance of user accreditations

Your thoughts and feedback

Develop a UK-wide and legally conformant user accreditation standard

- Identify a baseline user accreditation requirement and define this as the ‘core’ accreditation requirement
- Make value and benefits of information governance clear, with a mechanism to ensure regular top-ups (e.g. every 18 months)
- Leverage existing training modules – e.g. from the Office for National Statistics, Medical Research Council – and streamline with reasonable expense
- Leverage identity federation to deliver online training so these can be linked into the passport
- Separate training delivery/consultation from the TRE operator themselves to improve trustworthiness
- This should not be limited to just researchers – should be open to anyone handling sensitive data
- Improve visibility of the training content and which permission panels require them
- Develop standards with service users and public involvement
- Explore different levels of accreditation based on the type of access and domains of data required
- **Modularise accreditation with ‘core’ and ‘extended’ modules for different types of access request**
- Do we need heavier checks for very sensitive data?
- People may want to be accredited without a specific project in mind

First Draft Recommendations (3 of 5)

AA3: Develop an internationally recognised TRE standard and accreditation framework

- AA3a. Develop a working definition of TRE and iterate to get to a consistent standard definition of TRE with edge cases explored as needed
- AA3b. Develop a searchable central registry of TREs with transparent summaries of capabilities
- AA3c. Develop a framework to accredit a TRE, leveraging and harmonising existing accreditation frameworks (e.g. Digital Economy Act approved processor)
- AA3d. Implement and test the accreditation process with at least two TREs from separate domains to refine and consolidate the process

Your thoughts and feedback

Develop a internationally recognised TRE standard and accreditation framework

- Consolidate a range of certifications (e.g. ISO 27001, DSPT (Data Security and Protection Toolkit), etc.) as part of a TRE framework standard and accreditation process
- Leverage the Digital Economy Act standard and develop it, with possible route to BSI and/or ISO standard level
- Start with a baseline standard and develop plugins to extend the TRE for specific use cases
- Use funding to incentivise TRE accreditation and compliance
- TRE accreditation should also cover how TREs should interoperate, not just how they should operate in isolation
- Support the development of a central register of TREs
- Focus on UK-wide recognition of a TRE standard and then expand globally – link to Canada and Australia
- Not every secure data environment can be a TRE, but to be a TRE you need security, privacy and confidentiality
- Need to consolidate towards a business plan for TREs and federated network of TREs with a sustainability plan
- The DELPHI three stage process could be used to get to an agreed set of core standards

First Draft Recommendations (4 of 5)

AA4: Develop a standardised yet extensible process to request access to sensitive data from TREs

- AA4a. Leverage and harmonise existing Data Access Request procedures, processes into a single baseline procedure that can be instituted by a centralised service
- AA4b. Align Data Access Request forms using the Five SAFEs – SAFE People, SAFE Project, SAFE Data, SAFE Setting and SAFE Outputs
- AA4c. Interlink external identifiers of resources – datasets, tools, funder/sponsors, people, project/grant identifier to ensure a Data Access Request procedures can leverage system-wide intelligence
- AA4d. Publish Data Use Registers transparently for all approved Data Access Requests flowing through the network

Your thoughts and feedback

Develop a standardised yet extensible process to request access to sensitive data from TREs

- Convene a Research Data Alliance to consolidate data access request (DAR) standardisation and align to international efforts
- Minimising duplication is very much needed, and a standardised DAR will help achieve this
- Learn from and leverage existing efforts – e.g. HDR UK Gateway Five Safe DAR form; Health Research Authority IRAS system – as well as from consortiums (e.g. BHF Data Science Centre; SAIL Databank) to harmonise DAR forms
- Any standardised DAR must have endorsement from the data custodians and be linked to data sensitivity
- Being able to submit a single DAR to multiple data custodians to coordinate will be a transformative change in the ecosystem
- It could also be worth looking into standardising supporting documentation e.g. data protection impact assessments (DPIAs)
- Standardisation around timelines/processes is also needed, but appreciate that this would be the starting point of that work
- Link the DAR form and key requirement for TRE accreditation
- Would be useful to develop an intermediary broker to negotiate access to datasets on the researcher's behalf – the single form could be supplied to the trusted third party who can then coordinate with data custodians
- Even with a standardised processes, different organisations will have complex requirements – precedence will be a challenge
- Need to evaluate whether each question truly increases the safety of the data or is more related to administrative requirements
- Would be great to start with a single form, with additional questions appended as required and additional data custodians added to the access request
- Will this cover data sharing agreements between TREs and not just researchers? We need transparency with regards to data sharing between organisations too

First Draft Recommendations (5 of 5)

AA5: Develop an internationally recognised Privacy Risk Framework to assess privacy risk for secure TREs and federations

- AA5a. Evaluate and develop a Privacy Risk Assessment Framework specification
- AA5b. Develop complementary guidance and tools to enable privacy risk modelling to be performed by TREs consistently
- AA5c. Test the privacy risk assessment framework as an ancillary tool as part of real-world projects in at least 2 or more TREs

Your thoughts and feedback

Develop an internationally recognised Privacy Risk Framework to assess privacy risk for secure TREs and federations

- There are a number of existing risk assessment frameworks – leverage these as a starting point
- This would be a very useful tool to help data access committees evaluate applications; and could be an educational tool for researchers to understand the complexity of their applications
- Members of the public would like to see this as a checkmark for all applications made to use their data
- Trusted auditing is required – privacy risk evolves over time and changes to project scope must be evaluated accordingly
- This would allow creation of a universally accepted measure of trustworthiness
- This needs to carefully balance the utility of the data and the privacy risk associated with the data
- List the types of technical and non-technical parameters and assign a score against each
- This will require consultation of information governance experts across all four nations
- Could be created as an extension to the Information Commissioner's Office (ICO) Guide to Data Protection
- The true unblocker here is not the privacy risk assessment of a single dataset, but a joint privacy risk assessment of multiple datasets under the control of multiple data custodians
- There is also something to be said about managing privacy risk at the macro-level – is there a bigger role for the ICO to play here? We do not want to end up micro-managing each individual data access request

UK Research and Innovation

HDRUK
Health Data Research UK

ADR UK
Data-driven change

Thank you

Find out more about DARE UK: www.dareuk.org.uk