Architectural principles

Architectural principles influence and shape the way you design and deliver a SATRE-aligned TRE. They are a set of guiding considerations that sit above any specific architectural requirement, and can be applied across the entire architecture.

They are made up of
Statement: A singular sentence that summarises the principle
Rationale: Justification as to why this principle is important for the specification
Implications: Things you need to consider or do to practise this principle

Usability

Statement

A TRE instance that works for everyone minimises barriers to use, and provides a productive and accessible analysis environment for research.

Rationale

There is often a trade-off between increased operational security and the usability of a TRE. In order to maintain productivity, a TRE must balance these two competing aims. The design and configuration of a TRE should allow all individuals to effectively fulfil their roles.

Implications

- TRE design and implementation should start by understanding users' diverse expectations, needs, existing skillsets and preferences and responsibilities.
-
- How technical should users need to be?~~X~~ How do we know existing levels of technical proficiency?
- Are there lists of tools available for users who come to TREs; where should these be kept alongside; information about what data the TREs hold
    - One perspective - usability comes down to tools
    - Can't be too restrictive on requirements around tools
- Learning: users have to learn different ways of working depending on design/configuration choice
    - Via tutorials, documentation, co-piloting services (example from Open Safely; a real person helps with intial projects tasks) tailored to users' needs. ~~X~~
- The accessibility of the TRE itself is an important issue for users. ~~X~~

Commented [1]: Good to highlight that users aren't just the researchers but also the data providers and the info-gov teams

- Learning from user experience - orgs need people like product managers; also monitoring via helpdesk functions - e.g. tracking and logging issues like lag time, regulating backups, making sense over t
- If the TRE isn't usable, usres won't come
- We need to think about the usability of the standards and functional specification itself.
-

Other principles

- Something about describing data.
    - This is about users, but also quality control of research
    - This helpful for maintaining trust
    - Meta data about what data is being shared

Maintaining Trust

Statement

TREs should build and maintain the trust of data subjects and any other impacted individuals, groups and organisations by protecting privacy, keeping data secure and being transparent about their work.

Rationale

Maintaining trust in TREs to hold and use data is essential to prevent backlash or resistance to the use of data. This can include maintaining the trust of members of the public who are impacted by research, as well as the trust of commercial data providers.

In the case of public sector data~~health data research~~, public engagement work has indicated there is widespread support for the use of regulated and ethical TREs working for the public benefit. Consulting impacted parties including public can help show that a TRE is acting in their benefit. Being transparent about the data held and the projects or organisations who access the data can also help maintain trust.

Implications

- TREs should make information on the projects or organisations which access their data available to impacted parties
- Access to public sector data should be reviewed by a panel and follow governance to ensure they are in public benefit~~X~~and clarity around commercial access
- TREs should should be clear on infrastructure including ingress/accreditation~~accreditation X~~

Commented [2]: Broaden to communities and society

Commented [3]: This phrasing makes it sound performative rather than emphasing they should have real impact

Commented [4]: Add in implication for clarity around infrastructure

Commented [5]: And publicly

Commented [6]: This doesnt exist yet?

- Processes in place for rigorously investigating and reporting incidents such as data leaks including processes required by the Information Commissioner's Office ~~X~~
- X

Commented [7]: Should there be an equivalent of transport or fire/police investigative processes?

Observability

Statement

Human initiated and automated processes resulting in change within the TRE should be observable in real time?.

Cf. Virtual witnessing
Transparency
Provenance

Rationale

System/process observability is key to understanding whether your policies and controls are actually doing what is intended.

It also allows operators to continuously improve their systems and processes, measure their effectiveness, and identify the causes of incidents. Data can also be made available to other parties such as auditors, data subjects and data providers as part of the assurance process.

This applies to both technical systems and policies/processes.

Implications

- In order to understand what is happening within the TRE, both automated and human initiated processes should generate sufficient data.
- These data should follow standards for provenance and transparency for audit trails~~X~~
- Observing needs to be transparent
- Is this real time or is it also about recording and defending? How does this relate to trust?~~X~~
- Dashboards for surveillance and monitoring for TRE operators?
    - What is a key action?

- ~~X~~How do you monitor without intrusion on the confidentiality of a researcher's requests or are at least transparent about it
- What things are useful to expose and what is worth keeping private?
- Duty of care to researchers- balancing being nosey with being proactively helpful
    - Granularity - have to started? Coarsed grained. Vs why did you use that data set? Which could be helpful or could be nosey.
- Three persona: researcher, TRE operator, National auditor,
    - For each, what are the observable user stories
    - As a <who?persona/role> I can <what?capability>, so that <why?receive benefit>

Standardisation

Statement

TREs should adhere to standards or well-known patterns wherever possible.

Commented [8]: Do we mean standardisation of technology, data or both?

Rationale

Standardisation makes it easier to design, operate and use and understand TREs, and reduces duplication of work. This includes making TREs easier to use, deploy, and audit. ~~They also enable interconnectivity/interoperability for TREs that wish to federate, either now or in the future.~~ TREs should be built in such a way that they do not restrict/prevent interoperability where this may be desirable in future, by identifying and avoiding or removing barriers to interoperability. Standardisation is also linked to the public trust principle, because people know what they're dealing with when they come across a TRE built to SATRE specification.

Implications

- TREs should adhere to public standards
- ~~X~~TREs could be interoperable or federated
- ~~X~~TREs should adhere to existing technical standards where appropriate
- Possible: TRE data should be structured according to best practices for that domain (e.g. omop health data) - but this might be getting too much into "what researchers should do"
- Similar to ^ TREs should be designed to support standard data structures defined by the relevant community
- One example of a barrier to interoperability would be where user authentication is very different across TREs. User authentication should probably be familiar e.g. using common or standard authentication providers,~~using the same 3rd party providers~~ unless there is a reason not to
- TRE standard writers should reuse/incorporate existing standards wherever possible

Extra principles:

- Maintaining buy-in/ confidence in usefulness of the TRE for people using or wanting to use (or indeed paying to use) the TRE. Education and marketing are important. Cost effectiveness/ value for money/return on investment (in the general sense, not necessarily just £) are important.
-
- Accountability - registered owners for certain elements
- Transparency sits across various elements of these principles
- Culture of best practice and safety e.g. Near Miss Reporting requirement and transparency

-