Transparency Standards

The standards below have been developed from the recommendations provided by the Public Advisory Board and the Five Safe Action Force. They are designed to guide best practice for transparency and have gone through a process of consultation and feedback from the PAB and the Steering Group.

Standard 1: Open access application form and guidance

Custodians should have an accessible copy of the data access application form and accompanying guidance notes on their website.

Data custodians should:

- Publish a version of their data access application form that it is accessible without the need for registration or any other additional requirements.
- Publish guidance notes including details as to why the information in the form is being requested (e.g. for compliance with national standards or legislation) as well as examples and case studies.

We recognise that there is a need to balance transparency with the risk of receiving an increase in inappropriate data access requests. Providing an un-editable PDF copy of the form, this way researcher will still need to register before completing and submitting the live form, thereby mitigating the risk of inappropriate submissions. The un-editable versions of the application form should remind researchers to ensure they are filling in the most up to date version of the form before submission.

Standard 2: Transparent application process and criteria

Custodians should provide clear information on every step of the data access process, including the criteria for granting access and how members of the public are involved in the process.

Data custodians should:

- Clearly set out each step in the data access process in an accessible format with appropriate structure and language (e.g., through diagrams, videos, animations, swim lane diagram or process flows for both researchers and the public), including indicative timescales for each step where possible and where responsibility lies.

- Provide clear guidance notes and actionable steps to satisfy the application process.
- Describe on their website how their data access process incorporates the Five Safes Framework and explain what this means in a transparent and accessible way.
- Explain how applications are assessed by the custodian, including how members of the public are involved in assessing applications and developing the criteria used to assess applications.
- Include clear definitions of key terms such as Trusted Research Environment (TRE), Secure Data Environment (SDE), Data Safe Haven (DSH). Consistency of language across data custodians will help facilitate better understanding by the research community and the public.

As a next step, the Five Safes Action force is planning to review currently used and publicly available definitions of terms such as Data Safe Haven, Trusted Research Environment/Secure Data Environment etc and consider whether there is an opportunity to work with members of the public to streamline terminology and understanding.

Standard 3: Clear website navigation

Information about data access processes should be easily discoverable and comprehensive.

Data custodians should:

- Consider accessibility when creating website content.
- Make information about the data access process easy to find and clear from the homepage. It may not be possible to include data access information on the homepage, particularly for larger organisations, but drop-down menus or similar can be used to signpost data access information.
- Include clear information about how public benefit is assessed.
- Have separate website sections for information about clinical trials and secondary re-use of data for research (where applicable).
- Where the data custodian supports different types of research with distinct processes for access (e.g., service improvement versus health research), have separate sections of the website with the required information.
- For linked data sets with multiple controllers, provide clear and detailed information on requirements for data access, with a clear pathway setting out what the researcher should expect in terms of approvals, timescales, access, and data management and information about the role of relevant data controllers.

Standard 4: Consider Target Audience

Website should use appropriate language for the audience and should include content specifically developed for members of the public in readily understandable terms.

Data custodians should:

- Consider having separate website sections, using appropriate language, for researchers and members of the public, in each case using appropriate language for the target audience.
- Involve researchers, information governance professionals and members of the public in writing and checking of all materials intended for the public to ensure that the web design and its contents are accurate, comprehensible, and accessible.
- Provide a mechanism for members of the public and researchers to provide feedback on the language, structure, and content.
- Consider how to provide information in an appropriate language to members of the public who may not have access to the internet access.

Standard 5: Regular review of website content

Website content should be periodically reviewed and updated as appropriate.

Data custodians should:

- Commit to regular review periods (for example every six or twelve months), where the information on their website is reviewed and updated.
- Where there are downloadable application forms and guidance notes, custodians should include the last review date and the next review date to ensure researchers and the public know they have the current version.
- Have a "frequently asked questions" section and or equivalent on the website and keep this regularly updated.

Standard 6: Transparency of Data Use and Auditing

Custodians should be transparent about how data is used for research.

Custodians should:

- Publish a summary of approved studies/protocols (lay summary, technical summary, public benefit etc) and resulting research outputs for full transparency at least 3 months after approval.
    - Where a particular project, change in best practice or regulation means the data controller can set a precedent this should be shared to encourage consistency of decision-making.

- Publish minutes and/or core decisions made in Data Access Committees meetings (noting that redaction of sensitive information may be appropriate).
- Publish case studies each year, particularly case studies that highlight public benefit and examples of how lives are improved by use of data for research.
- Publish a data use register that is updated at regular intervals[1].
- Consider whether rejected requests for data access should be published, and if so the level of detail that should be published (e.g., it may not be appropriate to publish the name of the organisation or researcher that made a request that was rejected). Publishing the reason why certain types of requests are rejected may give the public reassurance that standards are being upheld and encourage consistency of decision making. The reasons do not have to be sensitive and give specific details around a specific researcher; they could be summaries such as data sensitivity, organisational concerns around data sensitively, public perspective etc.
- Consider publishing how factors such as governance, transparency, regulatory or specific concepts such as access mechanisms, data and tech specific issues that have been changed has impacted certain projects which will lead to better patient and public endorsed use of data.
- Publish an up-to-date and clear privacy notice in compliance with data protection legislation.
- Consider publishing:
  - A short summary of audit findings and sanctions that are applied if breaches are detected (noting that redaction of sensitive information may be appropriate).
  - A general overview of the number and type of sanctions that have been applied and some examples or case studies illustrating how to improve on these.

Some of suggested published material such as audit findings and or breaches are mechanism for organisations to be seen by members of the public to be transparent- often members of the public do not know if a particular organisation has had an audit and or the findings from them.

---

[1] https://zenodo.org/record/5902743#.ZDgTHcrMKUn