4. Service Provider Information

Service Providers, who receive attribute assertions from another Participant, shall respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Such information must be used only for the purposes for which it was provided.

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

4.1 Attributes

eduPerson Scoped Affiliation is REQUIRED
the rest, especially email and eduPerson Principal Name, ARE HIGHLY DESIRED.

4.1.1. What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service application that you offer to CAF participants.

eduPerson Scoped Affiliation, eduPerson Affiliation, eduPerson Principal Name
eduPerson Entitlement, email, displayName

4.1.2. What use do you make of attribute information that you receive in addition to basic access control decisions?

record in SERVICE log, use for authorization/access control

4.1.3. Do you use attributes to provide a persistent user experience across multiple sessions?

Yes

4.1.4. Do you aggregate session access records or record specific information accessed based on attribute information.

Yes. Actively looking into recording attributes with access control response
No other application of collected attributes is done

4.1.5. Do you make attribute information available to other services you provide or to partner organizations?

No

4.2 Technical Controls

DATA ACCESS IS PROTECTED BY PASSWORD AND FIREWALL AND special role IDMI.

4.2.1. What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted for storage in your system?

* We do not make access control decisions on individual basis to shibboleth users. We use eduPerson Scoped Affiliation attribute to determine access

4.2.2. Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

All Data is password protected, and only 2 people in the organization have roles to access data. Also, VPN/firewall.

4.2.3. If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

The data is locked At Stanford secure lab, password protected.

If stolen, we work with publishers to notify users that have insecure shibboleth Access.

Today, we do not own any individual user attributes.

5. Other Information

5.1 Technical Standards, Versions and Interoperability

5.1.1. Identify the SAML products you are using. If you are using the open source Internet2 Shibboleth products identify the release that you are using.

2.5.1 Shibboleth SP + wrapper services

5.1.2. What operating systems are the implementations on?

Linux

5.1.3. What versions of the SAML protocol (1.1 or 2.0) do you support in your implementations.

SAML 1.1

SAML 2.0 ✓

5.2 Other Considerations

5.2.1. Are there any other considerations or information that you wish to make known to other Canadian Access Federation Participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

N/A