Supplemental Guidance to IFR.09 Cross-Enterprise Authentication Guidance

In order for systems to make access control decisions (i.e. grant or deny access to authenticated users or entities) and generate accurate and detailed audit trails, the cross-enterprise transactions must contain sufficient identity information when communicating across networks.

IFR.09/SC 06.12 applies to a person or entity (e.g. users, services acting on behalf of users, applications, and systems) seeking access to electronic health information across a network. The standards included by HHS in the IFR for this purpose requires that the transaction seeking electronic health information must contain sufficient identification information in order for the receiving system to be able to make access control decisions and produce accurate and detailed audit trails. Therefore, these transactions must include adequate identification information such as the relationship of the entity (e.g. a partner organization, another enterprise, etc,) and attributes and entitlements of the subject, such as assigned privileges and restrictions.

Networks/organizations could maintain either independent user directories or common user directories, and it is likely that the transactions will be going between two enterprises that maintain their own independent user directories. In order to authenticate cross enterprise users regardless of the type of the user directory, the transaction must include sufficient identity information, as described above.

As part of the standards compliance to IFR.09, HHS has included the example of the use of IHE's Cross Enterprise User Assertion (XUA) with SAML identity assertions:

Cross-Enterprise User Assertion Profile (XUA) provides a means to communicate claims about the identity of an authenticated user, application, system, etc. in transactions that cross enterprise boundaries. For additional information, applicants can refer to:

1. http://wiki.ihe.net/index.php?title=Cross-Enterprise_User_Assertion
2. IHE IT Infrastructure Technical Framework Version 5 or later.

The OASIS Security Assertion Markup Language (SAML) standard defines an XML-based framework for describing and exchanging security information between on-line business partners. SAML allows entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, such as a partner company or another enterprise application. For additional information, applicants can refer to:

1. SAML V2.0 Executive Overview http://www.oasis-open.org/committees/download.php/11785/sstc-saml-exec-overview-2.0-draft-06.pdf.
2. Technical Overview http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0-draft-03.pdf.

The use of other methodologies based on secure communication channels such as TLS or SSL protocols will be permissible if adequate authentication mechanism (e.g. PKI Individual Certificates) to verify the authenticity of the person or entity and appropriate authorization process to verify the privileges and restrictions described above are included.