Draft Statement for Virtual Hearing from Thomas Sullivan, MD

HIT Standards Committee's Privacy and Security Workgroup

Wednesday, March 12th from 10:00-2:45 PM

The following statements are an expression of one person's opinion and are not meant to be interpreted as an endorsement by the members of the IDESG Healthcare committee Workgroup. However, as the Chair of the committee which has met regularly almost every other week since we were formed about 18 months ago, I have a sense of the issues we are trying to address incorporating the NSTIC guiding principles which are widely endorsed.

Focusing only on Trusted Identities in Healthcare, we believe there are far too many examples of unnecessary redundancy in IDP and Identity Management of both providers and patients. This leads to higher costs, inefficiency, errors, fraud and frustration throughout the industry, despite almost universal agreement of the need for simplification.

Privacy and Interoperability are among our most pressing concerns and they often conflict where implementation in the real world of competition, multiple vendors, multiple standards, complex user demands for control and heightened liability for errors are all factors we are obliged to consider.

To briefly illustrate the problem I have simplified two scenarios (perhaps oversimplified).

In scenario #1 the Patient is in total control of his/her own identity and decides what, when and with whom any and all information is shared. This scenario represents enhanced privacy for the consumer with the risk of danger and harm if the information associated with a particular identity is incomplete, misleading or not shared appropriately. For the best results, this scenario implies very active patient engagement.

In scenario #2 the Enterprise/Provider Practice controls the identity attributes of the patient with the associated advantage of convenience and efficiency for the treatment and administrative professionals (TPO in HIPAA language). There is also a certain element of patient safety added in this scenario since it is easier to discover aggregate data that may bear on treatment decisions, e.g. more comprehensive and accurate Medication lists, Procedure history, lab results, etc. However, the patient loses a certain element of control regarding data sharing and thus, perhaps less Privacy protection.

Outside these two scenarios it is likely that given the rapidly growing trend of consolidation of medical practices within large systems and large groups, corporate attorneys may play a much larger role in the future of influencing how healthcare identities are managed. In Massachusetts it is currently estimated that up to 75% of all providers are employed by these entities or enterprises.

We, in the committee have discussed these issues at length and presented a very small number of use cases with many more "in the wings" both from within our committee and from others in IDESG outside the Healthcare environment yet equally concerned with Privacy, Interoperability and implementation of the other NSTIC principles.

In simple language we have tried to model a Use Case of Identities in the environment of a Relationship Locator Service (RLS) that could include delegation. It is still in draft form though it has been published on the IDESG WIKI since mid December2013. An excerpt is presented below. We welcome all comments and suggestions for improvement and request more interaction and collaboration with both ONC and CMS (particularly in the Provider enrollment area).

Respectfully submitted,

Thomas E Sullivan, MD, Chair, IDESG Healthcare Industry Committee

A Brief Discussion of Data Segmentation and Multiple and Unverified IDs in the Healthcare Cyberspace (December 2013)

Segmentation of encounters for mental health and other sensitive conditions is a patient's right, as described in federal and selected state law.

On the other hand, involuntary surveillance and data aggregation for certain activities such as prescriptions for narcotics, other controlled substances and legend drugs are also required in many situations. A general solution to patient ID must accommodate both of these requirements while reducing the overall risk of treatment errors and patient harm due to mismatch of patient identity in both the false positive and false negative sense.

One possible approach to defining a patient ID consistent with NSTIC principles is to enable a patient to create multiple globally unique identifiers. One of those identifiers would be externally "verified" in a mandated or coercive manner such as through biometric matching or stringent authentication protocols on a national or international scale. The other voluntary identifiers would not be associated with the verified attribute.

A patient registering for a medical service would have the choice of presenting either an externally verified or an unverified ID (We understand "verified" to mean legally accountable).

Both the patient and the physician should be held responsible for discussing the risks in using an unverified ID. Such discussions are consistent with the trusted and confidential nature of the physician-patient relationship. However, a physician is not obligated to check the verification status of a patient-supplied ID unless required by law or contract.

Clinical practitioners communicating with an RLS (Relationship Locator Service, aka Record Locator Service) would always send the patient's preferred globally unique selected ID, be it verified or not.

Relationship Locator Services would respect the patient's voluntary ID assignment even if other demographic information such as name and DOB could be used to correlate or track the patient across voluntary IDs. The RLS would respond to queries based only on

the patient controlled ID. The RLS has the option of contacting the patient to help resolve ambiguous or close matches. The RLS can allow patients to re-designate an encounter to another voluntary ID as long as verified IDs are not removed or changed to unverified IDs.

This approach to patient ID introduces two kinds of authorities or federations. The first is an authority capable of verifying or authenticating a voluntary patient ID and attaching that attribute to the voluntary patient ID. The second is the RLS itself. The RLS must be legally authorized to perform the identity matching activities according to specific statutes or a federation agreement that enables the patient's right to voluntarily segment some health service encounters, (similar to those rights outlined in the HIPAA/Omnibus Rule updated in 2013.) The trust framework for these two federations and the health service providers that rely on them is a key design goal for the NSTIC / IDESG.

A health service provider who is unwilling or unable to accept the potential liability of treating a patient who presents with multiple or unverified IDs for healthcare purposes for non-life threatening conditions should not be obligated to provide care under those circumstances.

Final Draft 5 (A. Gropper, MD & T. Sullivan, MD) 12/11/13 1:05 PM ET