Farzad Mostashari, MD, MPH
National Coordinator for Health Information Technology
Department of Health and Human Services
Submitted electronically

Topic: ONC Federal Health Information Technology Strategic Plan 2011 – 2015

Dear Dr. Mostashari:

The management of HIPAAT appreciates the opportunity to respond to the request for comments regarding the Office of the National Coordinator (ONC) for Health Information Technology's Federal Health IT Strategic Plan.

HIPAAT has been pleased to contribute to ONC initiatives dating back to 2007:
- HISPC III: Intrastate and Interstate Consent Policy Options Collaborative
- HITPC Privacy & Security Tiger Team: Consumer Choice Technology Hearing
- HITSP: Security, Privacy & Infrastructure Technical Committee
- NHIN II Forum 5: Consumer Access to Clinical Information Use Case

Strategy I.B.3: Ensure that health information exchange takes place across individual exchange models, and advance health systems and data interoperability.

"The S&I framework will support not only existing specifications for the Nationwide Health Information Network, but also support new meta-data tagged approaches recommended by the President's Council of Advisors on Science and Technology (PCAST) December 8, 2010 report."

PCAST:
"[p45] A key advantage of the tagged data element approach is that it will allow a more sophisticated privacy model, one where privacy rules, policies and applicable patient preferences are innately bound to each separate tagged data element and are enforced both by technology and by law."

While HIPAAT agrees that explicit tagging of data elements for uniqueness greatly enhances the management of patient privacy, crystallizing privacy rules with data elements which cannot be changed according to a patient's subsequent privacy preferences however does not serve an individual's best interest.

For example, a subsequent healthcare encounter may prompt the patient to want to restrict disclosure of individually identifiable health information (IIHI) that they had previously allowed. In another instance, it is conceivable that a patient may wish to permit a greater sharing of their previously restricted IIHI to their own benefit. Further, what about other use cases such as a move to another jurisdiction, power of attorney or change of minor consent formerly by the parent to this patient now

having reached the age of majority or minor/emancipation? An individual's privacy preferences should be able to be changed and adjudicated accordingly at any time.

In support of this objective, the method of marrying a person's privacy policy with IIHI was recognized as a limitation by HITSP over a year ago and documented in their Security and Privacy Technical Note – TN 900 (Version 1.4: 25JAN10):

"The Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Basic Patient Privacy Consents (BPPC) Content Profile (IHE-ITI-TF BPPC) standard supports only a pre-negotiated set of consent policies."

"This constraint is recognized as a gap. There is work ongoing in the standard development organizations (HL7, ISO, OASIS) to fill this gap. The construct will be adjusted as the standards fill the gaps."

This gap has subsequently been filled by SDO work as evidenced by the presentation made by Ms. Ioana Singureanu to the HIT Standards Committee Privacy & Security Workgroup on the work of the HL7 Community-Based Collaborative Care (CBCC) method for consent management on May 14, 2010. (The ONC may recall that both the SSA and VA have made contributions to this standard.)

Meeting Audio:
http://healthit.hhs.gov/media/standards_committee/2010-05-14_standards_ps.mp3

Presentation Slides:
http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911865_0_0_18/StP&S_Consent_Directive_Standards_Singureanu051410.ppt

PCAST:
"[p50] Identity is also a crucial aspect of security. Determining the identity of a principal is commonly called authentication. Except for patient-consumers, all of the principals in the health IT system can be authenticated using physical credentials (such as smartcards), biometrics (such as fingerprints), and a secret such as a password. Requiring two of these three methods, a possible design choice, is termed "**two-factor authentication.**" Credentials could be issued to healthcare professionals by participating institutions and medical-certification agencies. Whenever data are accessed, an audit mechanism records the actions taken by principals, along with the information used to authorize those actions. Credentials can be revoked when necessary."

While HIPAAT believes that two-factor authentication has an obvious role to play in security, it is often falls short of "appropriateness" of access. That is to say, just because one's role (fine grained or otherwise) permits access to an individual's IIDI, does not mean that the access is appropriate from a privacy perspective. In this case, the system often must rely on an audit trail or forensic tools to detect

the activity retrospectively (reactive), rather than prospectively (proactive) as is the case with consent management.

PCAST:
"[p48] It seems likely that the modifications to HIPAA enacted in Subtitle D of the HITECH Act—in particular those that require covered entities to track all disclosures to associates61—will further stifle innovation in the health IT field while offering little additional real-world privacy protection."

As to an auditing method for an Accounting of Disclosures, I would point to the HIPAAT response to HHS Docket ID: HHS-OCR-2010-0009 Request for Information on an Accounting of Disclosures submitted on May 18, 2010.

We hope these comments are of some benefit and wish to express our appreciation for the opportunity to be part of the process.

Sincerely,

Kel Callahan
President & COO
HIPAAT International Inc.