



Observations on PCAST Report

January 24, 2011

In December 2010, the President's Council of Advisors on Science and Technology (PCAST) issued a report entitled, *Realizing the Full Potential of Health Information Technology to Improve Healthcare for All Americans: The Path Forward*. At a high-level, the PCAST report recommended that the federal government facilitate the nationwide adoption of

- a universal exchange language for healthcare information (an XML variant, for example) and
- a digital infrastructure for locating patient records at a "data element" level while protecting patient privacy.

As envisioned, no universal identifier or national database of healthcare records is required for this proposed approach. Further, PCAST recommended that Office of the National Coordinator (ONC) and the Centers for Medicare and Medicaid (CMS) develop guidelines to spur adoption of this exchange language.

The PCAST report concluded that to build and maintain the public's trust in health IT includes comprehensive privacy and security protections that:

- Are based on Fair Information Practices.
- Set clear rules on how patient data can be accessed, used, and disclosed, and that are adequately enforced.
- Include an individual's right to have some meaningful choice in how that information is shared; he or she must be able to understand the flow and uses of information in order to make informed choices.
- More persistently honor individual privacy preferences.
- Provide significantly better security than traditional paper records. This will include a well-designed combination of:
 - Encryption of data when stored and transmitted,
 - Identity, authentication and authorization,
 - De-identification for research purposes,
 - Audit capabilities, and
 - Administrative, civil, and criminal penalties.

With regard to security and privacy, PCAST recommended that the Department of Health and Human Services (HHS) convene a high-level task force to develop specific recommendations on national standards that enable patient access, data exchange, and de-identified data aggregation for research purposes, in a model based on tagged data elements that embed privacy rules, policies and applicable patient preferences in the metadata traveling with each data element.

We were asked to compare the PCAST recommendations to ONC's Privacy and Security Tiger Team (TT) existing recommendations to look for possible synergies and identify open issues that may need further discussion. The following table identifies key areas of overlap and our detailed analysis.

The MITRE Corporation
Working in the Public Interest

Observations on PCAST Report

January 24, 2011

PCAST Finding	TT Recommendations	Analysis
Fair Information Practices:		
To build and maintain the public’s trust in health IT requires comprehensive privacy and security protections that are based on fair information practices. (p. 46)	All entities involved in health information exchange—including providers, third party service providers, and other intermediaries—should follow the full complement of fair information practices when handling personally identifiable information. (Letter dated 8/19/2010; Policy and Technology Framework)	TT recommendations appear consistent with PCAST observations.
Clear Data Rules:		
To build and maintain public trust requires comprehensive privacy and security protections that set clear rules on how patient data can be accessed, used and disclosed, and are adequately enforced. (p.46)	<p>TT recommended:</p> <ul style="list-style-type: none"> • Limitations on the collection, use, retention, and disclosure of personally identifiable information by third parties involved in exchange. (Rec. 1; 8/19/10) • That public health and quality reporting by providers (or HIOs acting on their behalf) should take place using the least amount of identifiable data necessary (Rec. 5; 8/19/10) • That the exchange of identifiable health information for “treatment” should be limited to treatment of the individual who is the subject of the information, unless the provider has the consent of the subject individual. (Rec. 5; 8/19/10) 	TT recommendations appear consistent with PCAST observations. (TT recommendations provide further detail on implementation of fair information practices.)

Observations on PCAST Report

January 24, 2011

PCAST Finding	TT Recommendations	Analysis
Transparency, Notice, and Patient Education:		
<p>A patient cannot make meaningful choices unless he or she understands the flows and uses of information. While face-to-face counseling on privacy choices should be available, most patients will probably educate themselves. (pp.46-47)</p>	<p>One of the TT core values is that transparency about information exchange practices is a necessary component of establishing credibility with patients. The TT recommended the use of layered notices to improve clarity and emphasized that providers should be encouraged to discuss information exchange practices with patients, particularly when there is a new significant development, such as “indirect exchange.”¹ (10/20/10)</p>	<p>TT recommendations appear consistent with (and are more detailed than) PCAST. <i>Note:</i> TT recommendations place greater emphasis on the role of the provider in educating patients.</p>
Patient/Provider Choice in Health Information Exchange:		
<ul style="list-style-type: none"> • With respect to data element access services (DEAS)—which locate patient information and bring it together on the provider’s desktop—patients would have the right to restrict the types of data elements indexed at all, or could opt out of the DEAS completely (although such a choice might negatively impact that patient’s future care). (p. 42) • PCAST recommended that HHS modify “meaningful use” to incentivize providers’ adoption of a tagged data element format. (p.73) 	<ul style="list-style-type: none"> • The patient should be provided with an opportunity to give meaningful consent before a provider releases control over exchange decisions. If the patient does not consent to participate in an exchange model that triggers consent, the provider should, alternatively, exchange information through directed exchange. (Rec. 3.2; 8/19/10) • Stage 1 Meaningful Use is a voluntary program; ONC is not requiring providers to participate in any particular health information exchange. (Rec. 3.5; 8/17/10) 	<ul style="list-style-type: none"> • TT recommendations appear consistent. (Note: TT recommendations specify that patient consent be provided <u>before</u> a provider releases control over exchange decisions; PCAST position on the timing is unclear.) • Both PCAST and the TT cite meaningful use as the mechanism for incentivizing a national approach to health information exchange; neither is suggesting that providers be compelled to participate.

¹ The Policy Committee has not yet adopted these recommendations.

Observations on PCAST Report

January 24, 2011

PCAST Finding	TT Recommendations	Analysis
Better Informed, Meaningful Consent:		
<p>A universal exchange language can potentially allow patients to make better informed, persistent privacy choices not just in the rush of a medical encounter but reflectively and in an informed manner. Patients will probably make choices through a web interface, where they will be able to change their choice at any time. (pp. 46-47)</p>	<p>When required, patients should be able to exercise <i>meaningful consent</i> to their participation in an exchange. Specifically, meaningful consent:</p> <ul style="list-style-type: none"> • Allows the individual advanced knowledge/time to make a decision. • Is not compelled, or is not used for discriminatory purposes. • Provides full transparency and education. • Is commensurate with the circumstances. • Must be consistent with reasonable patient expectations for privacy, health, and safety; and • Must be revocable. (Rec. 3.3; 8/19/10) 	<p>TT recommendations focused on consent with regards to participation in health information exchange and are consistent with PCAST observations re: DEAS (although, as noted above, it is not clear from the PCAST report that patients would be allowed to make a choice about whether or not their data is indexed in a DEAS in advance). Also, the TT recommendations provide more detail on what makes choice “meaningful.”</p>
Granular Consent:		
<p>An exchange language based on tagged data elements allows for finer-grained individual privacy preferences to be more persistently honored. (p. 46)</p>	<p>The TT has recommended that all participants in health information exchange should follow the fair information practices when handling personally identifiable information. These principles include the individual’s right to consent to identifiable health information exchange. However, the TT concluded that the technology for supporting granular patient consent is promising but is still in the early stages of development. It recommended that ONC specifically pilot technological approaches for honoring granular consents; and in the meantime, patients should be educated about the extent to which their requests can be honored. (Rec. 4; 8/19/10)</p>	<p>TT recommendations could be read to be consistent with PCAST observations if ONC pilots metadata tagging as an approach to implementing granular consent.</p>

Observations on PCAST Report

January 24, 2011

PCAST Finding	TT Recommendations	Analysis
Security:		
<p>A well-designed combination of encryption, authentication, authorization, and for research purposes, de-identification can yield a health IT infrastructure that is secure, and where all principals are auditable. Technical security must also be augmented by administrative, civil, and criminal penalties to deter misuse and negligence. (p. 51)</p>	<p>The TT observed that in a digital environment, robust privacy and security policies should be bolstered by innovative technological solutions that can enhance our ability to protect information. This includes requiring that electronic record systems adopt adequate security protections (like encryption, audit trails, and access controls). (TT letter dated 8/19/10)</p> <p>The TT has begun to address authentication (see following section for additional details) and plans to address additional authentication issues, research, and de-identification.</p>	<p>TT recommendations initially appear consistent with PCAST observations. There may be a need to further explore the particular approach recommended by PCAST.</p>
Authentication:		
<p>Identity is a crucial aspect of security. 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-factor authentication is a possible design choice. 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. (p.50)</p>	<p>The TT evaluated trust rules at the organizational or entity level, and did not address authentication of individual users of EHR systems. With respect to these users, the TT concluded that provider entities and organizations must develop and implement policies to identity proof and authenticate their individual users, which is already required under the HIPAA Security Rule. The TT plans to address patient authentication and may also be addressing special cases concerning user authentication, including software-as-a-service (SaaS), remote access, and mobile devices. (11/19/10)</p>	<p>TT did not take up individual authentication and the other special cases yet.</p>

Observations on PCAST Report

January 24, 2011

PCAST Finding	TT Recommendations	Analysis
Third Parties:		
PCAST recommended the use of DEAS operated by states, large health delivery networks, or the private sector. DEAS will not have access to personally identifiable health information. (pp. 42, 51-52)	The TT recommended limitations on third parties' collection, use, and retention of personally identifiable health information. In addition, third-parties should be open and transparent about their practices. If they have access to personally identifiable health information, they must execute and be bound by business associate agreements. (Rec. 1; 8/19/10)	TT recommendations are more detailed on limits on intermediaries. Before finalizing the TT's transparency recommendations, the TT may want to consider the implications of the DEAS proposal.
Patient Linking:		
PCAST envisions a health ecosystem that would use associations of intrinsic patient-related information to link the appropriate data to specific patients. Since an automated system can use many more than the two factors (such as name and birth date) now often used, it can be correspondingly more accurate. Indeed, "identity resolution" is an established technology, with commercial offerings available. For greater accuracy and convenience in the record-keeping associations, some patients (e.g., those named "John Smith") might elect to index their records by an email address or a reference to a personal health record account, but this would be optional. (p. 42)	The TT recently held a hearing on patient matching issues. A primary theme was that accurate patient linking has a number of benefits but achieving greater accuracy in linking is a challenge. (12/13/10) The TT is currently considering recommendations, which may include: -Standards for demographic data fields; -Internal evaluation of matching accuracy by providers and HIEs; -Research into, and dissemination of, matching best practices; -HIEs establishing and enforcing matching performance parameters for participants; and -Supporting the role of individuals/patients in improving matching accuracy.	The direction of TT recommendations appears consistent with PCAST. Note: there may be a need to explore these issues further when more is known about how the PCAST recommendations are to be implemented.