

Markle Connecting for Health Comments on ONC's "Consumer Preferences Draft Requirements Document"

October 16, 2009

We appreciate the opportunity to provide comments on the Consumer Preferences Draft Requirements Document released on Oct. 5 by the Office of Interoperability and Standards (OIS) and the Office of the National Coordinator for Health Information Technology (ONC).

Markle Connecting for Health is a public-private collaborative to improve health and health care for consumers through connectivity and information-sharing practices that respect privacy. For the past five years, our collaboration has explored consumer consent issues in detail as part of comprehensive frameworks for privacy and security in electronic health information exchanges and personal health information services. Our comments are rooted in the Markle Connecting for Health Common Framework, which was developed with and supported by a wide array of collaborators.

We urge HHS not to pursue a one-size-fits-all use case or technical approach to the issue of consent in advance of policy objectives and requirements. It would be neither practical nor privacy-protective to try to solve the problem of attaining consumer consent through technical specifications that may not take into account various contexts for information sharing, or various relationships that consumers have with different entities. Policies for consent, taken as an important element of a complementary framework for protecting privacy and security, should be articulated. Only with a framework of policies in place can the expectations for technical standards be defined and selected.

The Introduction of the Consumer Preferences Draft Requirements Document says "the need to protect the privacy of health information and promote security is paramount" — a priority that we deeply share.

However, we caution against the assumptions that "the electronic exchange of consumer preferences is an integral step on the path towards enhanced privacy, security and public trust in the exchange of health information" or that "a standardized approach to the exchange and use of those preferences will support common IT implementation as well as interactions among disparate organizations."

These assumptions can be deleterious to progress if they lead HHS to approach consumer consent solely as an interoperability problem to be solved based on technical specifications for a use case or harmonization of technical standards, particularly in the absence of clear policies and policy requirements.

The architecture implied in the Draft Requirements Document appears to require that standardized consumer preferences will be electronically exchanged across heterogeneous entities, integrated into various applications and workflows, and that subsequent changes in permissions will be propagated among data-sharing partners, automatically limiting the use of that data at remote sites. In essence, the assumption is that the consumer's preferences

go with the consumer's data as it flows from entity to entity, and become the rules for re-use every place they appear subsequently. Although this sounds logical in the abstract, it is not a practical experience today. Consumers receive care across a broad range of providers at varying stages of technology adoption and use. The lack of experience of this model across disparate health care settings should give HHS pause before developing it as a technical requirement that would no doubt add cost and complexity to implementations.

In health care, with its wide range in health IT sophistication, there is good reason to doubt any assumption that all care settings will be able to integrate unproven electronic standards for consumer data permissions into their complex and widely varying clinical and business workflows.

Tellingly, the model of attaching permissions electronically to data has proven very difficult to implement in other sectors. For example, the experience of the media industries in trying to specify use preferences embedded in files (Digital Rights Management, or DRM) has been poor. DRM raises costs, lowers interoperability, stifles innovation, and has proved a poor defense against the recipient of the data circumventing the constraints.

DRM fails because it is not a defense against an outside attacker, but against the recipient of the data, who must be allowed to see it in order to use it. In this case, technical standards can't be used alone to create the right outcome, because technical standards on their own are not the right tool for this particular goal. In the case of securing health care data, the remote holder of the data must be constrained by policy obligations, oversight, and enforcement, rather than with standards for codifying preferences.

Instead of treating consumer preferences as a technical issue, HHS should:

1. **Approach consumer preferences predominantly as a policy question:** Rather than creating requirements based on a use case that assumes a specific architecture or set of applications, HHS would better serve its purpose by focusing on the key policy questions at stake. HHS does not want to be in a position in which technical standards set de facto policies, especially when dependent on unproven architectures across as diverse a sector as health or create technical dependency on a narrow set of applications.

In every health care entity, health information exchange, personal health information service, etc. — policies must be set for when, and under what circumstances, consumer information may be captured, used, or disclosed to other organizations. Ultimately, it is the responsibility of the entity that holds the consumer data to determine whether its use or its disclosure of the data complies with law, conforms to its own policies, and satisfies reasonable expectations of consumers. When the consumer's data are shared with a secondary receiving organization, that secondary organization must then do the same. Although not perfect, this approach has the advantage of being understandable and implementable.

For it to work, it is not necessary to establish every detail of every policy across the country, but the basic rules of the road should be set for how personal health data will be handled, and a set of accountability and enforcement mechanisms should be established to protect consumers and merit their trust. With clear policy expectations in

place, there is a greater likelihood that technology and standards can innovate to advance consumer and provider preferences over how personal health information is handled.

2. **Refrain from trying to solve consumer preferences in isolation:** A privacy approach that rests predominantly on consumer consent in isolation can have the unintended consequence of providing weak protection for consumers. While consumers must be informed about and agree with how health information is being collected, used, or disclosed, codifying permissions cannot be a substitute for a comprehensive approach to privacy that protects consumers and builds trust. A complementary set of privacy and security polices — rooted in Fair Information Practices — is needed to provide meaningful protection to consumers, including transparency, audit, use limitation, collection limitation, security, and enforcement.

The broad set of collaborators within Markle Connecting for Health have articulated our approach to consumer consent in the following documents:

For the context of health information exchange among professionals using a record locator service, please see:

Markle Connecting for Health, 2006: Notification and Consent When Using a Record Locator Service:

[http://www.connectingforhealth.org/commonframework/docs/P3_Notification_Conse
nt.pdf](http://www.connectingforhealth.org/commonframework/docs/P3_Notification_Conse
nt.pdf)

The following two document reflect a practical approach to consent for networked personal health information services such as PHRs:

Markle Connecting for Health. 2008. Connecting Consumers, Common Framework for Networked Personal Health Information, CP3: Consumer Consent to Collections, Uses, and Disclosures of Information.

<http://connectingforhealth.org/phti/docs/CP3.pdf>

Markle Connecting for Health. 2008. Connecting Consumers, Common Framework for Networked Personal Health Information, CP2: Policy Notice to Consumers.

<http://connectingforhealth.org/phti/docs/CP2.pdf>

Conclusion:

It is a critical priority for HHS to develop clear information policy guidelines against a comprehensive framework to fulfill the expectations of the health IT provisions of the American Recovery and Reinvestment Act of 2009. There is good reason for pilot experimentation of technical standards that help information to flow according to the consumer's needs and wishes.

However, it is premature to commission or endorse a technical standard for propagating consumer data preferences across networks, particularly if that standard assumes that all applications will be able to pass the consumer's consent along with the consumer's data, and process changes to those permissions each time information is obtained.

The burden to ensure that technical requirements are implementable and derive significant benefits to consumers across heterogeneous settings should be high. Because this burden is unmet, we recommend that HHS reconsider focusing its efforts on prioritizing a complementary approach to setting policy expectations and information policies through appropriate and accountable processes.