



June 04, 2008

Interoperability and Privacy: Are They Mutually Exclusive?

by Thomas H. Lee M.D.

Just when you thought all was harmonious in the land of open-source and socially collaborative Web 2.0, Facebook recently announced it would no longer allow Google's Friend Connect application to access Facebook users' data over "concerns about privacy."

According to Facebook engineer Charlie Cheever, "In the past, when we found applications passing user data to another party (for instance, to ad networks for the purpose of targeting), we suspended those applications and worked with those developers to ensure they respect user privacy. Now that Google has launched Friend Connect, we've had a chance to evaluate the technology. We've found that it redistributes user information from Facebook to other developers without users' knowledge, which doesn't respect the privacy standards our users have come to expect and is a violation of our Terms of Service."

For those not familiar with Google's Friend Connect, it's an interoperable application framework that allows users to bring their social networks and information to other sites without having to rebuild their social network information. As described by Google to potential beta hosts, "Google Friend Connect lets you grow traffic by easily adding social features to your Web site. With just a few snippets of code, you get more people engaging more deeply with your site."

Most view this move by Facebook as not for the sake of privacy (after all, this is the same company that created Beacon, an application where third-party sites were allowed to send unauthorized notices to friend networks in Facebook) but rather for the sake of maintaining control of user and social network data.

As odd and remote as the turf war for friendship networks may seem, the case helps illustrate some of the pivotal issues that could potentially impact the national roadmap to interoperable, private and secure health information. If powerhouses like Google and Facebook can't even reconcile how information about friends should be shared, can we expect anyone to do the same with sensitive health information? Who will own your patient data? How will it be shared? And who will enforce privacy? Ultimately, are interoperability and privacy mutually exclusive?

Interoperability Defined

Interoperability, as a concept, is very powerful. Being able to effortlessly view and transact information from disparate sources is dangerously seductive. Who wouldn't want everything at their fingertips? But the reality, as we know, is quite different. One of the difficulties arises from simply trying to define what is meant by interoperability. To most, the term is defined along technical dimensions:

"In health care, interoperability is the ability of different information technology systems and software applications to communicate, to exchange data accurately, effectively, and consistently, and to use the information that has been exchanged." - National Alliance for Health Information Technology

"Interoperability means the ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of health care for individuals and communities." - Healthcare Information and Management Systems Society

However, technical interoperability, in and of itself, does not make for a fully interoperable system. Once a system can share information effortlessly, one needs to determine how that information should be shared.

A functional level of interoperability needs to be defined. Whose information is available and how is that information shared with others? How is individual privacy protected while enabling maximal sharing of data across systems? Can information be shared across secondary parties or just within a controlled framework?

These are just some of the issues facing Facebook and Google today. Without clear consensus, health care could face a similar path, potentially devolving into a complicated patchwork of functionally non-interoperable systems in the future.

The Dissonance of Functional Interoperability

At first glance, functional interoperability appears to be relatively achievable, certainly when compared with the difficult challenges associated with technical interoperability. It's simply a matter of developing sharing rules, privacy regulations and authentication protocols, right?

A deeper look suggests that simply might not be the case. Information is a valuable asset both to individual consumers and to commercial vendors. However, it resides in many disparate locations, and the tools for aggregating and sharing that information cannot be readily developed by individuals themselves. Thus, individuals are inherently dependent on third-party organizations such as vendors to host and provide that information.

Though vendors are the most able to offer these information services for the benefit of the individual, they must also support these services with a viable business model. Such business models can range from ad-supported revenue to subscription and transaction-based fees, but the underlying principles are universal: information is more valuable to an organization when it is more complete and more unique than what other organizations can offer.

It is this simple principle that not only creates disincentives for sharing information with competitors and other related organizations (as in the case with Facebook), but also fosters incentives for individuals to disclose as much as they can about themselves, despite concerns about privacy.

The less information individuals share with vendors and other related parties due to privacy concerns, the less valuable the product/service becomes to the vendor. A company with online traffic from 20% of all known diabetics will be worth more than double that of a company with the

same volume of diabetic traffic but with only half reporting themselves as such due to privacy concerns.

Adding to the complexity, there are capitalist forces that promote interoperability at the expense of privacy (reselling data to third parties, transaction-based models) as well as privacy at the expense of interoperability (corporate consolidation/oligopolies, privacy-based subscription services). It is this fluid, complex dynamic that we're just beginning to see in the social networking space. And, as the stakes get higher, it's unlikely that it will get any simpler in the future.

Toward Resolution

How then do we foresee any resolution? Are we doomed to witness endless interoperability/privacy turf wars between Google Health, WebMD, Revolution Health and a myriad of upstart social network and health information service companies? Possibly. Unchecked, the forces seem to be moving us in that direction.

Nevertheless, it's possible that there are a few scenarios in which a more functional and balanced system could emerge.

One possibility is if the rules of engagement for using and sharing sensitive health information were to be more centrally or federally controlled. Currently, many information service vendors including Google Health are not subject to HIPAA or other privacy/sharing regulations. Instead, we must rely on privacy policies and trust the shareholders and executives of a corporation.

By mandating a uniform playing field for all vendors, some element of protection could be created for how information must be shared or not be shared. Though appealing in concept, this may also stifle the incentives and desire for developing such services in the first place.

Another possibility is if one or a few companies ultimately became successful, gaining massive traction and adoption. This would allow the select few to shape the playing field from the private sector. Such a model could promote a balance of interoperability and privacy without huge detriments to the business because of strong market powers. As we've seen with Microsoft, however, this route has both its benefits and costs.

Lastly, a variant of the above with a neutral third party with no economic incentives for profiting on information services could step in and serve as a utility for managing and brokering sensitive health information. This could take the shape of a not-for-profit or a foundation/government-sponsored entity. The concern with this approach would be the ability and motivation of the entity to constantly evolve and develop its service offering.

Regardless of the path we ultimately travel, there is still much work to be done. Technical interoperability is still many years in the making. And Google and Facebook have yet to clash in the next round of battles. But given the challenges that lie ahead, it is in our best interest to begin considering how the actual work toward functional interoperability can be achieved. We need to start asking ourselves: Who do we really trust with our health information?

More on the Web:

- [HIMSS' definition of interoperability](#)
- [National Alliance for Health IT's definition of interoperability](#)
- ["Sudden Disconnect Over Social Networking Deal"](#) (Whoriskey, *Washington Post*, 6/2).

© 1998-2008. All Rights Reserved. iHealthBeat is published daily for
The California HealthCare Foundation by The Advisory Board Company.