Breakout Session 2: IT Security Breaches and Implications for the Enterprise

Moderated by Eric Johnson, Benjamin Ames Kimball Professor of the Science of Administration and Director, Glassmeyer/McNamee Center for Digital Strategies

Healthcare landscape: public opinion, legislation, and technology

Q: What is different about the healthcare industry compared to other industries?
In terms of security and especially privacy concerns, the healthcare industry is different from other industries such as banking. "Healthcare data is like a genie in a bottle". Once it gets out, it cannot be put back. Furthermore, the sensitivity of the data varies for individuals, and also depends on who can access the information. Any error or leak with someone's financial data can be compensated and the consequences can be minimized or even eliminated. However, with healthcare data, the consequences cannot necessarily be controlled. An error can prove fatal or a data leak can stigmatize a person for life.

Concrete public policies (about data sharing and data storage) can create consistency and bring some certainty in public opinion, making people comfortable with data sharing. People should be comfortable sharing data, because patients don't necessarily know what is relevant information, and if they are not comfortable sharing data with doctors, they may hide vital information putting themselves at risk. There is something to learn from privacy policies in social media (e.g., Facebook, Twitter) about how privacy policies can evolve and how people learn and understand privacy sharing policies over time.

Q: Has there been any change in the mindset about healthcare security?
People don't vote on privacy, but that doesn't stop legislators from acting on privacy issues - to drive their points, to drive fan-fare, etc.

Peoples' response to whether they care for privacy depends on how we ask questions in a survey. But in general it has been observed consistently that people do not care about privacy (as much as we would like to think) and are willing to sharing for some (often minimal) gains.

We often claim that giving patient access to their health records will improve their healthcare (as the patient gets more involved). However, researchers have studied this question (whether giving access to their health records, changes a patient's behavior towards improving their health) since the 1960's, and have not found a connection. People who have access to their data, do not do much with it. It is an open question whether this remain true going forward.

People have an (old) mental model for the healthcare industry. They trust their doctor to take care of their health records, and this came up in a study with 60 patients, where patients were asked if they had any concerns/experiences with how their health information is shared. Very few people had concerns, and when they talked about how their information is handled, they think their physician is taking care of their data. This model was good in the old days, but with things going electronic, the doctor does not control the data sharing/access. People don't have this mental model yet, and we need policies and awareness among people to push this model to them.
In banking, a bank has direct relationships with the customers, but in the healthcare industry hospitals don't have a direct relationship with the patient (doctors and nurses have a direct relationship with patients). Only clinicians and payers have relationships with patients. This is slowly changing as we move towards new healthcare delivery models.

Patients rarely change hospitals due to privacy or security issues. They care more about healthcare services rather than security/privacy issues. And some patients seem to care more about customer service than healthcare quality. For example, in a survey in which patients were asked, “what can hospitals do to improve the healthcare?” some patients said they would feel really good if the caregiver (doctor/nurse) knew their name.

Until breach laws came into effect, there were few consequences for breaches. Since then there have been a number of minor breaches, but nothing major. This could be because the PHR industry is relatively new and small.

Policies are also driven by public opinion, and currently the public perceives the healthcare industry as health service, and does not understand the severity of data breaches. One large malicious healthcare data breach will likely change public opinion and bring about new federal policies.

**Q: What changes have there been in the technology landscape?**

The healthcare industry is immature in IT technology, and has always been behind the current technology. Now, it is doing multiple generational leaps, moving to all-electronic, and at the same time, it has to deal with mobility, cloud-services, and consumerization. And, the industry has to make this technology leap, while supporting legacy systems; for instance, basic encryption is not yet wide-spread because legacy systems don't support it, and the legacy system owners lobby policy makers. Cost is a major factor deciding security: to reduce cost, organizations often opt for less secure options.

**Opportunities**

Given new policies (in the making), public perception, and the technology generation leap, there are many challenges, and hence many opportunities. Two popped out - training and usable-security.

**Training:** Humans are typically the weak link in any secure system. It is really hard and painful to make users aware of security and privacy practices. People don't sit through security lectures, but they sit through risks lectures. Therefore, we need to have new training programs that will drive the point of the security and privacy practices to the users. Time is a major constraint for training; employees just don't have time for training.

**Usable security:** To make employees compliant with security practices, there are two important steps: i) to make them aware of the importance of the security practices, and ii) integrate the security mechanisms in their workflow such that it doesn't impact their effectiveness.

In healthcare, employees get point i), because they are aware of doctor-patient confidentiality and that the health data needs to be kept confidential. But we fail at point ii). We continue to see security blunders in healthcare (most infamous of all: passwords on post-it notes), and non-
compliance with other security practices. This is not because people don't want to be compliant, but because the current practices make them ineffective at their job.

There are studies that show employees who feel a higher sense of job satisfaction are more compliant with HIPAA. The take away from the studies is: make sure that the security and privacy practices do not hinder employees jobs, and fit in their workflow well, and they'll be compliant. This calls for usable security technology.