Panel 1: Usability and Healthcare Data Breaches

Chaired by Eric Johnson, Benjamin Ames Kimball Professor of the Science of Administration and Director, Glassmeyer/McNamee Center for Digital Strategies
Panelists: Ritu Agarwal, University of Maryland; Eric Cowperthwaite, Chief Security Officer, Providence Healthcare; Khaled El Emam, Children's Hospital of Eastern Ontario Research Institute; Paul Connelly, Vice President and Chief Information Security Officer, Hospital Corporation of America

Summary of the Panelists’ Presentations and Panel Discussion

The panel began with a series of presentations by Eric Johnson, Eric Cowperthwaite, Ritu Agarwal, Paul Connelly, and Khaled El Emam. After these presentations, there was an open discussion on the challenges of healthcare breaches. Here are some highlights of each of these presentations, then of the discussion, and a short concluding analysis.

Moderator/Panelist Presentations

Eric Johnson (Moderator)

Eric's high-level introduction motivated the problem with data: there were 20 million breaches of PHI as of 5/31/12. These breaches were due to direct or inadvertent failures. One poignant example of an inadvertent failure is the story of Bob Quick, who was photographed while he got out of his car with an exposed agenda facing cameras of the awaiting press. At the time Quick was the most senior counterterrorism officer in Britain. Unfortunately for him, the exposed agenda was at a Secret Clearance-level. He lost his job as a result of the inadvertent disclosure.

In Eric's own research, peer-to-peer file sharing programs that are intended for music serve as a conduit for inadvertent disclosure of PHI. In the post-HITECH world, Eric found 3766 spreadsheets (788 of which were unique) that had healthcare-relevant keywords via such programs. In one case, a hospital chain leaked approximately 20,000 names, each with as many as 82 fields of information per name. The leak was an indirect disclosure stemming from an outsourced collection service.

After the introduction, Eric introduced each panelist.

Eric Cowperthwaite (Panelist)

Eric is Chief Security Officer (CSO) at Providence Health, a very large Catholic Healthcare provider. They have 33 hospitals on the West Coast and they want one EMR to bind them (and by them we mean 12 million records). Providence is currently rolling out EPIC.

One of Eric's main points: the California $1000 fine-per disclosed name forces hospitals to accept a massive amount of risk relative to their budget as we have witnessed with the recent Sutter Health breach.
Eric noted that workarounds are common in healthcare. For example:

- “Print Screen” as a workaround for patient records that cannot be printed
- Excel spreadsheets that are easy to use.

Ritu Agarwal (Panelist)

Ritu is a professor at University of Maryland. She motivated the need to understand how usability affects data security and cited Eric Johnson as a good example of this kind of research. She showed a slide on data flow of PHI through the healthcare system and juxtaposed that with the figure there is $100 billion in identity theft per year. According to her, digital information is more vulnerable because of the volume. She said, however, that the main sources of breach are due to the insider.

In her work, she has four factors that contribute to a potential data breach:

- Interference with clinician workflow
- Poor organization of technology
- Increased cognitive burden of technology
- Poor design of system functions

She concluded by giving an overview of her work to understand technology, process, and people.

Paul Connelly (Panelist)

Paul is the CISO of Hospital Corporation of America. HCA is one of the largest US hospital chains, with 163 hospitals, 109 freestanding surgery centers, 700 physician practices, and 199,000 employees. Paul mentioned that there was a perfect storm for PHI breaches consisting of the following four points:

- Growing volume and value of information
- Growing distribution, access, and communication
- Growing impacts from losses of the data
- Growing threats to the data

He also stated that the workarounds fall into the categories of physical, network, or data. For example, some of the latest products (such as those that are bedside) do not engineer for security. Alas, the security folk do not steer the product development, the doctors do (a point that came out in conversation). Furthermore, Gmail, Dropbox, and all these other cloud/network-based technologies provide superior usability and so Paul quipped it is no wonder that clinicians use these technologies to get their jobs done.
Paul argued that we need to build systems that help clinicians get their jobs done - then we can reduce workarounds and increase security. Specifically we need to design for speed, new technologies, and consistency.

Khaled El Emam (Panelist)

Khaled’s is a professor at Children's Hospital of Eastern Ontario Research Institute. His presentation focused on snooping and peeping. He motivated the example by mentioning love triangles. The reason they are bad news is because ex’s can get PHI of former interests. Furthermore, the current state-of-the-art in audit is to have complaint-driven audit as there are too many audit logs to automatically check.

Khaled explored granular, entry-based locks on components of an EMR as a way to address snooping and peeping. He played Pharma Jeopardy with clinicians to see (even if some fields in the EMR were redacted) whether clinicians can guess what is in those fields based on non-redacted info. Clinicians could because fields are highly-correlated. This makes Khaled wonder about the future of granular locking.

Discussion

Overall the themes of the discussion were (1) workarounds and (2) role-based controls.

Eric J asked about good workarounds, and it was concluded that most workarounds are well-meaning, but without clearly understanding the consequences.

Andy Gettinger from Dartmouth lamented de-authentication as a problem. He had seen examples at hospitals where clinicians used post-its saying “I'm logged-in here” on machines.

Ross Koppel from Penn talked about Fat COWs (where a nurse carried around a movable scanner and finally had to use the attached handheld one because the scanner couldn’t reach everywhere; she failed to notice the alerts about wrong patient on the main machine, when she used the attached handheld scanner).

Jesse Walker from Intel said that IT security addresses 5 percent of the problem. New environments may require new solutions.

Ritu said that out-of-the box solutions were pretty clearly not designed by clinicians. We need to go back to see how clinicians work.

Carl Gunter of Illinois talked about RBAC and how we need to be able to define roles, maybe via audit logs
Sean Smith said that people in large banks have used logs but that the problem is huge. Managers in these large companies lament that they can't just stop the company. He asked about role drift.

Eric Cowperthwaite said it is very possible for a clinical employee to have three different roles on three different days. That creates a major role drift problem in the clinical environment.

Brad Malin of Vanderbilt asked how the current IT situation can be assessed and how we plan to deal with the existing issues; Paul replied the solution depends on the rigidity of the technology and that currently, IT folks spend time in hospitals to observe usage of their systems.

**Analysis**

Overall the discussion motivated the need to prevent breaches. Inadvertent disclosure was the cause of many such breaches, and workarounds often cause inadvertent disclosure. We need to understand the workarounds.

We need to understand workflows and build technologies that support clinician workflow. Perhaps this is why people keep so much information in Excel, so that they can define their own data schema that out-of-box EMRs cannot support. Nonetheless, these organizations are dynamic, role drift occurs quickly, and so rather than thinking about "paving common paths/workflows that we observe", perhaps we should think about technologies that allow clinicians to encode data within workflows, and then migrate that data as their needs and technologies change. We should be building lightweight technology that can adapt to the environment (including the hospital and technology landscape) rather than thinking about paving workflows into concrete pathways that last for years.