

**Testimony of
Robert Seliger
Chief Executive Officer
Sentillion, Inc.**

For

**The U.S. House of Representatives
Committee on Veterans Affairs
Subcommittee on Health**

June 21, 2006

Chairman Brown, Mr. Michaud, distinguished members of the Committee, thank you for the opportunity to testify before you today on a subject of critical importance for our nation's veterans, but also to every citizen—how to safeguard sensitive personal health and related information from external and internal security threats. My name is Robert Seliger and I am co-Founder and CEO of Sentillion. Sentillion is the industry leading provider of Identity and Access Management solutions to hospitals and healthcare systems. Everyday, Sentillion helps hundreds of institutions and hundreds of thousands of physicians, nurses, and other caregivers at those institutions employ effective security and privacy practices while also assisting the care delivery process. We are exceedingly proud to say that among these institutions are all 163 medical centers of the Department of Veterans Affairs.

I have twenty six years of experience in the field of healthcare information technology including eighteen years at the former Hewlett Packard Medical Products Group where I served as a senior R&D manager and distinguished scientist and eight years at Sentillion, a company founded to serve the healthcare industry. I have served on numerous healthcare standards committees and have chaired a variety of healthcare industry initiatives. Recent activities include serving as the chair for the Healthcare Information Management and Systems Society (HIMSS) steering committee for Integration and Interoperability, and serving as an advisor on standards uptake for the Pan-Canadian Electronic Health Record Standards Steering Committee. My degrees are in electrical engineering from Cornell University and Computer Science from MIT.

Over the past several weeks, this Committee has spent many hours examining why personal information of Veterans was lost and what can be done to effectively safeguard the privacy and security of this data in the future. You have focused a great deal of attention on what management policies and technical solutions need to be implemented at the enterprise-level to prevent another breach. It is a hugely complex challenge as you have found, but your oversight role and your responsibility to our nation's veterans demands nothing less.

Today I want to focus on one aspect of that complex challenge that is particularly critical in the clinical setting. That is, how we can we safeguard patient data without also impeding the clinical work flow?

The terms security and privacy are often used in conjunction so as to imply that they mean the same thing. Actually, they do not. Security means that people who do not have the proper permissions are not allowed to see information, or access systems, even if they try to do so. Privacy means that people who do have access do not intentionally or even inadvertently share sensitive information with others. Breaking into a hospital's computerized medication order entry system in order to maliciously change the dose of a medication with the intent to do harm is an example of a security breach. Talking by name with a medical colleague about a patient's diagnosis in an elevator occupied by other random people who are in earshot is an example of violating the patient's privacy. Protecting patient security *and* privacy are key concerns for healthcare organizations, but different measures are required.

One of the key reasons that different measures are required is the fact that in healthcare, the foremost mission of caregivers is to care for patients. By definition, practicing safe and effective medicine will always take precedence over concerns for security and privacy. Our nation's nurses and physicians are among the smartest, most highly trained people in the world. This fact, coupled with their deep sense of mission, will compel them to avoid, work around, and challenge policies that impede the care delivery process. This is because the care delivery process, by its very nature, requires immediate information access and the constant sharing of information with others.

As a simple example, the seemingly trivial task of logging off of a computer after a physician or nurse is finished reviewing a patient's record is almost never done in the hospital. Logging off takes too long to do, is often forgotten when more pressing activities occupy the caregiver's attention, and is often viewed as discourteous because it will require that the next caregiver who wants to use the computer in order to access patient information would need to take the time to log on. A caregiver in a busy hospital might need to log on and off fifty to one hundred times a day. At a minute or two for each log on and log off, you can quickly see how this seemingly trivial best practice is avoided because it interferes with the pace of providing care. And so our nation's physicians and nurses practice good healthcare but leave millions of personal computers across the country open to access or even simple perusal by any passerby – from other healthcare workers who have no valid reason to view the information, to other patients to people visiting patients, to anyone else who might be in the hospital.

My younger brother fell ill several years ago and wound up in the intensive care unit of a Massachusetts hospital. Fortunately he is now fine. I arrived soon after he was admitted. There was not much to do but worry and wait while my brother lay in front of me, intubated and unconscious. That's when I noticed the elegant flat panel display next to his bed. What then caught my eye was that on the display was an application that I spent many years of my life developing when I worked for Hewlett Packard. The application was unlocked and the data on the display could be easily seen by anyone, including me, my brother's wife, and his boss who came to visit later that day. Even though I was curious about the application and wondered if I could remember how to use it, I did not look at the display, because that would have been an invasion of my brother's privacy.

More recently, while visiting one of our customer hospitals with a colleague, we got lost in a labyrinth of corridors and asked a nurse who was walking towards us for directions. She pointed us to a hallway that led through a women's clinic. Outside of every patient's room was a computer on a mobile cart. No one was using these computers, but they were unlocked and each display presented personal health information about one of the patients. My colleague and I averted our eyes and simply found our way out of the building. This is another example of disrespect for patient privacy.

In both of these cases, as best I could tell there were no hackers or criminals in sight. My guess is that the networks upon which these computers were connected were also reasonably secure and protected from unwanted external access. Nevertheless, in two

state of the art healthcare facilities, during normal working hours, in broad daylight, many doors (so to speak) to sensitive patient information were left wide open.

I would like to assert that the real security and privacy challenge that the healthcare industry faces are not attacks from outside, but rather transgressions from within. The question is, "How do we as a nation change this situation without compromising the care delivery process?" How do we improve the security and privacy of patient information without impeding access to the caregivers who need immediate access to the information to care for patients?

The answer is that security and privacy practices that we ask our caregivers to follow must fit with their workflows. Better yet, these practices should enhance the workflows. Let me give an example. What if we could reduce the time it took for a caregiver to log on or log off from minutes to just a few seconds? Data that we have from a study we conducted shows that under such circumstances, nurses in one hospital who only logged off fifty percent of the time were now doing so one hundred percent of the time. And physicians, who were not logging off at all, were now doing so eighty-six percent of the time. I have attached as an Appendix a more detailed description of this issue.

This change in behavior was not due to a new policy or the threat of punitive measures. Rather, we simply made it easier for caregivers to be good security and privacy citizens. By the way, they were also more likely to access the information they needed to make timely and informed decisions from a computer than by looking at paper records, asking a colleague, re-performing expensive tests, or making decisions without information that is available but not used because electronic access is too slow or cumbersome. In other words, security and privacy solutions that are thoughtful and that support the caregiver's workflow can also result in safer, more effective, and less costly healthcare.

I make bold claims and you might be wondering if what I am saying is too good to be true. The basis for these claims is not a specific magic technology or product, but rather the assertion that in healthcare, people want to do the right thing. This is about making sure that things we do to keep the bad guys out do not effectively prevent letting the good guys in. This is about making sure that we engineer healthcare information technology solutions from a systems perspective and not attempt to force upon healthcare organizations mechanisms that make sense for office or other types of business environments, but which do not make sense for healthcare.

People often ask me why I have committed my career to the healthcare industry. I am a businessman, and certainly part of my answer is that it is how I make my living. However, I do have an idealistic streak, and part of my motivation is that I also want to make a difference. One of the fascinating things about working in healthcare is that virtually everyone I meet has the same personal commitment. This is particularly noticeable at the VA, where I have had the privilege to work with physicians, nurses, and IT staff for many years. I realize that the VA has had its challenges, but I have never once thought that these challenges were due to a lack of commitment or caring.

Delivering effective healthcare is an intense and complicated process. It is also a truly mission critical process. Our industry must find the right balance between applying security and privacy measures that are known to work and applying measures that could be detrimental to patient care. We can assert, for example, that every caregiver must have a password for each application that they use, but what in fact are we asking of our caregivers if they need to remember ten different passwords and enter each one in dozens of times a day? To truly safeguard patient security and privacy requires a broad set of measures. These measures include not only good network security and the appropriate encryption of data, but also involves tools and mechanisms that enable good people, well meaning caregivers, to do their jobs without compromising patient health, patient security, or patient privacy.

Mr. Chairman, this concludes my remarks. Thank you for the privilege of speaking before you today. I am happy to answer any questions the Committee may have.

Appendix: Additional Testimony

Barriers to Effective Security and Privacy Practices in Hospitals

The following steps illustrate what is required today for a typical physician to actually practice proper security and privacy within the four walls of a hospital. In this scenario the physician is attempting to review a patient's test result from a computer located in an intensive care unit:

Step	Description	Cumulative Time (estimated)
1	Log onto the computer by entering network username and password.	00:04
2	Wait for computer logon to be completed.	00:34
3	Launch a results reporting application to review patient's test results.	00:35
4	Wait for results reporting application to present its logon screen.	00:40
5	Look up username and password on index card carried in shirt pocket. (Note: this is not the same username or password as that for logging onto the network.)	00:45
6	Enter username and password for the results reporting application.	00:49
7	Wait for the logon to the results reporting application to be completed.	00:55
8	Using the results reporting application, select the patient of interest from the list of available patients.	00:59
9	Select the data of interest (e.g., the latest lab test results) and wait for the data to be displayed.	01:03
10	Based upon the test results, decide which medication dose to adjust.	01:13
11	Launch the medication order entry application.	01:14
12	Wait for order entry application to present its logon screen.	01:19
13	Look up the necessary username and password on index card carried in shirt pocket. (Note: this is not the same username or password as used for logging onto the network or for logging onto the results reporting application, but is the same index card.)	01:24
14	Enter username and password for the order entry application.	01:28
15	Wait for the logon to the order entry application to be completed.	01:32
16	Using the order entry application, select the patient of interest from the list of available patients.	01:36
17	Select the data of interest (e.g., the current set of	01:40

	medications) and wait for the data to be displayed.	
18	Select the medication of interest and adjust the dose.	01:50
19	Log off of the order entry application.	01:53
20	Log off of the results reporting application.	01:56
21	Log off of the computer (ALT-CONTROL-DELETE, then select Log Off).	02:00

In this example, 20 seconds of productive work required 1 minute 40 seconds of additional tasks pertaining to signing on, selecting the patient of interest, and signing off. A typical physician might need to access a computer thirty to fifty times a day, meaning that between a half hour and an hour is spent on the minutiae of logging in, selecting the patient, and logging out. In addition, while the physician is trying to focus on clinical decisions for the care of patients, she has to keep focusing on remembering which usernames and passwords are used for which applications.

In the absence of a more productive solution, the vast majority of physicians will not perform these tasks. The same situation generally plays out as illustrated in the following scenario:

Step	Description	Cumulative Time (estimated)
1	Walk up to an unlocked computer.	00:00
2	Using the results reporting application, which is already running under another person's log on, select the patient of interest from the list of available patients.	00:04
3	Select the data of interest (e.g., the latest lab test results) and wait for the data to be displayed.	00:08
4	Based upon the test results, decide which medication dose to adjust.	00:18
5	Handwrite the new medication order on a paper form and hand it to a nurse.	00:28
6	Leave. The computer and the results reporting application (which is still displaying the patient's data) is now visible and available for anyone to use.	00:28

The same 20 seconds of productive work is encumbered by only 8 seconds of additional tasks. This overhead represents between four minutes and six minutes of overhead each day and require few interruptions to the physician's thought process about patient care. Clearly the cost of complying with security and privacy best practices is too great for most physicians to tolerate.

Possible Solutions

The technology now exists to enable caregivers to be productive while also performing proper security and privacy practices:

- Single Sign On enables a caregiver to enter their username and password (or other credential, such as a fingerprint or smart card) only once per logon, and as they open applications they are automatically signed on. This obviates the need to remember usernames and passwords, to have to carry them on “cheat sheets”, or to even type them in.
- Single Patient Selection enables caregivers to select a patient of interest once, in any application, and in so doing automatically tune all of the other applications in use to the selected patient’s records. If an application is newly launched then it automatically tunes to the selected patient’s records.
- Single Sign Off enables caregivers to sign off of all of the applications that they have logged on to, and to sign off of the computer, all in one easy button click.
- Fast User Switching enables caregivers to share the same computers so that the time it takes to sign on to the computer and the underlying applications is dramatically reduced. Some techniques employ the capability to keep applications running “hot” and ready to go as soon as a valid user logs on to the computer. The applications are not visible until the computer is unlocked by a valid user.

Solutions that support these behaviors are in use throughout the United States. The VA presently employs Single Patient Selection, has the capability to deploy some elements of Single Sign On, and is evaluating the addition of Fast User Switching and Single Sign Off.