

Attendees:

Leo Bodden, Reidar Bornholdt, William Cochrane, Frank Fries, Manny Gonzalez, Charlotte Nichols, Karen Pagliaro, B.J. Pinsky, Ilya Pisman, Brent Powers, Soumitra Sengupta, Bob Sideli, Bill Wozniak, John Zimmerman

Impact of American Recovery and Reinvestment Act (ARRA) on Healthcare IT

- Robert Sideli, Chief Information Officer, CUMC IT, opened the discussion on the increased compliance around HIPAA in the new ARRA (commonly referred to as the Stimulus bill). Dr Sideli drew the attention of the attendees to a few important points from [ARRA](#), quoting extensively from the [Gartner report's](#) interpretation of ARRA's impact on Healthcare IT. A few points presented for discussion by Dr Sideli:
 - Patients now have the right to get an electronic copy of their health information, not just paper records. Security provisions and penalties now apply to business associates and employees of health care providers.
 - Notification of breaches to the affected patients: Covered entities must notify the Secretary immediately of breaches that involved the information of 500 or more individuals, and annually of all breached that involve less than 500 individuals; the Secretary then posts on an HHS website a list that identified each CE that has had a breach incident involving 500 or more individuals.
 - Higher penalties on HIPAA if the violations are willful, penalties may exceed \$1 million.
 - A part of the monetary penalties may also go to the individual whose records were breached within three years.
 - Business associates and Personal Health Record (PHR) vendors now face compliance issues. Patients can also ask for individuals who saw or had access to their healthcare information.
- Based on the points Dr Sideli put up for discussion, the attendees felt that these provisions can impact CUMC IT in different scenarios and discussed a number of them at length:
 - Brent Powers, Manager, Pathology suggested that CUMC IT should explore a policy that restricts use of thumb drives or laptops for carrying any type of sensitive information.
 - Dr Sideli expressed a thought that it can get very challenging in defining what exactly a breach is. He cited a scenario when an operator's monitor is open and someone else looks over, gets a chance to read patient information, and divulge this information to a third party – making the institution and employees liable for damages. Attendees opined that the challenge is to address behavioral issues, not just physical security issues.
 - Dr Sideli said that as CROWN may have time to catch up to the new regulations as the first patient's data was entered into CROWN by Orthopedics in October of 2008. Per ARRA if an EHR system is in place before January 2009, full compliance is required by January 2014, whereas for systems that come in place after January 2009, full compliance is required by January 2011.
 - Dr Sideli also mentioned that while the hospital may have a records department and policies in place, the academic institution may not have policies for safe keeping medical records across all the departments. John Zimmerman from the Dental School of Medicine, said they have policies in place in the dental school.

Information Security: Recommendations, Issues, Technologies, and Training

- Dr Soumitra Sengupta, Chief Security Officer, CUMC IT spoke about the findings from the Security Task Force set up for Information Security Enhancement. Some of the findings from the consultants suggested rigorous improvements in the policy area and involved around information security guidelines as set forth in ISO 27002 and ISO 27099.
- Participants, in conjunction with Dr Sengupta outlined the following areas where strict data leakage prevention steps may be possible: USB devices like thumb drives, web filtering on chat, e-mail, and access to internet sites.
- John Zimmerman spoke of a researcher whom he least expected carrying sensitive data using a thumb drive.
- Dr Sideli spoke about users using Google Docs to store sensitive information and said that with research and clinical trials activities going on there is an overlap and blurring sometimes of what is academic and what is clinical data.
- Dr Sideli and Dr Sengupta jointly presented to the members of the round table options to reinforce information security training by exploring the possibility of using “Soft Sting” operations. For example, sending out an e-mail asking the user to click a link or open an attachment to divulge some personal information; and, if the user did it, direct the user to a web page that chides them gently that they should not be doing it and reinforces security policies. They cited an instance during the recent past where more than five hundred users parted with their passwords based on a phishing e-mail that was sent out to the Columbia community which was luckily contained very quickly without causing any major mishaps by CUMC IT Security.
- Dr Sengupta opined that for controls to be effective they should be coming from top down and concluded that the CUSA group should continue to encourage policy level discussions on standard clinical workstation requirements.

Citrix vs. Microsoft Terminal Services

- John Zimmerman said that they were moving towards using CITRIX for their applications. He said the per license fee from the vendor CDW were very reasonable and affordable.
- Participants evinced keen interest around Citrix and discussed the pros and cons of using Citrix as opposed to Microsoft Terminal Servers. Manny Gonzalez, Director, Core Resources said that Citrix provided more functionality in tracking and managing traffic, had more granular controls at the CPU level, does more in terms of load distribution between applications, and offers a rich experience on the client side for Windows, Linux, Mac, Win CE, iPhone, etc., thereby making it a much better option than Microsoft Terminal Services.

Managed Workstations

- Members of the round table also discussed the idea of using managed workstations for applications like CROWN and discussed the following challenges if managed workstations were to be used:
 - Attaching scanners, webcams, microphones, and using applications other than the clinical applications—as some users wanted to do documents or presentations from those workstations.
- Leo Bodden, Director, CORE Resources, suggested that it may be a good option to give the users managed workstations and then allow the workstation to get locked if they did anything wrong. This can be a deterrent for not using workstations carefully within security guidelines or for the applications they are intended for use.

CROWN

- Charlotte Nichols, Asst Vice-President Information Technology Services, introduced William Cochrane, Project Director for CROWN implementation.
- Bill Cochrane briefed participants that CROWN is now in alpha testing in one department while it is in beta testing in two departments. He said that there are several new enhancements that have come out from beta testers and that beta testing is now on hold.
- CROWN is expected to go live all over CUMC IT by April 2010. Bill Cochrane expects about one thousand workstations in all will be rolled out with AllScripts on them for the project.
- Dr Sideli also spoke about a few issues in CROWN like formatting issues where the pagination was off, the characters did not print properly, or the pages were empty.
- Ilya Pisman, Systems Administrator, School of Nursing wanted to know if there were any resistance issues from users during the implementation of AllScripts.
- Dr Sideli said there were not any and said the only comment he heard from one of the users was that the novelty phase has now moved into the reality phase!
- Dr Sideli cited an example about the feature to store historical data in CROWN. During beta testing, a doctor was able to see information on the history of lymph node issues in a patient who came to see him for a routine pain. This helped the doctor prescribe the right medications to the patient.

Network Infrastructure

- Leo Bodden briefed the attendees as to how the estimates for upgrading network infrastructure in Columbia to support applications like CROWN went thru several iterations. He said there was a significant difference to their original plan to what was finally approved as there were several budgetary constraints.
- Dr Sideli said that the date when the data center would be turned on is not yet fixed.

Conclusion

- Attendees concluded to keep HIPAA compliance issues at the top of the agenda for future meetings.
- They also decided to discuss CUMC IT access issues to the IBM mainframe in the next meeting.

The next CUSA Round table is scheduled for March 26, 2009.