Newsbytes, 8/17

Raymond D. Aller, MD, and Hal Weiner

Health record security at root of personal grid architecture

Imagine the risks credit reporting agencies would face if they did not maintain databases of consumer transactions but instead requested information from various creditors and assembled credit reports from that information in real time. Yet that's how health information exchanges typically work. And that, says William Yasnoff, MD, PhD, a consultant, physician, and computer scientist, is not a safe or effective approach.

Rather than requesting and integrating medical records in real time when patients arrive for care, Dr. Yasnoff advocates storing medical data in patient-controlled, community-based repositories. "Everyone would have an account in a 'health record bank,' and when information is created, it would be deposited," explains the health informatics expert, who is managing partner of the consulting firm National Health Information Infrastructure (NHII) Advisors; former senior advisor, NHII, U.S. Department of Health and Human Services; and president of the nonprofit Health Record Banking Alliance.

"The first question I get is, 'Wouldn't health record banks be magnets for hackers, and what if we lost an entire community's data?'," Dr. Yasnoff continues. At which point he introduces the questioner to his personal grid concept, a hyper-secure architecture for storing health records in separate files, which is an alternative to the relational database concept, based on storing all records in a central encrypted database.

"The problem with a traditional relational database," Dr. Yasnoff explains, "is that the system administrator has access to the entire database. If the master key is lost or stolen, you could lose all the records."

System administrators for the personal grid architecture, on the other hand, do not have access to patient records. Rather than storing all records in one database file, the grid stores each patient's records in a separate file encrypted with its own password. Decryption keys are split into two parts, with one held by the system and the other by the patient to whom the record belongs or by a provider to whom the patient has authorized access.

All users have a login password that provides them with exclusive access to their own user key, which is needed to retrieve the user's record. The system keys are kept in a file encrypted with one of many available daily passwords. All daily passwords are stored in a separate table that is encrypted with a system master password. The act of a user logging in and entering his or her user key triggers the system to decrypt the system key and allows the user to access the user's own record.

But unlike relational databases, which are indexed to facilitate rapid searching, the personal grid can only be searched sequentially. This allows rapid retrieval of individual patient records, but searches across multiple patient records are dramatically slower. However, Dr. Yasnoff says, this issue can be circumvented through cloud computing. "You can speed up the process by doing a sequential search in parallel in the cloud with a large number of processors," he explains. In other words, multiple virtual servers can be allocated to complete parallel sequential searches.

In a paper published in the Journal of Biomedical Informatics (2016;61: 237–246), Dr. Yasnoff demonstrated that for a population of 30 million, the typical search response time for a 500-server personal grid would be about an hour. Yet the increased search time isn't an issue, he contends, because extremely rapid searches are not necessary across populations of patients.

As an added security measure, two system administrators would be required to initiate a global search. Each administrator would have an encrypted USB drive that contains half of each password for the servers being used in the search. To initiate the search, both administrators would need to plug the drives into the system at the same time, decrypt the drives, and upload the passwords for the servers doing the searching, setting off a search authorization flag. When the search flag is authorized, the system would automatically allocate the necessary search processors and orchestrate the process of logging each search server into its own processor.

The key advantage of the personal grid is that information about multiple people cannot be accessed in a single operation, even using system or search administrator credentials obtained fraudulently, Dr. Yasnoff says. Even if a hacker stole the computer storing the data, the time and effort it would take to decrypt one record at a time wouldn't be worth it, he adds. And while the personal grid doesn't prevent phishing or ransomware attacks, it does prevent large amounts of patient data from being compromised at once.

"Even if system administrator credentials are stolen in a phishing scam, it doesn't matter," says Dr. Yasnoff. "The system administrator has access to precisely no patient data."

Another benefit of the personal grid is that it can be implemented without changing the user interface of an EMR system; only the system back end would differ, Dr. Yasnoff explains.

The biggest drawback to the architecture, he acknowledges, is the cost for a hospital or other health care entity to program and implement a version of it. Therefore, he is in talks about potentially developing an open-source version of the software.

Ideally, he adds, a vendor will develop a commercial version of the personal grid for hospitals, health systems, and independent pathology labs within the next few years. —Charna Albert

New C-CDA tool for providers assesses quality of documents

The Office of the National Coordinator for Health Information Technology has released the One Click Scorecard, an online benchmarking tool to help health care providers determine the quality of their Consolidated Clinical Document Architecture. The tool will test Direct transport and C-CDA conformance for certified health information technology products.

To use the scorecard, a health care provider can email a C-CDA, via Direct exchange, to scorecard@direct.hhs.gov. One Click Scorecard will then test the C-CDA and send a score back to the provider's Direct account in the form of a letter grade-based "report card."

Health care providers and their business associates can disclose protected health information to the ONC while using the tool. The agency will immediately erase the entire C-CDA and any private health information once the C-CDA is tested and scored, HHS reported (www.bit.ly/onc_scorecard).

"Use the results of the One Click Scorecard to confirm your system is producing C-CDA artifacts that conform to specifications," suggested John Snyder, director of standards implementation and testing, U.S. Department of Health and Human Services, via a LinkedIn post. "Or, if your system is having problems importing a C-CDA received from others—use the Scorecard to see if the problem is document conformance to the HL7 Implementation Guide."

The ONC released the original C-CDA Scorecard last year to help developers ready their IT systems for deployment by pinpointing areas that need improvement.

Hc1.com platform joins claims and clinical information

Hc1.com has introduced its Hc1 ProviderView cloud-based system, which integrates claims and clinical data.
The system "delivers an integrated view of more than 3.8 million provider profiles complete with billions of data points, including live clinical data, health care claims, and prescription information from [the] Centers for Medicare and Medicaid Services," according to a press release from the company.

ProviderView instantly organizes comprehensive provider information, allowing health care professionals to see trends and focus their growth strategies accordingly.

Users can access data in ProviderView from any device. The product seamlessly connects to the Hc1 customer relationship management system.

HHS funds project focused on electronic exchange of Zika data

The Office of the National Coordinator for Health Information Technology and the Centers for Disease Control and Prevention have announced a plan to improve the reporting and sharing of information about suspected cases of Zika virus through electronic data exchange.

"While most systems have the ability to establish contact between commercial labs and providers, public health laboratories do not have the ability to exchange this information electronically," according to an HHS press release. "Almost all Zika tests are performed at public health laboratories and, because the information can't be transmitted electronically, the orders, test results, and additional information (such as pregnancy status) are either sent via paper form or telephone."

The ONC and CDC, which are also partnering with the Association of Public Health Laboratories on this initiative, have established the goal of creating an interface between public health laboratories and EHRs to more efficiently transmit Zika lab test results to hospitals. The hospitals, in turn, could provide the labs with tracking information on Zika cases and standard pregnancy status. The national system will use HL7 messaging or another Web-based tool to transmit pregnancy status for the lab orders, according to HHS.

The project coordinators have received commitments from the states of Texas and Florida, which have the highest number of U.S. Zika cases, to pilot test the lab information management system-agnostic solution. "This is generally a 'one-size-fits-all' solution," the ONC and CDC jointly reported. "Once it is built and deployed, it can be scaled as necessary, with the opportunity to customize for the exact needs of the jurisdiction."

The project, which will be implemented in three phases, includes the future goal of extending the technology initiative to other diseases, including HIV and hepatitis B, for which pregnancy status is important.
The Zika project is one of five 2017 entrepreneurial initiatives financed through the Secretary's Ventures Fund, which provides growth-stage funding and support to develop HHS employees' ideas that advance the agency's innovation agenda.

[hr]

Dr. Aller teaches informatics in the Department of Pathology, University of Southern California, Los Angeles. He can be reached at raller@usc.edu. Hal Weiner is president of Weiner Consulting Services LLC, Eugene, Ore. He can be reached at hal@weinerconsulting.com*..*