HEALTHCARE DATA BREACHES ON THE RISE: IMPLICATIONS AND SOLUTIONS

Anthem's 2015 data breach exposed the records of more than 80 million people, many of whom were not even Anthem customers. Anthem handled records for some independent insurance companies, and the private information of those customers was also released in the breach.

A hospital environment generally has more data security, but when insurance organizations, outpatient centers, physical therapists and home healthcare workers have access to Protected Health Information (PHI), there is less robust security in these collaborative environments outside the perimeter of the hospital. In the future, the degree of this collaboration between healthcare professionals and payers will only increase. Government and private healthcare organizations will try to reduce costs by using more preventative medicine and outpatient healthcare services to keep patients out of the hospital.

The fundamental problem with today's approach to healthcare data is that PHI is linked to real names, DOBs, addresses and Social Security numbers. The truth is that we can improve data security, but probably only incrementally, and as technology gets more complex there will always be ways to penetrate security and access data that can be sold—identity theft is a very lucrative business. With HIPAA requirements, small healthcare organizations are held to the same standards as large ones with much more financial resources. We need a new paradigm, and that paradigm is to make the data valueless.

Today the conventional paradigm to maintaining privacy is to create 100 percent accurate unencrypted data files and then spend enormous amounts of resources protecting this data. If the hackers get the data, then we lose and they win. Another approach that could be tried is to encrypt and decrypt data on-the-fly. If the data is hacked, it is of no value since it is encrypted. Unless the hacker has vast resources, they could probably not decrypt the data.

It is difficult to decrypt data. If it was easy, the FBI would not be asking Congress and pressuring Apple to create a backdoor for them so they can decrypt data from the cell phones of terrorists. However, encrypting/decrypting is expensive in terms of resources that would be required to retool hardware infrastructure and software applications. Also, it is much more difficult to build systems that can be shared securely with an encrypt/decrypt approach. It is easy to encrypt the data on a cell phone when only one person is accessing it, but it is a much more complex undertaking when hundreds of healthcare professionals have to access this data across geographies. Full encryption/decryption of the entire data file is not the best approach.

HIPAA and patient privacy have placed a big burden on healthcare professionals, and they spend a lot of time making sure that they are in compliance. I propose that a better solution is in a "valueless data" approach resting on the foundation of a "need to know" basis. Healthcare data should have just enough information for the healthcare worker to do their job—and not any more. The true identity of a patient and all their personal identifying information is not important for the vast majority of

interactions with patients and clinical medical professionals such as a nurses, doctors and technicians. Of course, people do enjoy being called by their real names, but for the purposes of good security there will always be tradeoffs.

The vast majority of PHI does not need to be mapped to a real identity with DOBs, addresses, phone numbers and Social Security numbers. When a new patient, Janet Smith, is admitted to a hospital, she can be renamed “Liz Jones” and her fake profile will be given an ID number that is sent offsite to a central safe repository where security resources can be applied. That ID number maps the PHI information in Liz Jones’s local fake hospital profile with the true identity of Janet Smith. Nothing related to Janet Smith’s real identity ever needs to be retained at the hospital. Along with the ID number, some unique biometric data will be taken such as a fingerprint or DNA sample that can be sent along with the ID number of Janet Smith to a central safe repository. If tomorrow Janet Smith goes to another hospital, a new alias, ID number and another sample of her unique biometric data would be sent to the central safe repository. No healthcare provider needs to know the real identity of Janet Smith in order to provide services to her.

At the central safe repository, there would a database that would have Janet’s ID numbers and her biometric data proving her identity with the information mapping to aliases such as Liz Jones. This database could be protected outside of the hospital or healthcare organization with an extraordinary amount of security resources under the control of the private sector. In essence, only the mapping information needs to be secure—not all the Liz Smith alias profiles. This central safe repository should not be a government organization, which will help to increase trust. There have been so many data breaches in government organizations, and the suspicion is that governments will misuse the data. Recently, China hacked 21 million U.S. government personnel records. The U.S. Government cannot even protect the personal records of its own employees.

This approach will initially require some infrastructure changes in hospital and healthcare organizations. It will centralize the security of just the key mapping information, and the data at all healthcare organizations will have just enough value for clinicians to do their work and spend less time thinking about HIPAA and security.

ABOUT GIVA

Founded in 1999, Giva was among the first to provide a suite of help desk and customer service/call center applications architected for the cloud.

Now, with hundreds of customer driven releases, the Giva Service Management™ Suite delivers an intuitive, easy-to-use design that can be deployed in just days and requires only one hour of training. Giva's robust, fast and painless reporting/analytics/KPIs quickly measure team productivity, responsiveness and customer satisfaction resulting in faster and higher quality decision-making. Customization and configuration are all point and click with no programming or consultants required to deliver a substantially lower total cost of ownership.

Giva is a private company headquartered in Santa Clara, California serving delighted customers worldwide.