



Identity Theft Check Up:

Electronic Medical Records are the New Credit Cards

Research by: David Bailey, Security Engineer at Redspin

As credit card fraud prevention measures have made it tougher on identity thieves, identity thieves have found a new target, healthcare identities. And healthcare information systems are nowhere near ready to withstand the onslaught. A recent survey by Chicago-based HIMSS (Healthcare Information and Management Systems Society) found that most hospitals spend less than 3% of their IT budget on security, a level Lisa Gallagher, Senior Director for Privacy and Security at HIMSS, calls inadequate.

According to the New York Times, a single credit card number was going for as much as \$100 on the black market in 2005. The black market has gone through turmoil similar to the stock market and the same number today sells for about \$6 dollars to as little as \$0.40 cents per number. The market has become flooded with numbers and banks are able to detect fraud more quickly because of online banking and increased awareness. The amount of attention focused on credit card fraud, coupled with the loss of profitability for thieves, has made it tough for criminals so their interest is shifting to healthcare identities.

Enter electronic medical records (EMR). EMRs are essentially an identity plus medical information. In 2007, an identity typically sold for \$14 to \$18 dollars. An EMR will usually contain a name, address, Social Security Number, date of birth, prescription information, medical history, and possibly a picture of a driver's license. A single hospital would retain this information for every person who has ever checked in and this is all the information an identity thief would need. Patients with recent birth or death events would be perfect candidates for identity theft as no one is usually monitoring their credit. Medical records that were previously boxed up in the basement are now ripe for the picking as hospitals make the move to digitize EMRs and are slow to adopt the processes and technology needed to protect this information.

Identity theft is only half the picture. A trend is emerging with thieves targeting patient records for the medical information contained within them. These data breaches started with simple hostage/ransom demands of large record holders. In October 2008, Express Scripts was notified by an attacker that records of millions of their customers would be released into the public if ransom was not paid. In a similar April 2009 incident, an attacker hijacked the Virginia Prescription Monitoring Program web site and posted a message demanding a \$10 million ransom from the state.

A shift has started where attackers are starting to sell the actual electronic medical and health insurance information. In October 2009, it was discovered that a company in India was selling British medical records. The seller told undercover investigators "I have 30,000 files to give you today, right now. I've around 140 diseases here. You just tell me which disease you're looking out for – I can give you anything". This data breach was blamed on the British hospital outsourcing its medical record transcription to a third-party business associate who in turn outsourced it to another company in India. These records were fetching £4 (\$6.24) each, but the World Privacy Forum claims these records can get upwards of \$50 dollars per record.

It is only a matter of time before these stolen records are regularly used for social engineering attacks against patients. Also, people desperate for medical care will begin looking to the black market to buy an insurance identity to file fraudulent claims. Several of these cases, dating back to 2005, are documented by the World Privacy Forum along with many other patient record thefts. They also note an increase in medical identity theft victims from 86,168 in 2001 to 255,565 in 2005, and this number is still increasing. Only time will tell what new crimes come with the theft of electronic medical records.

How Can an Information Security Program Help?

As with most technological challenges, there are no quick fixes or easy solutions, however, there are steps you can take to mitigate data breaches. Medical records and health insurance information need to be available to those who require access and secured from thieves trying to steal the data. One cannot just say “those records are encrypted” and think they’re set, the company must demonstrate a true commitment to a complete Information Security Program (ISP). Safeguarding EMRs requires management and implementation tasks that range across the entire business enterprise.

The following recommendations can help a healthcare organization get on the right track:

1. Demonstrate a true commitment to information security across the entire enterprise – not just within the IT arena. The most effective Information Security Program takes a risk-based approach, balancing potential risks against the convenience and expense to mitigate identified risks.
2. View IT Security as a Competitive Advantage as companies that experience IT security breaches are subject to damaging consequences such as:
 - Large monetary penalties from regulators
 - Loss of mission-critical IT systems including web applications, business associate networks and internal networks
 - Breach notifications to customers/patients and the media
 - Legal action by affected customers/business associates/vendors
 - Theft and/or misuse of data
3. Implement and follow well-documented security policies and procedures. Periodically review and adjust these and monitor and measure compliance to industry best practices.
4. Collaborate with business associates on the implementation of EMR security programs.
5. Conduct independent security assessments. HIPAA law requires covered entities to conduct routine evaluations of the effectiveness of EMR security programs, policies and procedures. It is also important to evaluate business associates with whom health data is exchanged.

As with any new regulated law, it is important to take a step back and fully understand how this impacts your organization. There are no “cookie-cutter” solutions however understanding the current infrastructure by taking a holistic, risk-based approach and balancing potential risks against the convenience and expense to mitigate identified risks are the recipe for success. Strong leadership, organizational competency, risk classification, collaboration and continuous process improvements are the benchmarks for best practices in healthcare information security and compliance.