RobbLAW

IT Security &
Compliance Consulting

Healthcare Security

Why is Information Security important in healthcare?

By: Robert Adams, Esq.
Date: January 16, 2017

Information Security is important, especially in a healthcare setting because healthcare organizations are a target for criminal attacks. A stolen credit card number is worth less than a dollar on the black-market because the amount of time it takes to go from a fraudulent transaction to the bank cancelling that card number has dropped to a matter of minutes, and that time continues to decrease as technology advances.

Even though the value of stolen credit card numbers is decreasing, the value of medical records continues to sky rocket because of the type of information it contains. To fully understand the importance, think about the information that someone could learn from your medical record and the reason attackers are willing to pay more for it begins to make sense. Besides the standard information like your name, address, social security number, and date of birth (which an attacker can get from a number of different sources), your medical record also contains sensitive information about you like any medications you are taking, your blood type, and diagnosis and treatment plans. That information could take you a lifetime to recover from because the attacker has everything needed to make a false identity with your information and then all your personal details to sustain it. Attackers are willing to pay anywhere from $50 to $500 per record for your medical information.

For anyone who thinks that they are too small or unimportant for an attacker to target, think again. Attackers do not care who they attack; all they care about is money. Taking the last $20 from your bank account does not matter if it means they get an extra $20 in their pocket tonight. Do not ever assume that you are safe simply because no one knows who you are and you think you are not important.

Children's medical records are worth even more than adult records. Attackers know that most adults do not bother to check their child's credit report. Most parents assume that since children

do not use credit, they do not need to check it. That assumption gives attackers up to fifteen years to build a fake identity off of your child's information and it is not until the child turns 18 that they realize they are $300,000 in unpaid debt. By that point, it is really too late, too hard, and too expensive for you to fight it.

This is why information security in healthcare matters. The information inside a medical record is extremely valuable and desired by attackers; they do not care who gets hurt in the process. By protecting everyone's medical record, you are making your information, and that of your children, friends, family, and loved ones safer. Attackers want it and we protect it. This is why information security is important.

As a side note because I always get asked this question about credit reports, every person is entitled to one free credit report each year and if you have never bothered to check your report, or your child's report, then now is the time by visiting www.annualcreditreport.com. When you check your child's report, it should return with a report that says "No records found." That is ideal, however, if it does find a record, at least you caught it and can start the process of reporting it. If you notice anything suspicious on your credit report, or your child's report, you will need to report it to your local law enforcement agency, the credit bureaus, and the credit-issuing bank. The law enforcement agency will take a police report, which you will need to purchase a copy of to file with the credit bureaus and the credit-issuing bank. Once you contact the bank, they should immediately cancel the suspicious account to avoid any additional charges from posting.