WARD AND SMITH, P.A.
ATTORNEYS AT LAW

It's 2016: Do You Know Where Your Medical Records Are?

Written By **Leigh A. Wilkinson** (law@wardandsmith.com)
March 11, 2016

Most of us assume that our medical records are under lock and key, safe and secure, somewhere in a vault. But assumption is not always reality, and with the rapid conversion of paper records to electronic, the location – and accessibility – of your records are not always what they should be.

The Problem

Earlier this year, a Los Angeles hospital's medical records system was hacked and the records held hostage. Initial reports were that the "kidnappers" demanded $3.7 million in ransom. After more than a week, the hospital ultimately paid $17,000 just to gain access to its own patients' medical records.

Massive leaks of medical information have also been reported by big-time insurers like Anthem and Blue Cross, parties that clearly should have the most up-to-date security measures in place. A study published in The Journal of the American Medical Association in 2015 found that over 29 million U.S. health records were compromised in data breaches between the years 2010 and 2013.

The U.S. Department of Health and Human Services Office for Civil Rights maintains a "Wall of Shame" listing of entities that have experienced a breach of medical information affecting more than 500 patients and it reads like a "Who's Who" of the medical and health insurance industries. It's frightening to see that many of these titans of industry appear on the list multiple times!

Who Would Want My Medical Records, Anyway?

Well, sorry to tell you this, but your medical records are currently the "hot ticket" on the black market. Cybercriminals want these records because the theft of medical records is much harder to detect and medical records are much harder to make unusable than traditional cybertheft targets like credit cards and bank accounts. Your medical records have a much longer shelf life on the black market than those traditional targets and can be used for many nefarious purposes, like insurance fraud, identity theft, terrorist immigration, and even blackmail. Today, the average medical record goes for 10-20 times the price of a credit card number on the black market.

Not only is there a financial loss aspect to the loss of your medical records, there is also a health threat to you. If someone steals or purchases your records from a cybercriminal and then uses your medical profile to obtain care, then their information will be added to your medical record, which could be life-threatening to you when you show up and your healthcare provider attempts to treat you using the thief's blood type, known allergies, medical history, etc.

So, What's a Patient To Do?

To lessen the possibility you will become a victim of medical record theft or to reduce the damage if theft does occur:

- Stay vigilant.

  Take time to read all the Explanation of Benefits ("EOBs") that your insurer sends to you or the Medicare Summary Notices you receive and make sure that you have seen the listed healthcare providers on the listed dates and obtained the listed services. If you have not, immediately alert your healthcare provider and the Federal Trade Commission.

- Get a credit report.

  These reports are free and they can reveal if there are unpaid bills for medical services or equipment you never received, which is a red flag that someone else is using your records.

- Review your medical records.

  The Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule provides that all patients have the right to review their records and obtain a copy of them (with a few exceptions for mental health records). You may even request that a nurse or medical records professional review them with you and answer any questions you have about them. There may be fees imposed by your healthcare provider for copies or interpretations of your records, but if you are concerned that your records have been compromised, it will be money well spent.

- Ask your healthcare providers about their HIPAA security measures.

  Do they encrypt emails that contain medical records? Do they allow employees to access records from home computers and mobile devices? Most healthcare providers must comply with HIPAA and will have a designated HIPAA Security Officer who can answer these types of questions for you.

Conclusion

Remember that even if your healthcare provider has put in place the absolute best protections for your medical records today, tomorrow will be a new day and the cybercriminals will continue their constant attacks using new and "improved" methods. The law is constantly trying to catch up with the rapidly changing technology, but gaps will always remain (for instance, Medicare still uses a beneficiary's Social Security Number as an identifier on its cards). Regarding your medical records, remember to be your own best advocate and remain vigilant: it could save not only your credit, but your life.

This post is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this post without obtaining the advice of an attorney. If you have questions concerning this post, please contact Leigh A. Wilkinson at law@wardandsmith.com.

--

article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.