MEDICAL IDENTITY THEFT

30 November 2018

Alsulaiti, Hamad. Rincon, Alejandra. Rios, David. Sator, Adnan

Business Info Syst. & Analytics, GBA-327-CA02 | Professor Reagan.

As The Office character Dwight Schrute once said, “Identity theft is not a joke, Jim! Millions of families suffer every year!” Identity theft is when someone, who is not our self, is using personal information to use financial information and to gain something without hurting their own identity. We all know a person that it has happened to, yet we often do not take the precautions necessary to stay safe online, in person, or over the phone. While identifying the theft of things such as your social security and credit cards information may be a nightmare to replace, medical identity theft is an utter chaotic nightmare to navigate. Medical identity theft is the theft of your insurance names, and card numbers. The purpose, to take advantage of your insurance benefits, payment records, and your treatment, of course, this has an effect not just on your insurance policies, but also your financials, and not to mention your sleep.

2014 saw an estimated 2.3 million cases of medical identity theft which was up 22% from 2013 (Andrews, 2016) The numbers continue to rise as a whole society increases its use of the internet and putting their information online. Now, no one goes out of their way to deliberately give their information but some common ways this may occur; using unsecured websites, ignoring explanation of benefits, medical records laying around in cars and at home, losing your insurance card. Simple tips for prevention of this include; shredding medical documents and card no longer needed, reading the explanation of benefits, as insurance to provide you with a list of all claims and bills and go through it. Another use of your identity can be to create a new identity that can be sold on black markets, or perhaps the worst, the thief mixing their medical expenses/history with yours.

Whereas with financial theft the bank will call if there is any suspicious activity, we often find that we do not pay as close attention to our insurance benefits, making it easier to hide crimes for longer periods. The most frightening thing is that a whopping 47% of reported cases occurred

between family members (Andrews, 2016). Sharing information not just online but in person with those you think you can trust is the way to go if you plan on ruining your identity, there are multiple tools out to help add an extra layer of security. Websites such as LifeLock a security company not just for physical assets but the intangible ones too, they provide a great overview into identity theft and articles that will help you navigate the situation. (LifeLock, 2018) Consumer Reports, an essential for any consumer (which just so happens to be everyone) also provides the same service as LifeLock but keeps up with current events more so than LifeLock. The Federal Trade Commission and the Office of Inspector General (part of the U.S. Department of Health and Human Services) both provide you with information of local agencies you can go to and get help (Federal Trade Commission, 2018).

Most importantly a printer, keep copies of every record that is worth keeping and keep track of appointments. While it seems mundane and redundant, it is essential to keep track of this just as you would with your finances (assuming you do that too.)

The Healthcare Information and Management Systems Society (HIMSS) is a not-for-profit organization established in 1961 (Healthcare Information and Management System Society, 2018) with the goal of improving healthcare regarding quality, safety, cost-effectiveness, and the best use of the technologies and communication management systems. HIMSS vision is “better health through information and technology,” and a pillar of this vision is security within that information, that is why HIMSS provides an array of tools from introductions, webinars, and risk assessments for individuals to take. While they do not put in place the standards and the laws, they do aim to inform and push new standards. HIPPA, the health insurance portability and accountability act set in place by President Clinton in 1996 is to this day the national standard for security.

Who follows HIPPA healthcare providers, health care clearinghouses, companies that help administers health insurance, accountants, lawyers, IT specialists, and companies that store and or destroy health records. As for who does not have to follow HIPPA, schools, law enforcement agencies, employers, life insurers, and municipal offices. What is protected under it, anything in your medical records, conversations between medical professionals, billing information? This information is protected by safeguards in place on anything placed on a server, limited access to information, and reasonable limit used of disclosure of information for intended purposes. Just like most personal things nobody should care for it more than you do, granted those that are held to HIPPA standards probably will care for it pretty well given their career is on the line. Yet, you are allowed to ask for copies of your medical records, billing statements, and even reports on when your information has been share stating with who, why, and when. If these are denied to you, you can file a complaint to hhs.gov. (Human and Health Services, 2018)

When Dwight said that millions of families suffer every year from identity theft, it was not an exaggeration. We find it difficult to navigate our medical policies as they are the last thing we need is someone else's mixed in or ours stolen. As anyone can tell from this topic, the core value of integrity is at play here along with responsible stewardship. Both highlighting the glaring issue of privacy and security when it comes to the sharing of information. While we live in a society that complains about our privacy not acknowledging that we must inherently give up some of these privacies for our protection as a whole. However, when it comes to our medical identities, there is a fine line of who to trust, and how much should be shared. We rely upon the laws in place to protect us, but it is entirely dependent upon those who we trust our doctors, our insurers to uphold the promises. Even with that said it is ultimately our responsibility to protect ourselves by preventing it as best as we can.

Works Cited

Andrews, M. (2016, 06 25). *The Rise of Medical Identity Theft.* Retrieved from Consumer Reports: https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/

Federal Trade Commission. (2018, 09 13). *Consumer Information*. Retrieved from Federal Trade Commission: https://www.consumer.ftc.gov/articles/0171-medical-identity-theft

Healthcare Information and Management System Society. (2018, 11 28). *Privacy and Security Standards*. Retrieved from Healthcare Information and Management System Society: https://www.himss.org/library/interoperability-standards/security-standards

Human and Health Services. (2018, 11 28). *Health Information Privacy*. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

LifeLock. (2018, 11 25). *ID Theft Protection*. Retrieved from LifeLock: https://www.lifelock.com/learn-identity-theft-resources-what-is-medical-identity-theft.html