Healthcare Identity Theft: Back to the Basics

Michael S. D'Angelo, CHPA, CPP

Incidents of cybercrime, including those which have demanded and received ransom from hospitals and healthcare systems, are becoming more prevalent, the author concedes, but most crimes of identity theft in healthcare are low tech stemming from the mass of hard copy information that still exists. This still commands the attention of Security as it has in the past, he says.

(Michael S. D'Angelo, CHPA, CPP, is the Principal and Lead Consultant for Secure Direction Consulting, LLC., a South Florida based security consulting firm. Previously, he was a corporate security leader with Baptist Health South Florida for seven years. He is a retired Captain from the South Miami, Florida Police department where he served for over 20 years. Michael is the author of the highly acclaimed book: *From Police to Security Professional: A Guide to a Successful Career Transition* (CRC Press), as well as a regular contributor to the Journal. He is an IAHSS member and serves on the ASIS International Healthcare Security Council.)

In 2017 you could not pick up a security industry magazine or read an association's newsletter without discovering an article about a breach of cyber security and the subsequent ID theft. Victims of these cyber crimes range from credit card companies, large box retailers and all too often, healthcare organizations. The more robust IT security systems grew, the more determined "hackers" became with penetrating theses elaborate systems. This crime, like most others, works on the age-old market principle of supply and demand. The demand or desire for "clean" ID's that can be used for financial gain is at an all time high. With the advent of the "dark web", there are no more dark alley transactions. Trading names with social security numbers is now conducted in the same fashion you legitimately trade stocks from your laptop.

FOCUSING ON HEALTHCARE IDENTITY THEFT

Identity theft has also garnered the attention of the general media, whose coverage of cases has risen dramatically over the past 10 years. The media regularly report on the latest scams used by identity thieves to steal personal information, the dangers of conducting routine transactions involving personal data, and the newest products and services designed to protect consumers from becoming victims of identity theft. Although much of this attention is directed toward educating consumers and marketing products, the media regularly present identity theft as an ever-increasing, ever-threatening problem. Recently, the media's focus has turned toward healthcare after several notable stories centered around cyber-attacks.

BEWARE OF LOW TECH THIEVES

As high tech as the market for clean identities has become, one the largest sources of the desired information is very low tech. Patient identities are stolen via hard-copy theft at hospitals throughout the country on a daily basis. While high tech thieves work behind the scenes, low tech thieves continue to work among us and capitalize on opportunity. Even with the progress of our transition to electronic medical records, there are still plenty of hard documents laying around with vulnerable patient information (PHI). "We have become so used to security software protecting our computers, that we completely forget about leaving folders sitting on a countertop of nurse station" says one nurse manager I spoke to. "You could literally walk on any floor and casually pick up documents with no one batting any eye." Many of these documents contain PHI and to become valuable on the "street" they simply need to have a name and a social security number. When you review the street value of identities, you can extrapolate how quickly the proceeds of a sophisticated hospital theft ring could add up.

Hacker service	Price
Social Security number	$30
Date of birth	$11
Health insurance credentials	$20
Visa or MasterCard credentials	$4
American Express credentials	$7
Discover credit credentials	$8
Credit card with magnetic stripe or chip data	$12
Bank account number (balance of $70,000 to $150,000)	$300 or less
Full identity kits	$1,200 to $1,300

Source: Dell SecureWorks

TRAINING PATIENTS AND HOSPITAL STAFF

Hospitals can employ a variety of measures to ensure patient information is protected throughout the facility. Teach patients about the need to be cautious with their ID as many cases of fraud could be prevented or at least discovered earlier if patients paid closer attention to their records in order to spot suspicious activity. In addition, many types of fraud occur because of patients' own negligence, for example, letting someone else use their insurance card. Hospitals can help by teaching patients what they should look for and how they can protect themselves.

Efforts must be made to train hospital teams, as well as newly hired staff on anti-theft tactics. Many privacy breaches are blamed on hospital staff, either because of intentional theft or negligence that leaves information vulnerable. That's why it's important to properly vet all new hires who will have access to patient information, and to train them on their responsibilities for keeping that data secure from day one of their employment.

RECOGNIZING RED FLAGS

Hospital staff should learn to recognize the immediate signs during patient interactions and when processing paperwork. Everyone should be well versed in identifying red flags that could signal fraud. That includes infor-

mation collected when a patient visits that doesn't match what's on file, tests being ordered that are inconsistent with the patient's history, etc. Do not restrict these precautions to clinical staff as the data continues to show breeches by staff in all departments.

Some organizations have instituted annual Privacy training which refreshes staff on basic safeguards; including, computer and paper based methods of protecting PHI. These in-service programs should comprise a joint team of staff from Privacy, Security, Risk and Human Resources. This should be done with the goal of fostering a hospital-wide responsibility to protect PHI and prevent identity theft.

Multi-cut shredders should still be deployed throughout the hospital wherever there is an abundance of paperwork. As elementary as it may seem, documents containing PHI are often found disposed of in regular waste receptacles, leaving them vulnerable to discovery by anyone in close proximity.

BACK TO BASICS FOR SECURITY

As high tech as healthcare security has become, it is the old-fashioned privacy and confidentiality protocols of patient records that will continue to protect against this type of fraud. Since hospital Security teams have been tasked with addressing this issue long before the advent of cybercrime, they should continue to take the lead on educating their colleagues. Piggybacking on our adage of "security is everyone's responsibility", Security must lead the way with spreading the word of back to the basics.