Cyber Crimes Against Healthcare

Cyber crimes against health care organizations are growing exponentially more complex and frequent, especially with the increased reliance on electronic systems to coordinate care. These attacks have increased by 125% since 2010 and are now considered the leading cause of data breaches according to the Ponemon Institute. This surge in cyber attack has put pressure on hospitals to find new strategies in cybersecurity. An emerging insider threat company based out of Sarasota, Florida called CopyStrong, has created an application that mitigates these threats.

The last thing you want to deal with after being hospitalized for an illness is to then be victimized for years thereafter because of an insider theft scheme. This often happens due to inadequate or non-existent security measures surrounding the storage and use of your medical records.

When you have a hospital stay, hundreds of people, have access to your patient medical records, which can easily sell for anywhere from $300-$500 each, on the black market. What prevents these individuals from walking out the front door with your medical records ethics, morals, employee training manuals? These solutions are inadequate. Why are an individual's medical records so valuable? It is because these records contain personal data that can be used for further cybercrime. Unlike credit cards which can be swiftly cancelled, medical records have a long lifetime and hence greater possibility of re-use.

In a recent article from Forbes titled “Your EHR (Electronic Healthcare Records) could be worth $1,000 dollars to hackers” the author explains that the majority of all inappropriate accesses to EHR comes from the inside. They involved nurses, doctors, specialists, and administrators all of whom have legitimate access to a patient's EHR, but who have abused that access. In 2016, 450 breaches occurred, affecting 27 million patent records, and over 65% came from insider attacks.

An emergency room employee at Florida Hospital used his access to collect information on patients injured in car accidents, which he then sold to chiropractors and lawyers. This went undetected from 2009 to 2011. After he was terminated, his wife - who was also an employee at the hospital - continued the scheme. In many instances, like this, breaches go undetected for several years.

Without consequences, early detection, and a cost effective legal solution in place, health care systems and patients will continue to be victimized. “Current detection usually takes years and the costs to the organization are exorbitant. Up until now, there really hasn’t been a reliable solution to stop these bad actors and hold them accountable” said Erica Bowles, founder of CopyStrong a cybersecurity company focusing on insider threat within healthcare, finance and defense organizations. CopyStrong provides early detection from bad actors while simultaneously launching a counter intelligence protocol that minimizes victimization of patients while protecting the reputation of health care systems.

ABOUT COPYSTRONG

CopyStrong is a leading edge cybersecurity company, headquartered in Sarasota, Florida. CopyStrong is powered by a series of proprietary algorithms providing early detection and actionable insight to administrators.