CYBER DEFENSE MAGAZINE

eMAGAZINE

JUNE 2024

In This Edition

Special Cybersecurity Considerations for Medical and Legal Practices

Understanding the Dark Web: What You Need to Know

How and When to Know You Need a Fractional CISO

...and much more...

MORE INSIDE!

`

CONTENTS

Special Cybersecurity Considerations for Medical and Legal Practices

"Protect The Most Vulnerable at Their Most Vulnerable Times"

By Jim Ford, Founder and CEO, PatientLock® and JurisLock™

In the spring of 2018, my (then) pregnant wife and I went in for a 28-week sonogram of our twins. Like most soon-to-be parents, we expected it to be a fun, exciting visit, and another opportunity to see our babies in the womb. Little did we know it would turn out to be one of the scariest days of our lives.

Shortly into the exam, the sonographer looked troubled and quickly called a physician into the room, where it was discovered that our daughter was in distress. Our daughter was no longer able to effectively push blood back out through the placenta, causing her heart rate to continually decelerate. As a result, the medical staff informed us that both of our kids needed to be delivered immediately and that only a few hospitals in the area had NICU's (neonatal intensive care units) capable of supporting them.

Spoiler alert: While both kids came into the world weighing less than two pounds a piece, following a three-month stint in the NICU at Overland Park Regional Medical Center (HCA), (and six years later), we have happy, rambunctious, and perfectly healthy kindergartners.

The relevance to this (cybersecurity) story stems from the fact that we chose, in large part, to forego using a well-known pediatric hospital in our city because of breach events that had occurred beginning in 2016 and continuing through January 2018, resulting in the theft of approximately 70,000 patient records.

Between our two kids, the NICU bills (covered by insurance) were nearly $3-million dollars. Patient identity and safety concerns aside, the decision we made as parents and consumers had a detrimental monetary impact to the pediatric hospital in the form of a significant, lost revenue opportunity. Amongst others, that event, or I should say decision, poured gasoline on the vision I had in founding PatientLock, and a few years later, JurisLock. That vision (turned Mission) was to make "enterprise grade" cybersecurity available and affordable to any size of business using channels servicing the Defense community.

Those in the healthcare and legal professions, specifically, are tasked with protecting and serving patients and clients in some of their most vulnerable times. Their goal as professionals is to provide help during some of the most stressful, life-threatening, or otherwise impactful times an individual may ever go through. On the medical side, this could be delivering premature babies, assisting a patient through a cancer diagnosis and treatment, or making the end-of-life process as comfortable and painless as possible. On the legal side, this might be working with a client who has suffered a catastrophic injury. It might be a divorce, a child custody case, working through criminal/civil litigation matters involving freedom or one's life savings, or helping a business make a strategic acquisition.

I would not imagine that during these interactions, cybersecurity is priority one (or two, or ten, or twenty). However, because these professionals often meet and work with extremely sensitive information during their work, this information must be properly safeguarded. Otherwise, there can be significant, negative results. Cyber criminals could gain access to a provider's network, compromising a surgery already in process. Information in a patient's electronic medical record could be deleted, or changed (think allergies, dosing information, or other significant information like a patient's blood type), or a physician office or hospital could be locked out of its computers such that patient care is disrupted (also leading to significant revenue loss). Worse yet, a double extortion tactic including data exfiltration and ransomware might be used simultaneously. This occurs when a bad actor steals records to then sell on the Dark Web, while also executing a ransomware attack and demanding payment.

Due to these factors, those practicing law and medicine have special and unique obligations to protect the information of those they serve. Just to name a few:

- Doctor-patient privilege/attorney-client privilege
- Ethical obligations/ABA Rule 1.6
- HIPAA
- Special laws protecting substance abuse information
- State law requirements

The practice of law and medicine have in common several important features, in particular the doctor-patient privilege and the attorney-client privilege. The goal of both of these is to ensure that proper care can be provided, without fear of repercussion (whether disclosure publicly or introduced as evidence in a lawsuit). If a patient or client cannot provide full details, their practitioners can't provide proper service. Often these details could be embarrassing, could lead an individual to believe the information could be used against them in a different context, or an individual may not understand that what they see as a trivial bit of information could be extremely important for their medical or legal professional.

This is where the tie-in to cybersecurity comes into play. Cyber criminals know that those in the medical and legal professions house some of the most sensitive data, and that such information, if made public, would have negative ramifications. Cyber criminals also know that, if hit with ransomware, these professionals are likely to pay the ransom to ensure this information is not made public and/or that these professionals can continue to provide uninterrupted service to a vulnerable audience.

PatientLock and JurisLock were developed specifically with the most vulnerable in mind. PatientLock and JurisLock have bundled services specifically designed to harden a healthcare organization or law firm's cybersecurity posture through a fully managed suite of cybersecurity technology and compliance/advisory services, designed to force-multiply IT resources and satisfy regulatory frameworks and rules like HIPAA, PCI, NIST, ABA Formal Opinions, as well as cyber insurance requirements.

PatientLock's and JurisLock's Security Operations Centers (SOCs) are the same that provide service to the DOD and the largest military-defense-contractors in the world, allowing clients to take advantage of previously unattainable economies-of-scale. With 400+ cybersecurity professionals, PatientLock and JurisLock eliminate the need to hire security staff and solve the talent issue by managing the security technologies (MDR, XDR, MEDR, VUMA, EPS, etc.), monitoring for threats 24/7/365, and taking action in real-time to address them.

In our experience, it's become clear that it's often the case that C-Suite executives just don't know what they don't know (NOT a typo). Among other duties, a CISO's responsibilities include educating decision-makers on cyber risks and risk management. Most small and medium-sized organizations don't need or can't afford to hire a full-time CISO. PatientLock's and JurisLock's virtual vCISO program provides a fractional CISO to exercise oversight of enterprise-wide cybersecurity and governance, while helping achieve compliance for regulatory frameworks including NIST CSF and HIPAA Compliance, Security Risk Assessments, HITRUST and SOC2 Readiness, GAP Assessments, and more.

We recognize that technology alone isn't enough. Cyber insurance can also protect organizations against many different risks associated with cyber incidents, especially since cyber incidents are often not adequately covered, or covered at all, by D&O or E&O policies. Cyber insurance is designed to help an organization mitigate exposure through risk transfer by offsetting costs associated with responding to an incident like data and system recovery, business interruption, extortion expenses and claims and lawsuits asserted by others directly affected by the incident. We see cyber insurance as a risk management device similar to commercial property coverage for a fire in a restaurant's kitchen. Even though restaurants have sprinkler systems, extinguishers, fire alarms, etc., a restaurant would never forego having property insurance because it mitigates the damage that the inevitable kitchen fire will cause.

In practice, PatientLock and JurisLock have found that “stapling” our documentation to a cyber liability insurance application provides underwriters and carriers the opportunity to increase the limits of risk transfer offered, lower annual premiums, reduce retentions, and offer broader coverage options for PatientLock and JurisLock customers.

We started with a simple goal: to protect the most vulnerable at their most vulnerable times. It started with the trip to the NICU several years ago, and the needs and risks have only continued to grow. Cyber criminals are making things as complicated as possible, and the potential impact of a breach is now more devastating than ever. However, we will continue to work with those in the medical and legal professions to protect those that they serve. There are steps that those in these fields can take to limit this risk, and we are here to help them on that journey.

About the Author

Jim Ford, Founder and Chief Executive Officer of PatientLock and JurisLock. Prior to founding PatientLock, Jim spent nearly two decades working in healthcare, or healthcare information technology, beginning his career in the laboratory of an HCA hospital in 1998. Prior companies include Cerner, athenahealth, Aprima/eMD’s, and Fortified Health Security, a healthcare focused managed security services provider, or MSSP.

Jim founded PatientLock in 2019 with the vision of making enterprise-level cybersecurity technologies and services available and affordable to any size of healthcare organization. PatientLock is now deployed on network assets used by thousands of US-based healthcare organizations.

Following the successful launch of PatientLock, Jim was approached by legal professionals looking to address the cybersecurity and compliance issues faced by law firms. JurisLock was then launched for law firms where the handling and storage of personally identifiable information (PII) and electronically protected health information (ePHI) create the same compliance requirements and cybersecurity challenges faced by healthcare organizations.

Jim earned certification as a HITRUST Practitioner, (CCSFP) was certified by the Supremus Group as a HIPAA Privacy and Security Expert - Level-4 (CHPSE) and holds a master’s degree in business administration (MBA).

Jim can be reached online at jford@patientlock.net and at the PatientLock or JurisLock company websites: https://patientlock.net/ or https://jurislock.com/