HIT•IQ Health IT Investor Quarterly

Illustrated intelligence for investors, bankers and entrepreneurs

WINTER 2019

Inside this issue

This newsletter brought to you by:

Howard Burde Health Law

MOUNTAIN SUMMIT ADVISORS

HIMSS Analytics

First Analysis Securities Corporation

HEADING INTO HIMSS AND JUST WHEN YOU THOUGHT IT WAS SAFE...

By Howard Burde

The close of 2018 saw appropriate attention devoted to the growing problem of cybersecurity.

Since then, the problem having been exposed and vetted, it has been relegated to the province of security officers and CIOs. After all, they are paid to deal with the inevitable headaches.

From an investor or entrepreneur perspective, such dismissiveness would be foolish. It would be foolish to develop or fund a solution that lacks security infrastructure. Security cannot be an afterthought. It needs to be the product of forethought. More important, the purchasers of innovative solutions will be demanding rigorous security. Security has achieved the prominence that privacy reached years ago: it is a market imperative.

Fortunately, the Department of Health and Human Services provided a belated holiday gift on December 28, 2018: a four-volume publication entitled *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* ("HICP").

The HICP guidance (it is non-regulatory guidance, not law) is intended to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the most pertinent cybersecurity threats. HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores current threats and presents practices to mitigate those threats.

The five threats explored in HICP are: E-mail phishing attacks; Ransomware attacks; Loss or theft of equipment or data; Insider, accidental or intentional data loss; and Attacks against connected medical devices that may affect patient safety. In short, HICP explores the common threats that can undermine a health care organization and any of the solutions.

The Technical Volumes detail ten practices to mitigate these threats: E-mail protection systems; Endpoint protection systems; Access management; Data protection and loss prevention; Asset management; Network management; Vulnerability management; Incident response; Medical device security; and Cybersecurity policies. Technical Volume 1 focusses on small healthcare organizations; Technical Volume 2 on medium and large health care organizations.

Entrepreneurs should review the technical volumes for advice: They are speaking to your customer base. Investors should use these volumes to test the cybersecurity readiness of portfolio and prospective investments.

Join me at HIMSS'19. I will be in the Investor Room, 240 A/B on Tuesday February 12, and at Venture Connect Wednesday, February 13. Let's schedule at time to get together. 215-292-1246.

Howard Burde, Principal
Howard Burde Health Law
howard@burdelaw.com

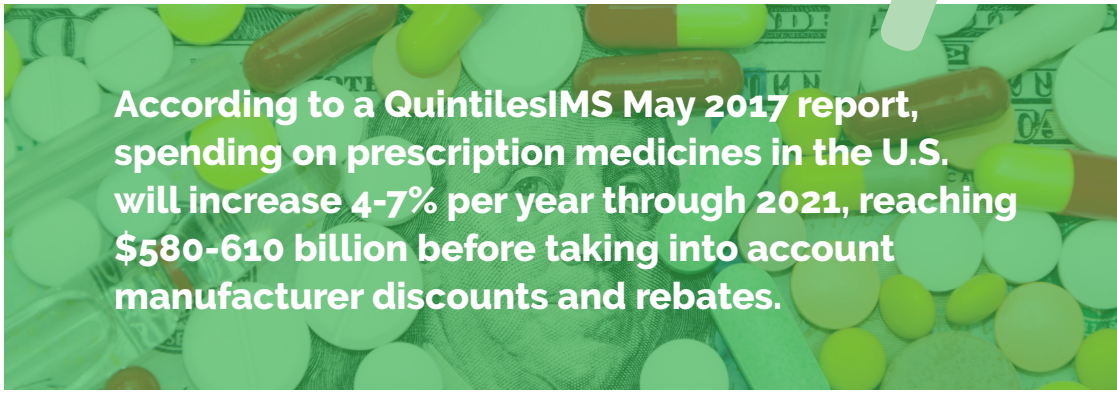
Links To Recources

- **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)**
- **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations**
- **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations**
- **Resources and Templates**

LOOKING FOR SOLUTIONS THAT ADDRESS FUNDAMENTAL MEDICATION PRICING PROBLEMS

By Brian Friedman

Recently, the U.S. Senate Committee on Health, Education Labor & Pensions (HELP) held hearings on stabilizing the health insurance markets. During the hearings, a broader theme emerged: Lawmakers should be focused on the larger and fundamental problems of the healthcare delivery system that are driving unsustainable cost increases, specifically ***1) high and increasing prescription drug costs, 2) payment reform to align incentives between payers and providers, and 3) price transparency.***



According to the Centers for Disease Control and Prevention, in any given month, 48% of Americans take a prescription medication and 11% take five or more prescription medications. This latter group, typically the elderly and chronically ill, is at significant risk of an adverse drug event (ADE) and account for a disproportionate share of overall healthcare spending. A study by the U.S. Department of Health and Human Services (HHS) notes ADEs cause approximately 125,000 hospitalizations, one million emergency room visits, two million affected hospital stays, and 3.5 million physician office visits every year.

The U.S. spends substantially more per capita on prescription drugs than any other country at $1,112 in 2015. According to a QuintilesIMS May 2017 report, spending on prescription medicines in the U.S. will increase 4-7% per year through 2021, reaching $580-610 billion before taking into account manufacturer discounts and rebates. According to CMS, 39% of people over the age of 65 take five or more prescription medications per day and a total of eight or more medications per day when factoring in non-prescription drugs.

A recent analysis of more the 30,000 user sessions showed 90% of those enrolled in Medicare Prescription Drug Coverage could be overpaying. According to the 2017 Medicare Choice and Impact report from eHealth, only 10% of enrollees were in a plan that covered their prescription drugs at the lowest possible price. Many Medicare prescription drug plans change the pricing, benefit tiers, and formularies of their drug plans from year to year, impacting drugs covered, monthly premiums, and out-of-pocket cost.

We see solutions that foster: 1) transparency, 2) adherence, and 3) risk management as areas of tremendous growth over the next several years. As entrepreneurs consider the directions to take their ideas, they should consider the same approach that the U.S. Senate HELP Committee did: address the big, intractable issues. Investors will always be interested in solutions that tackle the toughest problems.

Brian Friedman, Managing Director,
First Analysis Securities Corp
bfriedman@firstanalysis.com

HIMSS ANALYTICS CHARTS THE FUTURE OF HEALTHCARE WITH FOCUS ON ACCELERATING IMPACT OF MATURITY MODELS

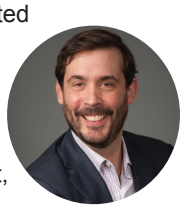
By Blain Newton

For over a decade, HIMSS Analytics has guided healthcare organizations around the globe in technology adoption and implementation through Maturity Models that provide benchmarks and standards to help organizations get the most out of their technology investments. As we move into 2019, HIMSS Analytics is making the strategic shift to further invest in all of our Maturity Models, with a focus on building a framework for digital health transformation to drive clinical and financial improvements, globally.

The full Maturity Model suite includes the EMR Adoption Model (EMRAM), Outpatient EMR Adoption Model (O-EMRAM), Adoption Model for Analytics Maturity (AMAM), Continuity of Care Maturity Model (CCMM), Digital Imaging Adoption Model (DIAM), Infrastructure Adoption Model (INFRAM), and Healthcare Supply Information Maturity Model (H-SIMM). Each model has a specific focus on a different discipline related to technology and process. This framework will guide organizations looking to make improvements that will impact both patient care and their efforts to achieve organizational goals. The models shape a more holistic approach to technology usage and processes in healthcare with future opportunity for global comparability in clinical and financial health of healthcare organizations.

Additionally, our Certified Consultant Program is being strengthened to support healthcare organizations on their journey to Stage 7, the highest level of achievement on each model. Certified Consultants have been professionally trained on all of the HIMSS Analytics Maturity Models. These consultants are able to effectively educate, provide onsite assessment services and ultimately help build strategic roadmaps that guide organizations toward improved care and a healthier bottom line.

This new focus comes on the heels of a major shift in our business. Earlier this year, Definitive Healthcare acquired the data services business and assets of HIMSS Analytics, which includes the Logic, Predict, Analyze, Source and custom research products. With this change, we see immense opportunity in making Maturity Models accessible and usable for healthcare organizations globally, and we are excited to positively shape the future of healthcare.



Blain Newton,
Executive Vice President,
HIMSS Analytics
blain.newton@himssanalytics.org

MEDICAL MARIJUANA IN UTAH – REALLY?

By Scott Holbrook and Terry Pitts

According to the Webster's dictionary marijuana was first used in 1874. It was probably used long before, but nothing is officially recorded. The legalization of this drug has now been widely accepted in the United States. According to the National Institute on Drug Abuse In 2015, more than 11 million young adults ages 18 to 25 used marijuana in the past year. Even Utah has now accepted the use of this element to help relieve pain especially for those that suffer chronically. In the last Utah general election, the state referendum was narrowly passed. Following voter approval, the state legislature developed a bill that was passed and signed by the Governor. I am sure some may say "Utah, are you kidding me"? Have pigs started flying yet? Yes, Utah. Utah, predominately (62%) belong to The Church of Jesus Christ of Latter-Day Saints as a religion, has now agreed that in certain medical cases the relief that marijuana provides is medicinally viable through the legal prescription provided by a physician. So why are we writing about this seemingly unique occurrence? What does this have to do with Information Technology? A lot!

Those that passed this legislation are concerned about controlling this substance. How do you do that? There is now new technology available that can control the substance from the growers harvesting to the end user. This is what the Utah law is very interested in doing. The technology is a prescription pack that communicates to cell towers throughout the state. This technology knows where the prescription pack is geographically. In addition, the prescription pack sends a communication message to the clinical data base when any of the "buds" or marijuana substance is pressed out of the pack for the end user to consume. This technology tracks all of the marijuana from source to end user. This clinical and technology data is retained for reporting and trend analysis.

A pilot program is in the works to prove the concept and technology. Over the next six months the pilot will prove the technology and the controlling discipline of the drug. Leave it to Utah to innovate such an opportunity. If this can be proven, then the opportunity to propagate this technology across the country is formidable. Control is essential when considering the use of this substance to alleviate pain and suffering of those that have no other recourse. The use of a controlled substance like marijuana will definitely require technology to monitor and control, we will see many such solutions arise in the near future (some from unlikely places).
We look forward to these results.

Scott Holbrook, Principal,
Mountain Summit Advisors
sholbrook@mtnsummitadv.com

Terry Pitts, Principal,
Mountain Summit Advisors
tpitts@mtnsummitadv.com

HIT·IQ | THE LAST WORD

Featuring profiles of entrepreneurs and leading innovators

Ben Demonte, Managing Director, North American Leader, Cyber Risk
Kroll, A Division of Duff & Phelps

Ben, thank you for taking the time to share your thoughts with the HITIQ readership. This issue of HITIQ is the 2nd in a series focusing on cybersecurity considerations for HIT-related startups and the investors and bankers that fund and grow those enterprises. We wanted to speak with you to get your thoughts on a range of topics from changes in cyber forensics to some cyber best practices for small companies.

Q: Ben, you have an impressive background that includes time at the FBI in cyber investigations, incident response, computer forensics and more. We've heard a lot about computer and cyber forensics because of the ever-growing challenges to protecting organizations from cyber threats. You have been in this business for over 25 years. What are some of the most significant changes you've seen in forensics during your long career?

Early in Computer Forensics most tasks were categorized as dead-box or post-mortem forensics. It used to be that you would find a machine interesting based on suspicious activity you found after examining logs. You would make a physical image of that machine and then bring back to a lab to analyze.

That has drastically changed. Now we use methodologies in which practitioners can remotely deploy endpoint sensors or monitoring tools within a network, allowing real-time monitoring, collection of forensic artifacts, and analysis as events are happening – and ideally, before they happen. Often, we see malware being executed and its impact on the network in real-time.

Another significant change is the number of ways that sensitive or confidential data can be accidentally – or purposefully – exposed, and how the threat has become far greater than most organizations appreciate. Once a hacker has made it beyond the endpoints, and starts to collect data from servers, the data is essentially out of control and is dispersed quickly into the deep dark web, usually going for sale to the highest bidder many times over.

Because of these new trends, it is far more efficient to analyze suspicious activity in real time rather than conducting static analysis or reverse engineering of a piece of malware.

Q: We often see guidance for large organizations with regard for best practices for cyber protection, but what guidance would you give to smaller organizations? Many of our readers represent startups of fewer than 20 or even ten people, what are some practical considerations for them?

Some best practices should be happening regardless of the size of the organization, starting with some fundamentals: Does the entity have an incident response plan, and do they exercise it on a regular basis? Are they conducting periodic penetration testing and vulnerability scans?

One that is often overlooked relates to social engineering attacks, and whether organizations are exercises within the company? As we see social engineering attacks become more frequent, organizations of any size must train employees to understand what these look like and how quickly the attack methods are evolving.

Additionally, organizations of all sizes should ensure any remote access points, such as email, HR applications, a VPN, and many more have some multi-factor authentication built-in. Sometimes it's difficult because companies have many different vendors supporting I.T. It may generate some legal and operational costs, but they need to review those contracts and see who has sensitive data, find out if they have they been audited, and conduct appropriate due diligence on them. Don't forget about their cloud provider and any other I.T. these vendors may be outsourcing, because if those vendors ultimately have a breach, the entity itself will still need to mitigate because it's their data that's been exposed.

Investors should also build into the contract a reserve to audit sensitive data at certain intervals, maybe as often as quarterly, with vendors handling high-value data. They might not be able to do an entire assessment every quarter, but they should plan to do a more comprehensive review at least once per year. However, if one of their IT providers does something more significant, for example, maybe the vendors have switched cloud providers, the contract should include the requirement that they must alert you, ideally before they would make such a change.

Q: How about some best practices for staffing for smaller startups?

When you have a startup with under ten people, maybe as few as three or four, you can have real challenges trying to find, compensate and retain skilled cyber professionals. Companies of any size can benefit from this, but especially for these smaller startups, they should consider engaging a company like Kroll or similar for certain services that may not be full time, services like a virtual CISO, penetration testing, vulnerability scanning, vendor management, other advisory services including endpoint monitoring.

Q: What about frameworks and resources? If an organization is just getting started or an investor is new to this space, what are a few you would recommend?

There is a good framework from the Internet from the Center for Internet Security (CIS). Take a look at their CIS 20 Critical Controls which are broken in three categories and give better insights into how to meet the controls, assess maturity levels, and more. Another useful framework – the NIST Cybersecurity Framework - is available from the National Institutes for Standards and Technology (NIST) and is also very strong, but more extensive and potentially harder for smaller companies to address. https://www.cisecurity.org/controls/, https://www.nist.gov/cyberframework

Q: For our last question, what should our readers know about Kroll?

Kroll is a global company, with cyber risk and compliance resources in North America, EMEA, APAC, and Latin America. Kroll has recently announced new strategic partnerships and services which gave us new capabilities and greater flexibility to support companies of all sizes.

Lisa Spellman, General-Secretary,
DICOM International
lspellman@medicalimaging.org