HIT•IQ Health IT Investor Quarterly

Illustrated intelligence for investors, bankers and entrepreneurs

WINTER 2018

A CLOSER LOOK AT TEXT MESSAGING IN HEALTHCARE?

By Brian Friedman

Secure text messaging is a critical component of better care coordination, enabling faster communication and collaboration among providers across the care continuum—from patient admission to transfer to discharge.

The major risk/concern with text messaging is lack of encryption which compromises security and creates HIPAA exposure.

Sizing the market on a standalone basis is difficult as secure text messaging is often sold as part of a broader solution from a large range of vendors, including publicly traded Imprivata and athenahealth, as well as from a number of private companies such as TigerText.

INDUSTRY DYNAMICS

According to a number of industry sources, nearly 90% of health-care workers use personal devices, namely smartphones, to complete daily tasks inside and outside of the hospital or office.

As a result, secure texting is a critical issue to be addressed, and there are a number of vendors coming at this problem from different angles. Examples of texting include alerting physicians their patient has been admitted to the hospital; texting the radiology department that a patient needs an x-ray; or sharing an image, EKG, or lab result with another physician for a second opinion. In many cases, text messaging is replacing archaic communication devices such as pagers.

A number of companies, such as Imprivata, support the growing bring your own device (BYOD) initiatives in healthcare. According to a report from Imprivata and the Ponemon Institute, inefficient communications during critical clinical workflows cost the average U.S. hospital $1.75 million annually, and the use of secure text messaging could reduce more than half of this wasted time and loss. According to research published by the Robert Wood Johnson Foundation, nurses waste an average of one hour each day tracking down physicians. The Joint Commission found that 66% of sentinel events — any unanticipated event in a healthcare setting resulting in death or serious physical or psychological injury not related to the natural course of the patient's illness — are linked to communications breakdowns.

As highlighted in the table below, inefficient communications can delay patient admission, emergency response, and patient transfer. Text messaging helps improve provider workflow and productivity involving consults, referrals, and order verification. It can also improve patient care by allowing physicians to devote more minutes of their day to patients. San Joaquin General Hospital, a TigerText client, cited secure text messaging as a driver behind higher HCAHPS scores in areas such as medication delivery, patient hand-offs, and patient discharge times.

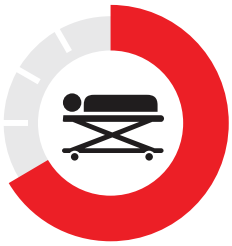
Inside this issue

Time Wasted during Critical Workflows (Imprivata estimates)

Inefficient communications waste time, especially during three critical workflows

33 minutes wasted during patient admission

40 minutes wasted coordinating an emergency response team



35 minutes wasted during patient admission

Source: First Analysis, Imprivata.

RISKS

The major issue with short message service (SMS) text is that SMS is not encrypted and lacks the ability to validate whether the recipient of the text is the intended recipient, a key requirement for HIPAA audit trails. As the provider side of healthcare transitions from paper to digital, protecting PHI is more challenging.

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

Brian Friedman is a managing director at First Analysis leading the firms HCIT investment banking efforts. Brian has completed numerous M&A transactions and public offerings for companies such as CoverMyMeds, Apixio, FairWarning, Healthstream and many others. Prior to joining First Analysis in 2010, he was an executive vice president and co-head of investment banking at National Securities where he managed more than 40 capital markets and M&A transactions. In 2000, Brian was the founding managing partner of Robotics Ventures, investing in ground breaking companies such as iRobot and Mako Surgical. Brian started his career as an associate at Guggenheim Partner. He holds a bachelor's degree in finance from the University of Iowa and a J.D./MBA from IIT Chicago Kent College of Law.

THE RATS KEEP WINNING THE RAT RACE

By Howard Burde

IT security is, by definition, defensive. Hackers will always be ahead of security because security defends against known or anticipated threats. It makes no sense otherwise.

In the past 24 months 194 cases of hacking/IT incidents resulting in reportable breaches of protected health information (500 or more individuals affected) have been reported to the Department of Health and Human Services Office of Civil Rights portal. Among the 194 are the notorious SamSam and Ryuk ransomware attacks which impacted over 6 million records.

Health care records contain critical information for the covered entities and attractive to hackers. Ransomware is effectively a racketeering scheme. The hackers are selling protection from a single attack and there is no guarantee that paying the ransom will protect against a subsequent attack.

How can healthcare organizations, developers and entrepreneurs protect against intrusions? And, what should investors demand from their companies?

1. Eliminate vulnerable devices. While fax machines were last useful when the mullet was still an acceptable hairstyle, many healthcare organizations, especially physician's offices, still use them for the transmission of PHI. A recent study revealed that hackers only need a fax number to launch a malicious attack. Fortunately, CMS Administrator Seema Verma recently announced her intention to eliminate the use of fax machines by 2020. Note that intrusion through an unsecured fax number may allow access to an entire network. As BYOD policies gain popularity and remote access is a business imperative, these conveniences also increase vulnerability. Secure organizations limit BYOD access, use multifactor

authentication, and prohibit storage of usernames and passwords.

2. Follow FDA Guidance. The Food and Drug Administration has issued substantial guidance for medical device developers in several publications since 2014. The FDA guidance includes both premarket requirements and post market monitoring of threats. While the FDA has been judicious in its exercise of authority with respect to medical software, its guidance is worthy of consideration for developers and entrepreneurs whether or not FDA approval is sought.

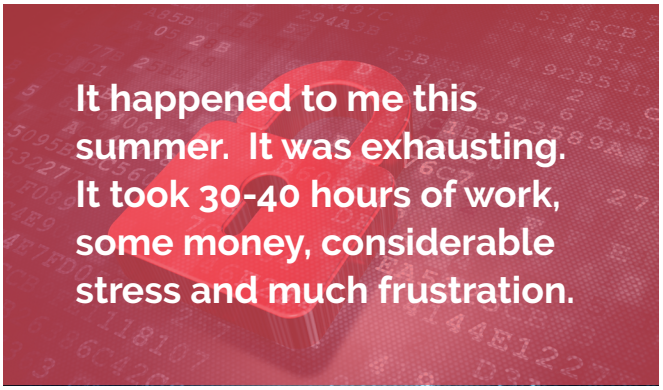
3. Comply with HIPAA Security Regulations. The HIPAA Security Rule requires covered entities and business associates to apply administrative, physical and technical safeguards. Among the requirements most easily met (and frequently delayed) is a periodic risk assessment. HHS even provides a risk assessment tool, so failure to perform a risk assessment is considered willful non-compliance with the law. The downside of a risk assessment is that the health care entity that performs a risk assessment must address the exposed vulnerabilities.

For investors, the lessons are simple. Only invest in companies that address security as part of the IT development process. Security safeguards need to be met to even start a conversation with a covered entity or business associate. The same rule should apply for conversations with investors.

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

CYBER CRIME IT CAN'T HAPPEN TO ME RIGHT? WRONG!

By Terry Pitts



We always think that the stories we hear about Cyber security threats and ransomware attacks only happen to others not me, right? Dead wrong! What is ransomware anyway? Well the dictionary defines it as "a type of malicious software designed to block access to a computer system until a sum of money is paid." The occurrences of these cyber security crimes seem to be increasing. We hear more and more stories of those attacks to institutions and to individuals it seems everyday. They are costly and sometimes devastating.

With the increasing security mandate around HIPAA and the need for all of us to better protect all of the medical records and information we deal with everyday in our healthcare environments it has become a much larger issue than just a couple of years ago. Usually a threat goes like this. "Your hard drive is locked and we will release it back to you when you pay these amounts of dollars if not then you will never be able to unlock or access your hard drive." And if you have not taken the pre-cautionary steps to copy or backup your critical data then you are in deep trouble. The payments are requested to be made to some bitcoin account where it can not be traced. We have heard story after story where these occurrences are now everyday common place. Violations to the HIPAA laws are much more costly than ever before.

It happened to me this summer. It was exhausting. It took 30-40 hours of work, some money, considerable stress and much frustration. I was speaking to a CEO of a large Healthcare It company that hired a PhD of cyber security for his organization. After they implemented all kinds of protection software on their lap tops he was recording a threat every five minutes. This CEO had a neighbor that had to pay $250,000 to unlock his hard drive data because he had no other choice. In a third case the president of an HOA's hard drive was locked up and he just threw his computer away rather than deal with it. Do these sound familiar to you?

What do we do? How do we protect ourselves against this increasingly costly threat? It is paramount that you review your protection policies and implement fail safe processes that protect your data at the organizational and individual level. We all enjoy the benefits of the ultrafast information age but it can be a two edge sword. They call this a "white collar crime", my opinion is they should treat these people just like they treat a guy that sticks a gun in your belly.

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

A DEEP DIVE INTO SECURE MESSAGING IN THE HEALTHCARE MARKET

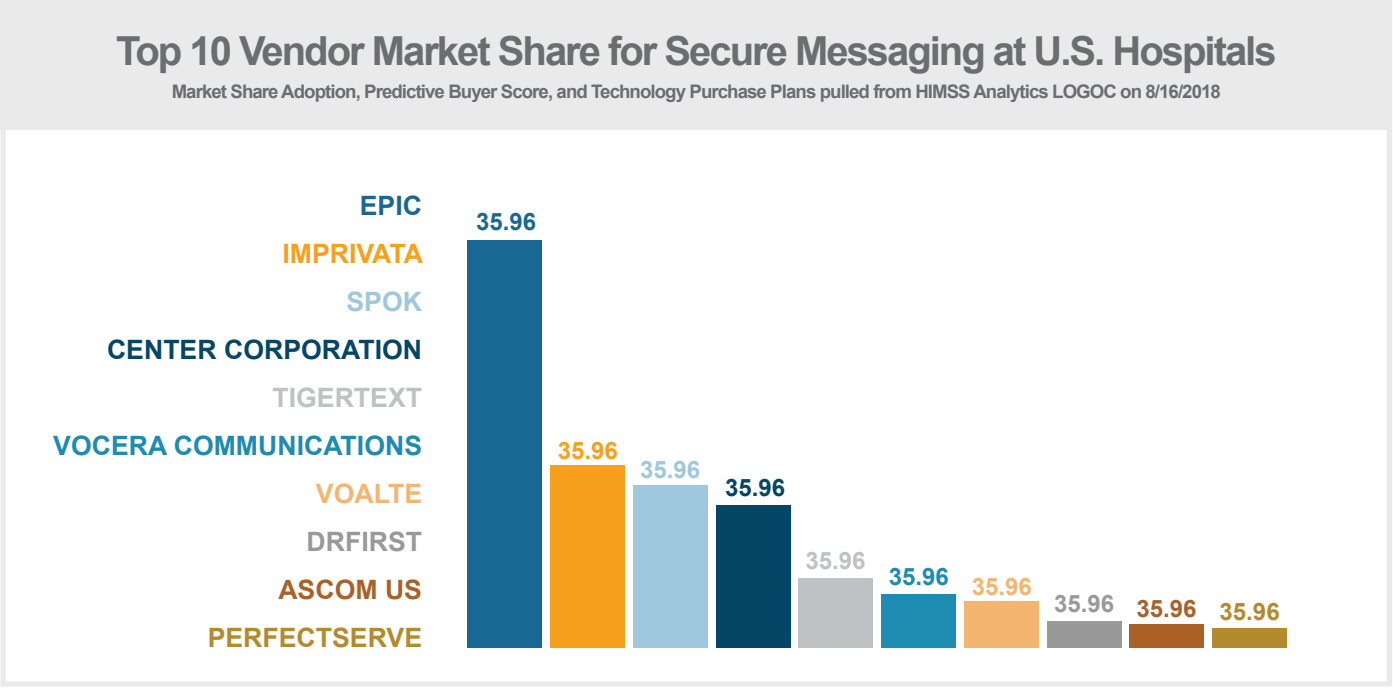
By Blain Newton

As laptops, smartphones and other personal devices become the norm in our hyper-connected world, it's no surprise that secure messaging has been gaining ground in the healthcare industry. Secure messaging technology enables healthcare staff to communicate via secure platforms to maintain compliance with HIPAA, HiTech Act and Joint Commission requirements.

Without a secure messaging solution in place, many providers may resort to texting about patient care via SMS or other unsecured channels, risking HIPAA violations, data breaches and fines. Considering the steadily-rising threat of hospital data breaches, the amount of protected patient health information going through these unsecured channels is an issue that needs to be addressed. Although adoption rates at U.S. hospitals are still fairly low — as of this year, adoption is just over 8 percent — secure messaging is a technology that will likely become an essential tool for coordinating patient care moving forward.

Low Adoption Rates Mean High Potential for Vendors

HIMSS Analytics began tracking secure messaging as one of our 200+ technologies in Logic in 2016, and we've seen adoption rates steadily rise. There's still a tremendous amount of greenspace in secure messaging right now, offering ample opportunity for vendors looking to break into this market. For vendors seeking growth opportunities, it's important to note that the secure messaging market share is led by Epic (35.96 percent), Imprivata (16.08 percent), Spok (14.33 percent) and Cerner Corporation (12.57 percent), (see chart below). The question then shifts to which hospitals are really ready to buy?



Secure Messaging Installation Led by Small, Not-for-Profit Hospitals

The vast majority of U.S. hospitals with installed or plans for secure messaging solutions are small, Not-for-Profit organizations. Just over 70 percent of the hospitals with installed or planned secure messaging technology have 250 beds or less, and only 16 of these 477 hospitals are For-Profit.

Why?

There could be several reasons. One of which may be that smaller hospitals are at the sweet spot for adopting new technology; in larger hospitals, it's more difficult to gain buy-in for new technology because most decisions are made by a committee. Smaller hospitals, on the other hand, tend to have fewer decision makers.

Additionally, there are differences between Not-for-Profit and For-Profit hospitals. For-Profit hospitals, for example, have to straddle the line between providing excellent patient care and turning a profit. They may not see secure messaging technology as a priority, because it doesn't have an obvious, immediate impact on the bottom line — but when the risk is being hit with a HIPAA fine and scarring the hospital's reputation due to a data breach, it may be cheaper to invest in secure messaging sooner rather than later.

The Security and Privacy of PHI is Everyone's Responsibility

Nothing's likely to change regarding people's propensity for using their personal devices at work. In this digital age, it's a fact of life. Regardless, providers can't make the mistake of texting protected health information without thinking about compliance; it's a dangerous, fineable offense.

The rise in data breaches is increasing the focus on securing patient data, and secure messaging technology is a key component of that. Along with secure messaging, Bring Your Own Device (BYOD) policies should be implemented to avoid further security risks. As communication technology becomes increasingly close and convenient, it becomes the responsibility of everyone involved — not just IT personnel — to take the privacy and security of patient data into mind.

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

HIT·IQ | THE LAST WORD

Featuring profiles of entrepreneurs and leading innovators

Jeffrey S. Muller

Jeffrey S. Muller, President/CEO at Muller Group International

Jeff, thank you for sharing your thoughts with our readers. Cybersecurity issues and risk across all sectors continue to grow exponentially. Many of our readers are HIT investors and bankers. Depending on when they engage with prospects, they may not be aware of early thinking and decisions that founders may make regarding security considerations. With that in mind: When conducting due diligence, what guidance would you give to investors as they consider funding a health IT sector start-up? What should be regarded as non-negotiable? For potential investors in any sector, there are three major areas: (1) the financial well-being of the company, (2) its structure, and (3) the personnel. Investors should include multiple levels of security due diligence. Finance and Personnel due diligence: Investors typically focus on the financials and business experience of the founders, which is important, but no longer sufficient. Investors should also conduct in-depth due diligence which includes all key personnel, associates and other investors.

Just doing a simple criminal background check is no longer enough. Investors and founders need to look into past activity, including social media, and we strongly recommend that they go into the Deep and Dark Web to see if there is any relevant negative information. You don't want to discover that one of the principals is active in criminal activity after the deal has already gone through. Some might find the guidance to research the investors surprising, but just as investors should conduct their due diligence on founders, so should the company on potential investors.

Many HITIQ readers are interested in expanding globally. What thoughts do you have about essential due diligence considerations when investing and building a business outside of the U.S.? We've had many clients where we've conducted in-depth background checks and discovered that the potential investors, key staff or other associates had associations with groups that the U.S. or other agencies, such as Interpol, have deemed risky or been found to provide funding to terrorist groups. Doing proper due diligence is fundamental to supporting positive brand management. We provide the information, and the company or investors can determine if they care about being associated with that individual. As noted, for key personnel, low-level criminal checks are usually not sufficient. You have to be able to go global and deep into people's backgrounds.

Comprehensive security due diligence is essential for all sectors, but I'll focus on Health IT (HIT) considerations. It all starts with understanding the company and its ability to protect data and information. We recommend ensuring the startup has had or will have a three-level security risk assessment: administrative, technical and physical.

Administrative: HIT companies must have a comprehensive health care security program to ensure they are following laws and requirements. Here are a few examples.

- Are the HIPPA rules understood and followed?
- Do they have a dedicated chief information security officer (CISO)? This job is often delegated as a secondary or tertiary to Finance or HR and is not being handled at the proper level in the organization.
- Have a reporting process in place where people feel safe to report issues of concern.
- Have an oversight board meet regularly (quarterly is a good start) to discuss cyber issues to ensure there is always a continuous focus.

Physical: Is their physical space protected? Who's coming in & out? Are staff and visitors properly badged? Do they know who's getting on & off the network? How they are securing digital data, and if they deal in paper, how are those assets protected? What about physical media, such as laptops and drives? Are those secure? A robust technology system should include data encryption and network devices able to track who's accessing network resources and regular checking of audit logs.

Technical: We do a lot of network analysis. Data encryption is probably the #1 area, along with proper audit logging, secure network configuration and more. Here are some less obvious, and hence crucial problem areas we see. Do they have end-to-end protection for their IoT-devices? We see increased incursions in areas that often go unnoticed. For example, we find too many companies not thinking about their printers - hackers can access networks through connected printers.

Incident response plan: Too many organizations fail to do this properly, if at all. Conduct a tabletop exercise – if one site goes down, is data still accessible? Do you have an early notification and response plan that has been adequately tested? What is the status of your disaster recovery plan? Many companies have IT disaster plans, which is fine, but these are not linked to their business continuity plan, and they should be. IT disaster and business continuity should be part of the overall plan so when it happens, they have already run the tabletop which will make the actual response much smoother. HR and Legal should also be involved – these are not IT-only issues – these impact the core of any organization.

Another challenge we see is IT sprawl. As cybersecurity has gotten more challenging, firms are doing more, and often find themselves with multiple IT systems. There is much in the media about this issue. What are your thoughts? We look at this from a couple of angles. Many firms are switching from big traditional providers to boutique firms for a variety of reasons including cost reduction and access to specialized services. At a minimum, we recommend that they ensure their vendors can provide continuous service and have strong backend support. Investors and companies also need to conduct their due diligence on their providers to ensure they are also following proper security procedures and protocols.

Another potential is to roll up several specialized companies. Many are sole source providers, and a firm could combine 3-4 companies with an integrator in the middle to bring it all together.

Tell us a bit about you and your firm and a current favorite project. We are a global security company. We consider ourselves a systems integrator with experts in critical infrastructure. We are also bringing new technology and approaches to market.

One program that we are excited about is the Safe in School Program which has layers of prevention and mitigation including shot detection developed for military uses. We are working with them to introduce this technology that can be applied to save lives – unfortunately, this need continues to expand. There are also other approaches. For example – teachers and school administrators can be provided with an alarm program on their phone for rapid reporting and reaction events. Our systems are designed to provide responders with enhanced situational awareness so that they can affect a more effective and efficient response.

Is there anything else you think our readers should know?
We see investors and founders invest millions or even hundreds of millions and yet fail to conduct more than an inspection of the books and a Google web search on founders. In today's complex world, they have a responsibility to themselves, their investors, employees, and customers to do more to keep all of them safe and secure.

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