HealthITSecurity

Best Practices in Secure Messaging

Balancing HIPAA Compliance and Accessibility

Sponsored by

imprivata

Preface

The "Wild West" of communicating within a clinical setting and outside of its four walls has undoubtedly come and gone. Instead of pagers, clinical employees have smart phones and often text each other while at work or perhaps at home. The truth for most organizations is that, without malicious intent, clinicians regularly communicate via insecure email or on mobile devices, regardless of compliance policies in place. With these realities in mind, healthcare organizations are not only expected to allow employees to communicate efficiently to help improve patient care, but also do so in a secure manner.

As such, healthcare organizations need to be proactive and stay out in front of consumer habits by having secure communication strategies in place and providing users options before issues arise. This guide will review how organizations can best approach internal communications and adhere to federal privacy and security requirements, such as HIPAA. Read how organizations are using secure communications platforms to help boost productivity while ensuring that messages are secure and users are authenticated.

Table of Contents

Top Five Qualities of a Healthcare Secure Messaging Platform

With the understanding that healthcare organizations absolutely need to implement some type of secure communications platform, the question becomes, what should they be looking for in a product?

Tech-savvy healthcare organizations know that there are no HIPAA-compliant secure messaging services, only the means to help organizations use communications technology in a HIPAA-compliant manner. Any solution will need to have the right blend of security and usability for clinical employees, but there are some specific qualities that are essential to an organization staying within HIPAA's boundaries.

Here's a look at five important qualities:

1. Integration capabilities with current and new infrastructure

Interoperability needs aren't just limited to EHRs, as a secure communications platform needs to be able to fit in with your environment. If, for instance, the organization's EHR software already has an automation function for internal communication, how would that align with a new platform that allows physicians to communicate on all devices? It's important for organizations with a large number of employees, including independent physicians who aren't on the payroll, to ensure that communications technologies interlock and there are no security loose ends.

2. Technical safeguards

This sounds obvious, but many organizations fail to adopt standard (and necessary) configuration and technical controls on mobile devices used to access their internal networks or systems.

Many organizations these days are enacting policies that prevent electronic protected health information (ePHI) from being stored on the device, some of which use platforms that store the data in a third-party cloud as well. However, regardless of the organization's approach, ePHI must be encrypted both in transit and at rest. For data in motion, using with RSA 2048-bit Secure Sockets Layer (SSL) and AES 256 bit encryption would be a good example of strong technical safeguards because 2048-bit has become the baseline for SSL certificates.

3. Support for platforms meeting BYOD demands and nursing workflows

There are quite a few secure short message service (SMS) applications out there, but many larger organizations are looking for a comprehensive product that can secure all forms of communicated PHI. Moreover, selecting a standard for communication for your hospital requires meeting the communication needs of both physicians and nursing users. Oftentimes, physicians bring in their own device, so having support for iOS, Android, and Blackberry devices as well an application for desktop users will enables them to communicate easily across desktop and mobile devices.

4. Having a BAA sign, sealed, and delivered

More than ever, healthcare organizations are conscious of which vendors they deal with and a bare minimum requirement for using any secure messaging platform should be having a HIPAA business associate agreement (BAA). Considering patients' ePHI may be either running through a vendor's network or stored in a remote cloud server (depending on the product), having a BAA will assure the organization that the vendor is responsible in the event of a breach as well.

5. Message logging and audit capabilities

Having control of communications and audit trails is important for some providers and these are certainly endearing qualities of secure messaging platforms. From knowing who is reading messages containing ePHI to being able to look through audit logs in case there's a clinical workflow issue, organizations want to have access to communications records. Also under this umbrella may be the ability to either remote wipe messages or put a protocol in place that deletes the messages after a determined amount of time.

Ensuring HIPAA Compliance among Inpatient, Outpatient Docs

The continuum of care continues to expand and is forcing integrated delivery networks and health systems to reconsider their health data privacy and security practices after addressing the features unique to inpatient and outpatient clinical settings.

Over the past several years, one of the largest nonprofit health systems in New Jersey has increased the size of its organization through the acquisition of physician practices and taken upon itself the task of making these ambulatory providers as HIPAA- and HITRUST-compliant as their inpatient counterparts.

"From a hospital perspective, we've been doing information security risk assessments since 2004 — third-party, outside — that includes penetration testing and all kinds of things," said Atlantic Health System Vice President and CIO Linda Reed, MSN, RN, MBA.

"A couple years after that, we started performing annual HIPAA assessments in which we run through what would happen if a HIPAA auditor came in, " she continued. "A few years ago, we extended this process to the physician practices because as we acquired more and more of them we had to make sure that they could also pass."

Ensuring privacy, security on the inpatient side

Consisting of four medical centers, one children's hospital, and a growing number of physician practices, the various settings have different health information technology in place and therefore differing perceptions of what best practices in health data security and privacy entail.

On the inpatient side, a trend toward mobility and virtualization has helped eliminate potential gaps in data security and privacy and increase access for clinicians. Recently, the New Jersey health system implemented a secure clinical communication tool called Imprivata Cortext to complement its virtualized desktop and single sign on functionalities.

"We've had something called mobile rounding in place for a long time and the physicians got used to it, but what happened is that you had to have a piece of software on your device and it didn't let them to talk to each other," explained Reed. "As texting became more ubiquitous and easier to use, they began using that and very quickly we all knew that that's not a secure medium to do that, especially if you're going to use PHI."

The decision to implement the secure texting tool came about as a means of safeguarding even well-intentioned providers against themselves in a convenient way.

"Telling them not to doesn't help because they are going to do it anyway," Reed continues. "Everybody puts the same policies in place — we did just like everybody else — no texting allowed and it promptly gets ignored. We figured that we had to put something in place as an alternative so if you are going to talk to someone or if something does happen, we do have the secure texting tool."

According to Reed, physicians sometimes cannot help themselves when working to improve the outcomes of their patients despite mandatory training about vulnerability and breaches. "So even though they know, they need to get something done. Physicians are the ultimate pragmatist. Sometimes there is that mentality — it won't happen to me," she reveals.

Ensuring privacy, security on the outpatient side

In her dealings with physician practices and extending the health system's health data security and privacy practices there, Reed quickly realized that a different kind of approach was necessary to bring these outpatient settings into a compliant state. "It is still a concern when we acquire physician practices. Some of them are not hosted and running their own little servers sitting in an unlocked office somewhere under a desk," she maintained.

The New Jersey health system has taken a direct approach to mitigating risk by putting boots on the ground.

"We go into the offices and do a walkthrough," Reed explained. "We take a look at where their screens are placed, where all the technology is, where the printing winds up. We've also done a bit of social engineering testing — calling the office and seeing if you can work a password out of somebody. And it does happen at times. Having the HIPAA audit, having all the HITRUST stuff documented — we put that all in place."

The process is particularly important for eligible professionals in the EHR Incentive Programs for meaningful users for whom the risk analysis is required and a major focus of auditors.

"As you look at meaningful use many folks skipped that piece," argued Reed. "I don't know if it just didn't occur to them or they didn't know what it meant. They had checked it off as doing it, but they never did. It's fascinating."

For these physicians, working with a regional extension center has paid off, says Reed. However, the risk is still there for those practices looking for a quick or cheap fix.

"It depends on who is doing meaningful use for some of these offices," she observed. "Some of them were working with our regional extension center and got some good direction and tools from it, but the ones who were doing it on their own found it a little difficult. There are lots of people out there selling info-sec security assessments you can do yourself — that's a little frightening."

To reduce risk, the Atlantic Health System has worked to move practices from an onsite to hosted EHR system before ultimately making one system available to these providers in the long run. "If we can move them to a hosted version, that's probably the best option for us temporarily until we can start rolling everyone on to the single EMR," added Reed.

Until then, the onus is on providers in both settings to be trained and tested on their health data privacy and security practices.

Why HIPAA Compliant Secure Messaging Is Crucial For BIDMC

Patient portals are slowly becoming more common in the healthcare industry, along with the option for patients to securely message their physicians through the portal. But just how effective are those messages, and what do healthcare organizations need to keep in mind to ensure that patients' information remains secure?

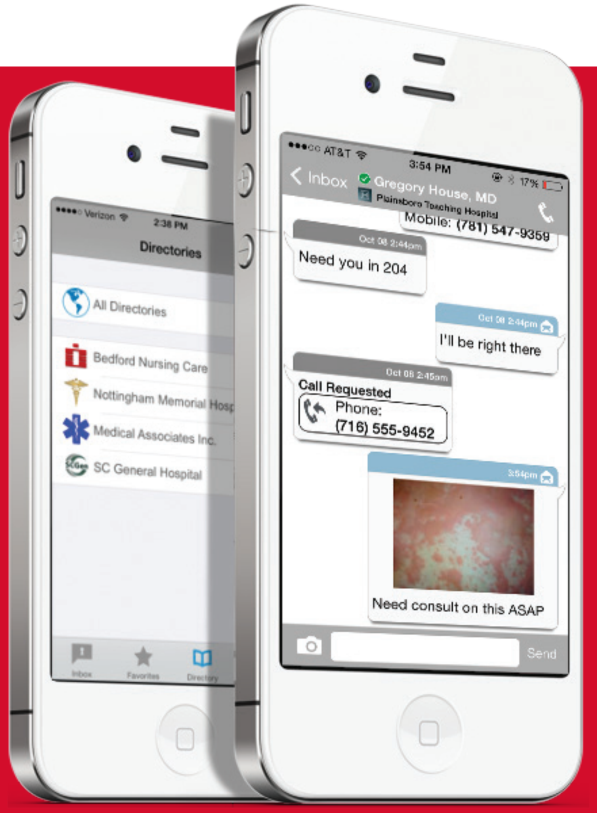
Beth Israel Deaconess Medical Center (BIDMC) recently released the results of a study it conducted on the effectiveness of secure email messaging between physicians and their patients. According to the results, reimbursement models and physician workflow may need to adjust to accommodate message management.

Bradley Crotty, MD, Division of Clinical Informatics for BIDMC was the report's lead author and explained that BIDMC was one of the nation's first hospitals to create a patient web portal that offered a secure platform for patients to view their medical records and send emails to their physician.

"One of the key messages that this study brings out is that practices and hospitals need to prepare for the secure messaging exchange between doctors and patients," Crotty said, adding that it should no longer be something that doctors do in their spare time. "It really should be built in the workday of a physician."

For the study, researchers gathered information over a 10-year period (2001–2010). At the end of 2010, 49,778 patients (22.7% of all patients seen within the system) had enrolled in the portal. Moreover, 36.9 percent of enrolled patients (8.4% of all patients) had sent at least one message to a physician.

The key takeaway was that the overall number of messages per patient did not increase over time, Crotty said. Instead, as more patients signed onto the system, more doctors had messages in their inboxes. As more patients sign up for secure portals, they are going to be something that all physicians will encounter, he said.



All Directories
Bedford Nursing Care
Nottingham Memorial Hosp
Medical Associates Inc.
SC General Hospital

Gregory House, MD
Plainsboro Teaching Hospital
Mobile: (781) 547-9359

Oct 08 2:44pm
Need you in 204

Oct 08 2:44pm
I'll be right there

Oct 08 2:45pm
Call Requested
Phone:
(716) 555-9452

3:54pm
Need consult on this ASAP

Communicate Securely with Imprivata Cortext!

Imprivata Cortext® is the secure communications platform for healthcare that enables organizations to replace pagers and improve care coordination inside and outside the hospital.

Imprivata Cortext can help your organization:

- Replace pagers and outdated communication technologies with secure communication across any desktop or mobile device
- Increase care team coordination across multiple healthcare organizations and affiliated networks
- Avoid HIPAA violations by eliminating insecure SMS texting of PHI

Visit www.imprivata.com/ct-demo for a demonstration.

For more information:
cortext@imprivata.com
www.imprivata.com

"The most important aspect of patient-to-physician messaging is the security of the message content itself," Crotty said. "These are often personal messages, they contain health information and they contain identifying information about patients. The messages need to be encrypted and then transmitted over the internet in a way that is encrypted from beginning to end."

This is not something that traditional email does, Crotty explained, which is why more organizations are leaning toward secure patient portals.

HIPAA did not specify how messaging between a physician and a patient needed to take place, Crotty said, it merely said that it needed to be done securely. Healthcare organizations can choose whether to do it through a secure patient portal or though secure email technologies.

Crotty also highlighted the fact that in many patient portals, the secure messages are captured as part of the patient's medical record. This is a good thing in many ways, Crotty said. Moreover, the messages can be reviewed by a physician at a later time, and transcripts are also recorded so the system is "basically self-documenting."

This approach keeps the messaging confidential, but there are risks and benefits with each messaging option, according to Crotty. For example, in a telephone call with your physician, just you are speaking to your physician. Whereas with patient portals, other people in the healthcare system who have a "need to know right" to certain information are able to access it when necessary.

Why Saint Mary's Hospital Opted for Secure Messaging

Waterbury, Conn.-based Saint Mary's Hospital recently implemented a secure messaging system to improve its overall clinical communications. The facility opted for Imprivata Cortext, which is a HIPAA-verified secure communications platform for smartphones, tablets, and desktops.

Tom Calo, Saint Mary's technical solutions engineer, and Birgit Koellmer, nurse informaticist at the hospital, spoke with *HealthITSecurity.com* about the recent changes and what it means for Saint Mary's in the long-term.

The duo agreed that communications have definitely improved and the staff is very pleased with the secure messaging options. In fact, many have said that "it's the coolest thing ever right now," according to Koellmer.

ELIZABETH SNELL: How is Saint Mary's using the secure messaging system?

TOM CALO: We just recently rolled it out and right now, we're kind of using it just as a general communication tool. It's the kind of thing where it builds its own workflows as you go, and people are figuring out ways to use it and things like that. We do have a couple of different workflows that we are trying to implement, with nurses contacting physicians, pharmacists contacting physicians, and physician-to-physician. We're in the initial roll out of it, so every day we're thinking of different ways they can use it. Just in an overall organization communication tool is what we're really trying to build it into.

ES: What was your selection process for finding a secure communications solution?

TC: We did talk to a couple of other vendors. We already were Imprivata OneSign customers, and had been playing around with their Cortext when it first came out, but were just kind of testing it. We realized that it was definitely something we needed to look into. And by walking around, seeing what the employees were doing, we tried to get them to use it in the beginning.

Most people weren't really interested until we really knew there were a couple of people who mentioned they were messaging in a non-secure way that we got our marching orders to go choose a vendor.

BIRGIT KOELLMER: We already had a good roll-out with the single sign-on from Imprivata. So we thought having it all in one hand is much better for us than choosing another vendor. We also chose it because we liked that it was specific to healthcare environments.

TC: Yeah, the value we see with Imprivata is they help you with workflows — the clinical workflows. They know them all, they had them figured out. They helped us and helped us design them. Some of the other vendors, they do healthcare, but they're more specifically selling licenses and moving on to the next. They don't really care what industry they're talking to. Everybody that I speak with at Imprivata understands the healthcare industry.

ES: How do you see this impacting Saint Mary's in the short- and long-term as technology continues to evolve and you potentially implement new systems?

TC: Well in the short-term, I think it's obviously bringing everybody in the organization to rapidly act on things when something is out there. I've been saying that I like this to become the de facto tool of how we communicate: This is where it's at. This is what's in effect right here. We don't want it to be messages that aren't that important, things like that. If we did want to do a broadcast we'd make sure we want everyone to know this.

In the long-term, I see it being something that is integrated into the entire delivery of healthcare. For example, we have too many EHRs here. We're a small hospital, but we must have six to eight easily. Some of them are flowing information, some of them aren't. It can be something that brings it all together.

BK: I also want to mention that we like to see it as an emergency preparedness. For example, if there would be an emergency, or an event going on, we can easily send messages out to the entire organization.

ES: What advice would you give other healthcare organizations that are considering this, but are hesitant for various reasons?

BK: The employees didn't want to realize it, or they wanted to close their eyes to what was going on. They said "Oh nobody is texting." But this is blind, because if you walk around in the hospital, you see everybody texting. They used their own phone because they're used to it, and want to use it in the workplace the same way. So they said, "We don't allow anything right now." And whenever somebody came around, they tossed it in their pockets.

We were seeing that. And if organizations say it's not happening in their work place, they really need to open their eyes a little bit more and look closer to what's going on in their organization. And you don't want that patient information outside of your organization — you want to keep it within.

We said, "We want to provide a tool so they can do what they do at home and everywhere else." We just didn't want to say, "We're shutting it off totally. Leave your cell phones at the door." We wanted to provide a communication tool for them. We wanted to make them more aware that this is still happening, and people are doing it even if you say that. So just provide staff the correct tools to do it correctly.

TC: Yeah, you definitely have to have that more modern thinking towards security. Our security teams kind of had their head in the sand in the beginning. They were saying that they weren't just turning their head away, they were banning it. You can't just ban something. Today's information technology is user-focused and user-centric, and you have to do what the users want because no matter what you do — and if you tell them what they can't do — they're still going to do it.

We're still struggling with this. I feel like you have to come to an agreement with the end-user. Say, "We're not going to stop you from texting, but we want to give you the right tool." That was the problem that we had.

We ended up getting it the way we needed, but we struggled in the beginning. It was a matter of not having everyone up to speed at the right time about how we have to do. There's no more fighting with the end-users.

ES: Any other general advice or tips for facilities implementing secure messaging?

TC: Again, working with the users from the very beginning will make a big difference. We had a lot of people that were against it like you wouldn't believe. And they've come full circle now. They're the ones promoting it.

BK: Actually, we have very good feedback from our users. They think "it's the coolest thing ever right now." We put so many medical records on them, and electronic records on them. Every month there is something new for employees to have to learn. And it's a struggle. But this is something that's easy for everybody to use. And it's easy to learn, not something you struggle with.

TC: This was the first time IT did something cool that employees really liked. We were pretty lucky to be able to work with Imprivata; both of the modules we purchased. Those were the cool things that everybody is loving.

Implementing Secure Text Messaging at Greenwich Hospital

Secure text messaging gives healthcare providers the opportunity to quickly — and safely — send critical information to patients. It's essential to choose a messaging option that not only meets HIPAA regulations, but also meets the needs of patients and facility employees.

Connecticut-based Greenwich Hospital recently found that balance, and according to Vice President of Patient and Guest Relations Christine Beechner, the secure text messaging program has seen great success since its July launch.

Thus far, the program is only offered in the hospital's ambulatory surgery area, but according to Beechner the patients and their families in that area always want information.

"That's a key driver for them, having information and understanding what's happening during the day," she explained. "For that reason we thought the secure text messaging would be a great fit for that area."

The program is a one-way secure system, Beechner said, and the patients must give their consent in order for their family members to receive updates. Messages can be sent in English or Spanish, and patients who consent to the system have their family members put onto a list. From there, people on the selected list are assigned a unique personal identification number (PIN) that the patient then sends to them. Employees will send updates once the PIN is verified.

The messages are from approximately 20 pre-selected phrases, according to Beechner. This was done for better healthcare security, while also to keep the hospital workflow running smoothly. Messages include sentences such as "Your mother has arrived in the unit," "The surgery has ended" and "Your father is resting in the recovery room and can have a visitor. Please call us."

"This is currently a one-way system only," Beechner said. "It works very well for both caregivers and families that way. With regards to developing it further, we're looking to use it in different areas of the hospital. Our next area would be for the Neo-natal Intensive Care Unit."

Examining the needs of all parties involved

Different healthcare organizations could benefit from different systems, which is why Beechner recommended that a facility must thoroughly examine any vendor before making a decision on secure text messaging.

"What was helpful for us is that we were able to create our own stock messages," Beechner said. "It met the needs of the staff and the families. If I did it again I would always go with stock messages because they're very quick to use and you know exactly what is being sent out."

Greenwich's system has approximately 1,200 patients signed up for the system and over 21,000 messages have been sent. More importantly, there is a high participation rate and high satisfactory rating, Beechner said.

Specifically, 60 percent of surveyed patients responded to the question of "Please let us know how you liked the program." From there, on a scale of one to five, with five being the highest, the system earned a 4.7 rating.

"It meets the needs of the families and patients," Beechner said. "If it didn't meet the need, it would not be worth doing. But knowing that our families want good information and information in a timely way, we matched the capabilities to the application to that need."

Approximately six months into the program, Beechner said that the experience and feedback overall has been "absolutely phenomenal."

"When you're able to share information in a secure and easy manner, I think it's good for both the staff, the patients and the families."

Beaufort Memorial Hospital Replaces Pagers with Imprivata Cortext as Standard Communication Solution for All Providers

Imprivata Cortext Streamlines Clinical Communication for Beaufort's Code STEMI, Radiology, Anesthesiology and other Departments to Improve Care Coordination and Workflow Efficiency

CHIME14 CIO Fall Forum—San Antonio, Texas, October 28, 2014—Imprivata® (NYSE: IMPR), a leading provider of authentication, access management and secure communications solutions for the healthcare industry, today announced that Beaufort Memorial Hospital (Beaufort, S.C.) is replacing pagers with Imprivata Cortext® as the standard form of communication for all its care providers. Imprivata Cortext is the secure communications platform for healthcare that enables healthcare organizations to replace pagers and improve care coordination inside and outside the hospital. Beaufort Memorial's Medical Executive Committee decided to standardize on Imprivata Cortext for all its physicians to improve clinical communication and care coordination.

"Several of our hospital departments have been using Imprivata Cortext and it has proven to be a far more convenient, effective solution for clinical communication and care coordination than pagers," said Kurt Gambla, D.O., chief medical officer at Beaufort Memorial Hospital. "We are excited to extend these benefits to our entire physician population by standardizing all communication on Imprivata Cortext, which we believe will greatly improve physician satisfaction, increase efficiency and, most importantly, enhance the quality of patient care."

With Imprivata Cortext, Beaufort Memorial will improve communications and care coordination while addressing the inefficiencies of pagers and other outdated technologies for a number of different clinical workflows, including:

Code STEMI—When a catheterization lab is activated, the percutaneous coronary intervention (PCI) team must be notified and mobilized as quickly as possible. Prior to implementing Imprivata Cortext, this required numerous pages to the PCI team members, waiting for callbacks and creating delays in organizing the next steps for care. Using the Imprivata Cortext group messaging functionality, an alert can be sent via secure text message to the entire PCI team simultaneously, which significantly improves Code STEMI response times and care coordination.

Radiology—Prior to using Imprivata Cortext, when a report was ready, radiologists would call or page specialists, who would then have to locate an available workstation to access the electronic health record to view the medical image and the corresponding radiology report. Using Imprivata Cortext, radiologists can more quickly alert attending physicians that the requested radiology reports are available, which improves efficiency and enhances patient satisfaction.

Anesthesiology—Anesthesiologists are highly mobile, moving between operating rooms and catheterization labs. Imprivata Cortext enables them to receive secure text messages that include not only current medications and recent lab results that could create a patient safety issue, but also updates about when they can expect patients to be prepped for surgery and administration of anesthesia.

“Our clinical staff has been extremely impressed with the functionality and ease-of-use of Imprivata Cortext, and it speaks volumes that clinical leadership—and not IT—made the decision to move away from pagers and standardize all physician communication on Imprivata Cortext,” said Edward Ricks, VP and CIO at Beaufort Memorial Hospital. “From an IT perspective, Imprivata Cortext gives us an easy-to-manage, cost-effective communication solution that also maintains compliance with HIPAA and security regulations. It also gives us a comprehensive solution for replacing costly, inefficient technologies, and in the past year, we have eliminated about half the pagers in the hospital.”

“Beaufort Memorial’s decision to replace pagers with Imprivata Cortext as its standard solution for provider communications reflects the clinical need for more efficient technologies to increase workflow efficiency and improve care coordination,” said Ed Gaudet, general manager of the Imprivata Cortext Products Group. “Imprivata Cortext is designed specifically for healthcare to meet the workflow challenges that care providers face every day, providing healthcare organizations with a secure communications platform that improves efficiency, meets compliance and security requirements and addresses inefficiencies caused by pagers and other outdated systems.”

According to the Imprivata Report on the Economic Impact of Inefficient Communications in Healthcare, more than 50 percent of the time it takes to complete patient admissions, coordinate emergency response teams and patient transfers is wasted due to inefficient communication, costing the average U.S. hospital about $1.75 million annually. The study also finds that about half this wasted time could be reclaimed using secure text messaging, saving about $918,000 per hospital, per year.

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata’s single sign-on, authentication management and secure communications solutions enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care. For more information, please visit www.imprivata.com.