Get the Message: Why Secure Texting Matters

Texting is convenient—but handling healthcare data is about more than convenience. Learn how secure communications policies protect both patients and providers.

Texting Isn't a Safe Option to Protect Health Data

Texting is fun. I like to send my friends photos of the cocktails I'm drinking. My brother texts me messages about long-lost songs he hears on Pandora. Even my 70-plus-year-old parents just got into it.

But do I want my doctor texting me about my lab results? Nope.

The whole format just doesn't seem secure. Bang out a quick message, hit send and wait for a reply. Texting is more like a game sometimes, which doesn't reflect the more serious business that healthcare should be.

Further, it's not difficult to imagine Doctor X texting the wrong info to the wrong patient by accident. It's hard to believe physicians would save patients' names as contacts in their mobile devices, which leaves docs or assistants typing out numbers on a keypad.

Ensuring secure messaging in healthcare facilities is a chore, and it's not necessarily because of the technology. As contributor David Weldon explains in this handbook, a sizable part of the challenge is simply educating people in the medical industry—from the CEO on down—that it is inappropriate and perhaps illegal to text clinical information between parties.

SearchHealthIT reporter Shaun Sutner delves further into the latter topic, issuing a warning about texting protected health information. He also rounds up some tips from a healthcare lawyer about how to avoid related HIPAA problems with these types of communications.

Columnist Reda Chouffani ends the handbook with interesting data theft figures from the U.S. Department of Health and Human Services' Office for Civil Rights. One chart shows the recurring risk of healthcare information breaches from portable devices, such as phones, laptops and tablets. Hundreds of thousands of patients have fallen victim to records stolen via these devices.

No one would text someone a credit card number for obvious reasons, and health data should receive no less security treatment. You want to text someone about the weather? Fine. Need to find out what time to come over for dinner? Sure.

But texting cholesterol levels from a screening? In such cases, skip the text and save that discussion for a one-on-one conversation or a message from a secure portal.

How has your organization handled the issue of texting by clinicians? Let me know by email at swallask@techtarget.com or reach me on Twitter: @Scott_HighTech. ■

Scott Wallask
Editorial Director
SearchHealthIT

Cultural Change—Not Tech—Key to Secure Texting

While data breaches in the retail and government sectors grabbed the lion's share of headlines last year, hospitals and healthcare systems remain a favorite target of cyberattacks. The reason is simple: the combination of vast amounts of personally identifiable information, along with electronic health records.

That combination makes the health data a potential double bonanza when it comes to successful cyberattack prizes. Without a tight lid on clinician communications and a dedication to secure texting in healthcare, thieves can exploit the risks.

"Healthcare has definitely been a growing target, and that is because of the personalized information available, plus the medical aspect," said Jay Jacobs, a senior data scientist at BitSight Technologies in Cambridge, Mass., that develops security ratings for vendors. Jacobs tracks cybersecurity incidents and data breaches, and he stressed that medical claim fraud is big business today.

BitSight publishes an annual report card on how various industries are doing when it comes to protecting data. The IT security research and consulting firm looks at a number of factors around network and data security best practices.

While some sectors—such as financial services—are doing fairly well by BitSight's reckoning, others are clearly not. That includes healthcare, which BitSight described as "poorly performing."

THE SECURE TEXTING CHALLENGE

The healthcare sector is an underachiever at data defense, even though most business and technology leaders today are well aware of the risks of compromised data and cyberattacks.

The answer to this dilemma lies in "the last

mile between the health system and the independent provider or the patient home," said Helen V. Thompson, an executive healthcare strategist and co-owner and founder of The Rockwood Group in Huntsville, Ala.

In other words, the lack of secure texting and communications is a primary factor in healthcare data risk. It is also a quick way for a hospital or healthcare organization to find itself in violation of HIPAA compliance, with swift and costly implications.

"This is a problem that we've been trying to solve for a while now," Thompson said. "Where [healthcare practitioners] don't necessarily have a good strategy or are particularly confident is in their ability to secure that data in a collaborative environment—say, between an independent physician and the hospital regarding a particular patient or that critical trilogy of the hospital, the patient and the provider."

The good news is that some healthcare organizations recognize the challenge of secure texting and messaging and are trying to do something about it.

"I have never seen so many ads for chief information security officers in the healthcare space as I have in the past year," Thompson said.

Still, one of the challenges with better securing healthcare communications is knowing at which point to start, Thompson said.

"How you secure communications is going to have many different facets because you have to ask, 'Who are you trying to secure communications with?' Is it between patient and physician? Nurse to patient? Are you doing it for marketing purposes, or for outreach to consumers? And what are you trying to share in that data?" Thompson said.

Concerns over secure communications in healthcare are certainly not lost on Mark A. Jacobs. As CIO at the Delaware Health Information Network, Jacobs' organization deals with most of the health data created within, or routed through, his state.

"In Delaware, we're the only health information exchange that exists," he said. "We're unique in some ways because we actually aggregate data from separate organizations, and we bring that information into a community health record, which represents the [accumulative] record for pretty much the lifetime of the

patient."

Like Thompson, Mark Jacobs said the fear of a data breach or compromised patient data remains a top concern. He also confirms that when an organization stores a patient's accumulative data in multiple locations that can be accessed by multiple parties, there is a notable risk. But it is the communication between parties, and the method of that communication, that can be the weakest link in the security chain.

WHERE TO START

So what is the healthcare organization to do about the problem? Jay Jacobs, Mark Jacobs and Thompson all agree that the most important first steps to ensure secure texting in healthcare are executive awareness and employee training.

That starts with the blunt notion that SMS, or short message service, communication—the technical term behind text messaging—is not secure, and it is definitely not HIPAA compliant.

"Everybody owns the responsibility for privacy and security," Mark Jacobs stressed. "You need to keep that in the forefront of everybody's thoughts. It's people, then process and then technology last. If you don't build that into your culture, and you're just buying technology and you think it's going to work for itself, it's not."

Thompson agreed, urging CIOs and CISOs to start at the top and educate hospital executives about the following issues:

- The full extent of risks to the organization's data;
- Recommendations on how to best secure a multitude of devices accessing that data;
- Access on a need-to-have only basis; and
- Applications that keep patient data secure in transmission.

The best approach is to target the individuals within the organization that are creating, accessing and sharing patient data in the first place. Make them the first line of defense, Thompson urged. —*David Weldon*

Secure Texting Strategies to Transmit PHI

Healthcare providers and their business associates are quickly coming to terms with the fact that texting protected health information (PHI) opens providers up to both security and legal issues. Not only does unsecure texting of PHI run afoul of HIPAA privacy rules, but it's also just too easy for texted PHI to be stolen, hacked, leaked or lost unless it is safeguarded.

Lawyer Lisa Thompson of LeClairRyan, a law firm based in Richmond, Va., amply underscores that message in a recent blog post.

Thompson notes that texting is popular for many reasons. It's "easy, fast and efficient," she points out. It's also considerably less cumbersome than email, and you don't need a computer to do it.

But for healthcare providers that aren't using secure texting, all this convenience can be dangerous and can lead to unauthorized access to PHI, she emphasizes.

Among the dangers that she cites are:

- Anyone with physical access to the mobile device can view text messages on it.
- Texts can be read when the device is lost, stolen or even returned or recycled.
- Traditional security protections used by IT departments of HIPAA-covered entities, such as firewalls, may not cover texts, which could then be intercepted and decrypted.

Another problem is that HIPAA also mandates that patients and their representatives, such as lawyers and families, have timely access to their health records. Thompson notes that when texts are used in healthcare decision making, providers could be out of compliance with HIPAA if patients ask for the texts in question and providers can't turn them over.

Thompson acknowledges that there is no easy response to these risks.

However, at the least, providers and business

associates should include mobile phones and other devices on which PHI is created, transmitted, received and maintained in text form in any risk analysis, a step that HIPAA requires.

The clearest path to protecting texts in healthcare settings is by using secure texting technology, according to many in health IT.

Indeed, secure messaging is one of the strategies Thompson lists for combatting the potential scourge of unprotected texts that contain PHI.

Others steps include:

- Establishing policies that require all texts to be deleted within a specified time period.
- Using technology that can wipe information from devices or remotely disable mobile phones if they are lost or stolen.
- Providing encryption and password protection.
- Setting policies and guidelines that limit information contained in texts, such as not using patient names or other identifiers.
- Requiring texted PHI to be added to formal health records and providing a technological mechanism for doing so.
- Training employees on texting policies and procedures.
- Handing down disciplinary measures for employees who violate texting policies.

Healthcare providers would do well to heed Thompson's advice.—*Shaun Sutner*

EXPERT ADVICE

Lessons to Learn from Healthcare Data Breaches

Security experts have been heavily warned about the dangers that health IT departments face from cyberthreats, but those warnings haven't been enough to prevent more healthcare data breaches from occurring. Hospital IT executives want to be sure they are taking the appropriate precautions to protect their data and infrastructures.

So what are some of the lessons to be learned from previous reported attacks? Are hackers bypassing commonly used security systems? What systems are the most vulnerable within a health IT infrastructure? Could secure communications policies lessen the chances of a data breach? These are some of the many questions IT executives are asking in evaluating their data security protocols.

Information on healthcare data breaches is available to the public on the HHS Office for Civil Rights' (OCR) website. The data provides insight into reported data breaches in healthcare and can be used to help prevent repeat scenarios.

For example, the OCR findings uncovered where health information suffered breaches in 2015 included:

- Network server: 228.9 million individuals affected
- EHR on a network server: 11.7 million
- Email: 1.1 million
- Laptop: 1 million
- Paper and films: 482,000
- Other portable electronic devices: 377,000

According to the OCR, hacking or other IT incidents have been the most frequent causes of data breaches, followed by data theft and unauthorized access and disclosure. Health plans have been the most commonly affected targets, followed by healthcare providers and business associates.

HOW TO AVOID DATA BREACHES

The general takeaway from this data is that more must be done to prevent healthcare data breaches. The following are methods to help keep patient data protected:

- Install and implement strong network security tools that can protect the IT environment, and provide visibility over what is happening in the network to avoid data leakages.

- Monitor internal systems for unusual data transfers and abnormal server activities. Hackers are able to steal data over long periods of time and their presence can go undetected for weeks or months.

- Encrypt laptops and implement strong passwords for any device that stores protected health information (PHI). This will reduce the number of patients affected by a breach. It should be a rule that the devices of anyone who interacts with or stores PHI should be given the strongest levels of protection and follow secure communications guidelines set by the organization.

- Ensure HIPAA Business Associate Agreements (BAA) are in place with all vendors. Healthcare entities must have their own processes in place or use contract management platforms, such as iContracts or SharePoint, to obtain and keep a BAA with all of their business partners.

- Implement a strong role-based access plan so that only the appropriate users have access to PHI. The plan also ensures that audit trails are available to offer visibility into who interacts with the data.

- Audit systems frequently employ third-party vendors to attempt to penetrate systems and perform security drills.

Security is a top priority for all healthcare IT executives. It is an area that will likely keep IT professionals busy and force healthcare providers to make investments to keep all internal systems safe. Without constant monitoring, data can fall into the wrong hands and patients and providers will both pay a price for such a breach.—*Reda Chouffani*

REDA CHOUFFANI *is vice president of development at Biz Technology Solutions Inc. Follow him on Twitter: @healthcareITGuy.*

SHAUN SUTNER *is news and features writer for SearchHealthIT. Email him at ssutner@techtarget.com and follow him on Twitter: @ssutner.*

DAVID WELDON *is a Boston-based writer and editor. He focuses on technology, business, education, retirement planning, healthcare and careers.*

TechTarget

Get the Message: Why Secure Texting Matters is a SearchHealthIT.com e-publication.

Scott Wallask | *Editorial Director*

Alex DelVecchio | *Site Editor*

Jacqui Biscobing | *Managing Editor*

Shaun Sutner | *News and Features Writer*

Kristen Lee | *News Writer*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Stephanie Corby | *Publisher* | scorby@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

COVER ART: FOTOLIA