The Only Safe SMS Texting Is No SMS Texting

Cheryl Toth, MBA,* and Michael J. Sacopulos, JD†

Many physicians and practice staff use short messaging service (SMS) text messaging to communicate with patients. But SMS text messaging is unencrypted, insecure, and does not meet HIPAA requirements. In addition, the short and abbreviated nature of text messages creates opportunities for misinterpretation, and can negatively impact patient safety and care. Until recently, asking patients to sign a statement that they understand and accept these risks—as well as having policies, device encryption, and cyber insurance in place—would have been enough to mitigate the risk of using SMS text in a medical practice. But new trends and policies have made SMS text messaging unsafe under any circumstance. This article explains these trends and policies, as well as why only secure texting or secure messaging should be used for physician–patient communication.

KEY WORDS: Text message; texting; SMS; secure messaging; HIPAA; privacy; safety; encryption; technology; patient communication; patient safety; clinical documentation; medical record; telemedicine.

A n on-call physician is enjoying dinner out with her family on a Saturday evening. She’s part of a progressive group of surgeons that allows patients to communicate with their doctor using e-mail and short messaging service (SMS) text messaging. The practice is smart. It has mobile-device policies in place, physician devices are encrypted, patients sign a risk disclosure statement, and staff is trained on the acceptable and unacceptable uses of electronic communication.

The surgeon receives an SMS text from a patient who had a knee arthroscopy last week. He attaches a photo of the incision and asks if she thinks it looks ok. Although the image is not the best, the wound appears acceptable. She replies, “yes.”

Could this physician have just incurred liability while waiting for her entree? Sadly, yes. What seems like a simple response to a patient has just opened the practice to a certain degree of risk. And this risk is more significant than in years past. In this article we examine the most current risks associated with physician SMS text messaging, and discuss better alternatives to this form of communication.

WHAT A DIFFERENCE A YEAR MAKES

In 2013, we developed a white paper about how to mitigate the risks of using SMS text message to communicate with patients. It included a number of still-valid recommendations about securing mobile devices, creating policies and procedures, and having patients sign a statement of understanding to show they accept the potential risks. In that position paper, we recommended that practices move away from SMS text messaging and toward secure messaging, although at that time, cost-effective options were limited for physician practices. Further, the risk was low that HIPAA audits would target SMS text messaging, and we were not aware of any litigation involving physician practices and SMS text messaging.

But by 2015, a number of things had happened, and we began to rethink the use of SMS text messaging, regardless of how many risk-mitigation strategies a practice has in place. Here’s what has come down the pike:

1. Earlier this year, the Joint Commission reiterated its position that SMS text messaging is too risky for patient care communications. The Joint Commission’s chief operating officer wrote a biting blog piece in April citing patient safety and communication confusion issues with SMS text messaging, and concluding that it does not have a place in healthcare.†

2. The Federation of State Medical Boards issued guidelines for telemedicine. At first blush this may seem unrelated. But it’s not. The new guidelines are intended to address telemedicine using video; however, the way
they are written, an SMS text message meets the criteria for “remote electronic communication.” The year 2015 is turning out to be a “sea change” year for telemedicine rules, and that has resulted in many state boards of medicine overhauling current guidelines by implementing these new rules.²

3. **In late July of 2015, the National Institute of Standards and Technology, in collaboration with the National Cybersecurity Center of Excellence, released a draft of its first cybersecurity practice guide, Securing Electronic Health Records on Mobile Devices. The overview of this guide lists its purpose as follows: “Specifically, we show how security engineers and IT professionals, using commercially available and open source tools and technologies that are consistent with cybersecurity standards, can help health care organizations that use mobile devices more securely share electronic health records.”³ This guide, which is approximately 80 pages in length, was open to public comment through October of this year and will not be finalized for some months to come. What is clear from this draft guide is how seriously the federal government is treating the topic of health information and mobile devices.

4. **Options for secure mobile messaging have increased significantly.** Just a few years ago, our research uncovered fewer than five secure messaging system options that enabled physician-to-patient mobile messaging. Today far more vendors are offering secure text messaging and secure message options, including practice management system (PMS) and electronic health record (EHR) vendors.

5. **The risk of practices failing to use exporting tools to extract SMS text messages from every mobile device and file each SMS text message in the patient’s record is very high.** Why? Because it’s tedious and time consuming. The result of not exporting and filing SMS text messages is a slew of “shadow records” that are strewn across physician and staff mobile devices. These bits of information are available only to the person holding the mobile device, and are nonexistent in the patient’s medical record. This is a clear and very present patient safety issue.

After assessing these new developments and risks, we have concluded that today, the only safe SMS text messaging is no SMS text messaging. Practices must move toward the use of secure messaging and secure texting as soon as they can. Even more important than the fact that SMS text messaging could be interpreted as a HIPAA violation, its use in patient care communications is a risk to both patient safety and medical record compliance. We’ve outlined eight specific risks in Table 1.

To be clear, this conclusion is intended for physician-to-patient or staff-to-patient communication, not appointment reminder text services. Such services can still be used

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Why Practices Should Care</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SMS is not encrypted or secure.</td>
<td>It can be intercepted or breached, and it is not confidential.</td>
</tr>
<tr>
<td>2. Messages are accessible only on the user’s individual device.</td>
<td>They cannot be shared easily with other clinicians, which means they frequently aren’t. This siloed nature of the messages makes them much like patient notes taken on cocktail napkins.</td>
</tr>
<tr>
<td>3. You cannot be sure that the person for whom the SMS text message was intended received it.</td>
<td>It’s anyone’s guess whether the postoperative patient or the physician’s Aunt Jean received the note. That is, until the physician receives an SMS text message back: wп, or “wrong person.” And by that time, the patient’s condition may have changed.</td>
</tr>
<tr>
<td>4. Text message “shortcuts” are cryptic, messages are asynchronous, and typos abound.</td>
<td>“Dr wdyt abt this?” accompanied by a photo of a postoperative incision site may seem like a harmless way for a patient to ask for his or her surgeon’s input about the wound. But text shortcuts do not follow standard medical abbreviations, and the risk of surgeon and patient misunderstanding each other is high. None of this bodes well for patient safety or proper documentation.</td>
</tr>
<tr>
<td>5. You cannot manage the escalation of a critical message across multiple clinicians or staff.</td>
<td>If the patient’s condition worsens, staff and physicians cannot communicate this in an efficient way. There is no written “audit trail” of what was done at what time or by whom, and when communication goes dormant, there is no way to “close” the communication or activate an automated reminder that the patient’s question may still be unresolved.</td>
</tr>
<tr>
<td>6. Messages reside on the mobile device, making them easy to breach.</td>
<td>Lose the device, and it’s easy for a hacker to find the SMS text messages, which will then have to be wiped remotely—creating the problem of medical record remnants being deleted (a big no-no).</td>
</tr>
<tr>
<td>7. Messages do not integrate with the patient’s medical record. They must be exported.</td>
<td>Very few practices ever export the SMS text messages into the record, creating a series of “shadow records” across all the physician devices.</td>
</tr>
<tr>
<td>8. Messages are sent and received from the device user’s personal contact list.</td>
<td>Trying to find a specific SMS text message for a specific patient is like looking for a needle in a haystack.</td>
</tr>
</tbody>
</table>

**Table 1. Eight Risks of Using SMS Text Messaging for Patient Care**

SMS, short messaging service.
Non-PMS/EHR Vendors that Offer Secure Physician-to-Patient Messaging/Texting

Contact your PMS/EHR vendor first. If the company does not offer secure messaging and secure texting, the following vendors are options. Each offers a cost-effective, physician-patient solution. Some may interface with your PMS/EHR system, enabling easier filing of messages into the patient record. (This list is not intended as vendor endorsement.)

- PatientReach (solutionreach.com)
- Healthloop (healthloop.com)
- PingMD (pingmd.com)
- AlertMD (alertmd.com)

because they do not run on the insecure SMS network used by cellular devices. Instead, most use similar encryption and security features as described above for secure messaging and secure texting, and comply with HIPAA guidelines. If you use such a service, check with the vendor to be sure the service complies with these requirements.

WHY SECURE MESSAGING OR SECURE TEXTING IS SUPERIOR TO SMS

To maintain patient safety standards and comply with medical records and HIPAA guidelines, practices must move toward secure messaging and secure texting as soon as possible. Whether they are included as part of a practice management system (PMS) or they stand alone, secure messaging and secure texting services use encrypted transmission, secure server environments, and message receipt verification. Messages are archived in accessible logs, data are backed up, and privacy and security comply with HIPAA guidelines. Physicians, staff, and patients must log in to access their messages, and they do so in a secure environment. Data resides on a secure server, not on the actual device, eliminating the possibility of a data breach if the device is lost or stolen.

Secure services offered by PMS and EHR vendors are ideal, because all of the messages automatically become part of the medical record, which everyone on the clinical team has access to. There are no more record bits lingering on an individual physician’s device. Stand-alone services also are an option, and many integrate with certain PMS/EHR systems.

Secure messaging and secure texting cannot solve every issue, however. Two risks that can persist even with secure messaging and secure texting are cryptic abbreviations and typos. A usage policy can outline the steps a physician or patient can take to clarify a message that is not understood.

THE “JUST SAY NO TO SMS” ACTION PLAN

It’s time to wean everyone off SMS text messaging. We know this will not be easy, and it won’t happen overnight. In fact, you should expect the no SMS texting pronouncement to be met with shock and irritation. Joseph Lister’s call for surgeons to wash their hands and sterilize their instruments was met with great annoyance too. But it was still the right thing to do in the name of patient safety.

Here’s a practical plan for going from SMS to secure:

1. Set a deadline for discontinuing SMS texting completely. A timeframe of 60 to 90 days is reasonable. Set a target discontinuation date, and back-in the action steps suggested in this article from there. Use the deadline as an opportunity to remind everyone in staff meetings and conversations that SMS must stop, and secure messaging is on its way. You might even make things fun by having buttons or temporary tattoos made that say, “Just Say No to SMS!” A little levity can go a long way toward alleviating the annoyances involved in the shift.

2. Contact your PMS vendor about secure messaging and secure texting options. Many vendors offer these features, and they often are included in the patient portal. Schedule a demonstration and training, and determine whether there will be additional costs. Many vendors include secure messaging features in their pricing.

3. If your PMS vendor does not offer secure messaging and secure texting features, evaluate stand-alone options. Just two years ago, there were very few of these and even fewer that were cost effective for small practices. Today, that has changed, and many may even integrate with your PMS or EHR. The list in the sidebar Non-PMS/EHR Vendors that Offer Secure Physician-to-Patient Messaging/Texting is not intended as a vendor endorsement. Rather, it’s a practical starting point and time-saver for busy practice managers who don’t have the time for endless Google searches. The vendor you select should offer these features at a minimum: Secure, encrypted transmission of all message data;

   - Data storage on a secure private server with backup and redundancy;
   - A remote mobile app “data wipe” option in case a mobile device is lost;
   - Automatic logout after a period of inactivity;
   - Ability to function on every spectrum of cell data and Wi-Fi in order to avoid hospital “dead zones”;
   - Message delivery validation, escalation, and tracking features; and
   - A maximum message data life of 30 days.

4. Encrypt all of the practice’s mobile devices. Encrypting all mobile devices is good practice. It reduces the risk of unauthorized parties accessing text and other data on a physician or staff’s mobile device. The details of how you do this should be included in the practice’s mobile device...
5. **Update the practice’s mobile device policy.** A mobile device policy is part of a practice’s overall data and device usage and destruction policy. Draft the mobile device portion of the policy by answering the following questions, and engage an attorney who understands your state’s privacy laws to review it.
- Who owns and has access to all mobile devices?
- What type of patient and communication data is stored on them?
- What is the level of sensitivity of that data (high, moderate, low)?
- Who makes sure cell phones and mobile devices are turned in and properly sanitized or disposed of when a physician or staff person leaves the practice?
- How do we destroy or dispose of the data on mobile devices before we dispose of the device itself?
- How do we destroy or dispose of mobile device itself, rendering it unusable? What is the process? Which data removal tools are used (e.g., Darik’s Boot, Nuke, Blancco)?
- Who does this?
- How often?
- What types of sensitive data or devices require that we obtain a data deletion certificate?
- Which third party is used to obtain data deletion certificates?
- How do we verify that the data and the device are really destroyed?

   If your practice does not have a comprehensive device destruction policy, use the guidance in our article, “Develop a Data and Device Destruction Policy in Five Easy Steps” published in the September/October 2014 issue of this journal.

6. **Develop a secure messaging usage policy.** Much like your e-mail communication policy, this one spells out the appropriate and inappropriate uses of secure messages, the practice’s turnaround time for responses, and what do when the patient’s condition is serious or worsening. For example, you want to make it clear to patients that if they have a temperature of 103°F for more than a few days, it’s best to call and speak to a nurse or schedule an appointment. And, as previously mentioned, cover the issue of using complete words to ensure clarity, and what to do if a patient or physician uses an abbreviation that is not understood.

7. **Purchase a small cyber insurance policy.** This is optional but highly recommended. Cyber insurance is a cost-effective way to protect you against expenses related to managing and investigating a security or privacy incident. It provides coverage for data and privacy breaches and crisis management, including the costs of remediation, patient notification and credit check protection, legal costs, and fines. Contact your local insurance broker for information about these policies.

   It’s a given that patients and physicians of all generations appreciate the speed and simplicity of communicating via SMS text messaging. But the risks of using this never-intended-for-patient-care method of communication can no longer be mitigated with mere policies and lack of security disclosures. Ditch SMS for secure messaging and secure texting to improve your patient safety and medical record compliance.

**REFERENCES**

1. Pelletier M. To text or not to text. The View from The Joint Commission. April 10, 2015; www.jointcommission.org/the_view_from_the_joint_commission/to_text_or_not_to_text/. Accessed October 14, 2015.

**Glossary**

**SMS (short messaging service) text message:** This is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed-line or mobile phone devices to exchange short text messages.

**Secure message:** A secure message uses encrypted transmission, and data are stored on a secure server. Access to messages requires users to log in, and data do not actually reside on the mobile device. Rather, the data reside on the secure server and are simply accessed using the mobile device.

**Secure text:** Available from some vendors (most use secure messaging), a secure text is similar to a secure message. It complies with HIPAA rules, but does not require the patient to log in to a separate application to read/respond, and patients do not use a separate mobile app to access their messages. They receive and respond using their mobile device’s SMS texting feature.