Codify
BY AAPC

# MDS Alert

## HIPAA Compliance: Texting Makes for Risky Business

**Understand why texting is dangerous before you craft policies or train staff.**

MDS coordinators and other nursing home staff spend so much time at work and with team members that the lines between work and the rest of life may occasionally blur. With texting becoming an increasingly mainstream means of communicating - between family members, between bosses and employees, between parents and schoolteachers, and even between patients and providers - it can be easy to forget how the stringency of healthcare laws and regulations doesn't necessarily align with the convenience of modern communication.

Texting on the job can potentially violate Health Information Portability and Accountability Act (HIPAA) privacy and security rules as pertains to residents' protected health information (PHI) or electronic protected health information (ePHI) - but unsecured messages can also cause facilities headaches even from an internal or human resources perspective.

In this article, "texting" refers to sending or receiving messages across a variety of platforms, including but not limited to short message service (SMS), iMessage, and WhatsApp. Facebook Messenger and other platform-specific messenger programs would also apply.

**Understand the Concerns Related to Texting**

**Context:** The HIPAA privacy and security rules apply to "all that is created, received, maintained, or transmitted by covered entities," says **Terry Fletcher, BS, CPC, CCC, CEMC, CCs, CCs-P, CMC, CMCSC, CMCA, ACS-CA, SCP-CA**, owner of **Fletcher Consulting Inc.** and consultant, auditor, educator, author, and podcaster at CodeCast, in Laguna Niguel, California.

There are multiple means in which texting (regardless of the platform) is incompatible with compliance, security, and privacy in healthcare.

Text messages on the most popular mobile devices and applications aren't encrypted, which can obviously become a problem if the mobile device is lost or stolen (or even if it's retired and not disposed of properly).

**Another issue:** "The sender doesn't have the ability to control if and when the message is discarded upon viewing," Fletcher says.

And perhaps the biggest problem of all: "The biggest one for me is no clear path to verify the reader's identity, which opens the door to unintended recipients, otherwise known as your HIPAA breach," Fletcher says.

An unintended recipient could be someone who is in the right place at the right time to see a text message pop up - the visual equivalent of eavesdropping- or even a person who was not supposed to receive the message in the first place.

Many people who are familiar with texting have had an experience where they send a message intended for one person to someone else; the most uncomfortable of those situations being when you send a message about someone to that person. If a resident's PHI is concerned, then you'd have a HIPAA breach on your hands in addition to whatever social awkwardness you'd feel.

Texting about a resident - even just clarifying information - is also tricky because any information exchanged about a resident's condition should be part of the resident's clinical record, Fletcher says. So, unless your facility and staff have established procedures for integrating the information exchanged into proper documentation, you have another reason to avoid texting.

**Craft Policies and Procedures; Provide Training**

Whatever you decide on the risks you're willing to take with texting, make sure you have thoughtful, written rules about it.

"Ensure texting is included in the policies and procedures, specifically administrative and technical policies. It's important to outline what is acceptable to text, along with an outline of steps should a text be sent to the incorrect recipient," Fletcher says.

"A trained workforce is any provider's best defense against any undisclosed PHI exposure. Workforce training should include the sharing of information, the securing of authorized devices, and using secure third-party apps that might permit sharing information in a secure way," she adds.

**Note:** If you're going to use a third-party app, make sure it's not "just an app you find haphazardly on your smartphone, but an application that comes on a list" written by a trusted source, Fletcher says. She suggests looking at the American Medical Association for appropriate apps.

When you conduct training (both during onboarding of new staff and continuing education for established team members), make sure you cover all aspects of texting, if you allow it. Include what's appropriate to text, what to do if staff messages the wrong person, and what to do if an unintended recipient gets a hold of the text, Fletcher says.

If texting doesn't seem like it could be an issue in your facility, consider how difficult the MDS can be, especially for new MDS coordinators. Texting a team member or a consultant a quick question about an item may feel like second nature, but there are obviously risks involved.

**Incorporate Texting Information When Welcoming Residents**

Draft and include a waiver about texting and other means of communication for residents and their families upon admission. Use straightforward, simple language so everyone is clear on the preferred methods for communicating.

Some residents' families may express a desire to be kept up to date about their loved ones through an unobtrusive means of communication, like a texted reminder that a care planning meeting is coming up next week. If you are set on incorporating texting with residents' families into your general communication, at least make sure you're operating with everyone's full consent.

**Resource:** For more information on how cell phone usage in a nursing facility can cause unsafe situations as well as major headaches, see "Social Media Training Tips: Avoid F-tags! Make sure staff knows your facility's cell phone policies" in MDS Alert, Volume 15, Number 8.