COMPLIANCE CONSULTING GROUP, LLC

CMS Guidance On Texting Protected Health Information

Many healthcare providers are confused about the use of text messages and whether sending messages violate HIPAA regulations. Part of the reason for the confusion is that there is no specific mention of text messages in the HIPAA regulations. There are two primary areas of concern when it comes to text messages: (1) HIPAA and the security of the electronic Protected Health Information (e-PHI), and (2) the probability that providers may inadvertently forget to include the texted e-PHI into the resident's medical record.

In order to provide some clarity on this issue, on December 28, 2017, CMS issued a memo that explained its position on using text messaging for transmitting e-PHI. In the memo, CMS stated that general texting of e-PHI is permitted as "CMS recognizes that the use of texting as a means of communication with other members of the healthcare team has become an essential and valuable means of communication among the team members." That said, the memo went on to state that texting of orders by physicians or other health care providers to a member of a care team is not in compliance with the Conditions of Participation (CoPs) or Conditions for Coverage (CfCs) and is therefore not permitted. Thus, in order to comply with HIPAA and the CoPs or CfCs, providers must use and maintain text messaging systems/platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality.

Below are some guidelines that assist in ensuring that text messages are HIPAA compliant:

- Facilities must implement procedures that provide for authorization and/or supervision of those who work with e-PHI.
- Each user must have his/her unique user identification and the actual text messages and the device that contains it should be encrypted.
- Facilities should maintain device and media controls by maintaining a record of the movements of hardware and electronic media and the individuals responsible for it.
- Facilities should have a documented texting plan for its authorized users that addresses the HIPAA Security specifications, including specifying:
  - Who is allowed to text;
  - What type of e-PHI can be texted and in what circumstances;
  - What security protocols are in place (e.g. encryption, password protection);
  - Whether e-PHI is being texted on private phones (not advised) or on company phones;
  - The security training and reminders that are provided to those who are permitted to text.

In summary, while secure texting can be a helpful tool, facilities cannot assume that texting is appropriate for relaying all information. Staff members at all levels must therefore be properly educated on acceptable forms of communication for e-PHI.