WARD AND SMITH, P.A.
ATTORNEYS AT LAW

FAQ: What Medical Practices Need to Know Regarding Communicating with Patients via Telephone and Text

Written By J. Michael Fields (jmf@wardandsmith.com)
July 30, 2024

Every day, physicians, medical practice managers, and administrative professionals call their trusted attorneys with a 'quick question' about the legality of a new approach to ensure patients come to their appointments on time.

Part I of this three-part series answers many of those most common questions.

On Leaving Messages at Home

Q: May health care providers leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments?

A: As a General Rule: Yes.

The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes -- whether through the mail, by phone, or in some other manner. In addition, the Privacy Rule does not prohibit covered entities from leaving messages for patients on their answering machines.

- However, to reasonably safeguard the individual's privacy, a health care provider should take care to limit the amount of information disclosed on the answering machine.
- For example, a health care provider might want to consider leaving only the health care provider's name and number and other information necessary to confirm an appointment, or ask the individual to call back.

A health care provider also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits health care providers to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present.

- However, covered entities should use professional judgment to ensure that such disclosures are in the best interest of the patient and to limit the information disclosed to what the person needs to know.

But be aware of this Exception: In situations where a patient has requested that the health care provider communicate with the patient in a confidential manner, such as by alternative means or at an alternative location, the health care provider must accommodate that request, if reasonable.

- For example, HHS considers a request to receive mailings from the health care provider in a closed envelope rather than by postcard to be a reasonable request that should be accommodated.
- Similarly, a request to receive mail from the health care provider at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances.

On Use of a Provider's Cell Phone

Q: Does a health care provider's use of a cell phone to exchange phi trigger the HIPAA security rule?

A: Yes.

The HIPAA Security Rule outlines national standards designed to protect individuals' electronic protected health information ("ePHI") that is "created, received, used, or maintained by a covered entity." Unauthorized disclosure of PHI is a risk because mobile devices store data on the device itself in one of two ways: (a) within the computer's "onboard memory"; or, (b) within the SIM card or memory chip. Thus, mobile devices used to exchange ePHI retain a record of that data on the device.

The use of mobile devices to access ePHI raises several risks for health care providers:

- **Authentication** – Mobile device users do not tend to enter passwords or provide biometric identification to access information stored on the mobile device. The lack of authentication on mobile devices presents a risk that any user of the device could access ePHI stored on the device.
- **Encryption** – Typically, data stored on personal mobile devices is not encrypted. Thus, ePHI stored on a mobile device could be retrieved and shared by anyone with access to the mobile device.
- **Wi-Fi Connection** – Mobile devices that use public Wi-Fi or unsecure cellular networks to send and receive information risk exposing ePHI. Unless mobile device users connect to a secure website to transmit data or connect using a VPN ("virtual private networking"), which encrypts data to and from the mobile device, there is a risk ePHI could be compromised.

The HIPAA Security Rule allows health care providers to communicate electronically with patients, such as through email, but the law requires covered entities to "apply reasonable safeguards when doing so." Importantly, the Security Rule "requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

Administrative Safeguards: Administrative safeguards "provide management, accountability, and oversight structure for covered entities to ensure proper safeguards and policies and procedures are in place" to protect ePHI.

Administrative safeguards include, but are not limited to, the following:

- Conducting periodic risk assessments of mobile device use, including an assessment of whether personal mobile devices are being used to exchange ePHI and whether proper authentication, encryption, and physical protections are in place to secure the exchange of ePHI;
- Establishing an electronic process to ensure the ePHI is not destroyed or altered by an unauthorized third party;

- Establishing processes and procedures to appropriately protect ePHI in a mobile device environment, including establishing encryption and security breach protocols for mobile device use, among others; and
- Training clinicians on the processes and procedures to use when using mobile devices to access ePHI and educating clinicians on the risks of data breaches, HIPAA violations, and fines.

Physical Safeguards: It is important to provide physical safeguards to protect ePHI stored on and exchanged by mobile devices.

Typical steps health care providers take to safeguard mobile devices include:

- Keeping an inventory of personal mobile devices used by healthcare professionals to access and transmit ePHI;
- Storing mobile devices in locked offices or lockers;
- Installing radio frequency identification ("RFID") tags on mobile devices to help locate a lost or stolen mobile device; and,
- Using remote shutdown tools to prevent data breaches by remotely locking mobile devices.

Technical Safeguards: Technical safeguards are the "automated processes used to protect data and control access to data."

Examples of technical safeguards for mobile devices include, but are not limited to, the following:

- Installing and regularly updating anti-malicious software (also called malware) on mobile devices;
- Installing firewalls where appropriate;
- Applying encryption to ePHI and metadata;
- Installing IT backup capabilities, such as off-site data centers and/or private clouds, to provide redundancy and access to electronic health information;
- Adopting biometric authentication tools to verify the person using the mobile device is authorized to access the ePHI; and,
- Ensuring mobile devices use secure, encrypted Hypertext Transfer Protocol Secure ("HTTP") similar to those used in banking and financial transactions to provide encrypted communication and secure identification of a network web server.

Parts 2 and 3 of this Series will explore more Frequently Asked Questions providers have regarding communicating with patients via telephone and text.

This is a part of our July series: "Rights, Responsibilities, and Regulations." For more insights, click here.

--