

The Risks of Digital Communication

What to know about texts, email, voicemails, and phone calls



At Devoted Medical, we're all about communication — helping you understand your health, answering your questions, and listening when you have concerns. With so many ways to communicate these days, we want to share information in the ways that work best for you.

In addition to mail and in-person visits, we also use different types of patient communication, including **phone calls**, **text messages**, **voicemail**, and **email**.

We do our best to keep messages and conversations safe and confidential across all the ways we communicate with our patients, but digital communication still has risks.

What are the risks of using digital communication with Devoted Medical?

In short, there's a risk that digital communications (like phone calls, texts, emails, or voicemails) could get out to people who weren't supposed to receive them. We try to prevent this, but here are some examples of how it can happen:

- People or companies can accidentally send digital communications to the wrong phone number or email address.
- Someone could send and forward digital communications to people who aren't supposed to see them — including to large groups or email lists. They may be able to change the communications and share versions that aren't accurate.
- Someone could steal copies of digital communications. Even if they've been deleted from a phone or computer, there might be backup copies that could get into the wrong hands.
- If digital communications get into the wrong hands, they could be used for illegal activities. For example, someone might use the information to send fraudulent (fake) claims to Medicare, or to try to trick you into sharing other personal information (like your Social Security number or credit card numbers).

There are also rules that can give other people access to your digital communications in certain situations:

- Employers and service providers may have a right to look at messages sent using their systems — for example, if you use a messaging app to communicate, the app owner might be able to view your information. Or if you use your work email address, your employer may be able to see your emails.
- If you have to go to court, lawyers could ask the judge for access to your digital communications. If the judge says yes, the lawyers could see your digital communications and use them as evidence in a court case.

Are the risks the same for phone calls, texts, emails, and voicemails?

Devoted Medical records all phone calls, so there's a chance that the recording could get into the wrong hands — but we have a good security system, so the risk is lower. For texts, emails, and voicemails (and phone calls *you* record), the risk is higher because there are other ways for the information to get out, like if someone steals your phone or hacks into your email.

What is Protected Health Information (PHI)?

PHI is any personal health information used for your healthcare — like your health conditions, medications, and doctors' names. This is private information and it can be dangerous if it gets into the wrong hands.

How do I know if I gave Devoted Medical permission to share my PHI in texts, emails, or voicemails?

We don't include any PHI in emails, voicemails, or text messages unless you ask us to.

- **For text messages:** You can check the box on the “Devoted Medical General Consent to Care and Treatment” form that says we can include PHI in texts. We'll include small amounts of PHI in text messages to help you manage your care.
- **For emails and voicemails:** If you need PHI sent to your email or left on a voicemail, give us a call.

If you're not sure what permissions you gave us, you can always ask. And if you change your mind, just let us know.

What does Devoted Medical do to protect digital communications?

Like all healthcare providers, we have systems in place to keep your personal information private. These systems are required by law.

We do our best to keep digital communications secure and confidential, like by using encryption (which turns digital communication into code that only people with permission can read) and training our employees on how to keep PHI safe. But because of the risks we discussed above, there's no way for us to guarantee that it will always be safe.

Here's the bottom line.

- Using digital communications comes with risks.
- It's possible that digital communications (like phone calls, texts, emails, or voicemails) could get out to people who weren't supposed to receive them.
- It's important to know this when or if you decide to give us permission to include PHI in texts, emails, or voicemails.
- Whatever you decide, we'll follow your requests and do everything we can to make sure your information stays safe.

Devoted Medical stores Patient Communications electronically in a patient's medical record. Devoted Medical is not liable for disclosures or breaches of confidential information caused by the Patient or any third party. Devoted Medical is not liable for improper disclosure of confidential information unless caused by Devoted Medical's intentional misconduct. Y0142_23D606_C