GUIDE

How to Respond to Patient Reviews in a HIPAA-Compliant Way

Reputation

Introduction

Reviews are essential to a patient's journey to receiving healthcare. According to a recently conducted Reputation survey of consumers, 86% of patients say they read online reviews, and 60% read at least five reviews when researching providers.

It's important that healthcare organizations and providers ask for reviews and respond to them. Reviews are the currency of reputation and low review volume can create a disadvantage.

However, it is essential that all healthcare organizations and providers manage reviews in a HIPAA-compliant way. After all, exposing protected health information (PHI) can leave your organization vulnerable to serious financial, legal, security, and reputational fall-out.

How can you be sure your organization is responding to online reviews in a HIPAA-compliant way?

86%

of patients say they read online reviews when researching providers.

2023 Healthcare Trends

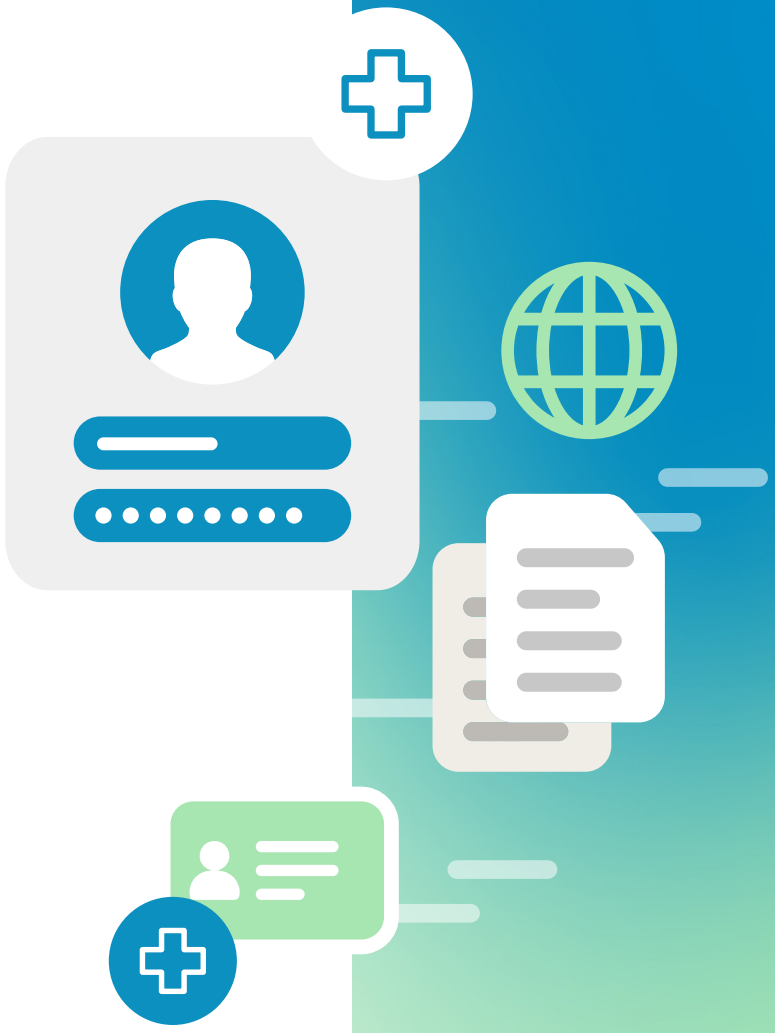
1 PHI Is More than Medical History

Firs off, it's important to understand what protected health information (PHI) is.

PHI is any information that can identify a patient during the course of their care – including but not limited to their medical care.

Examples of PHI include name, date of birth, address, phone number, Social Security Number, treatment and diagnosis details, and health care plan information.

In all, there are 18 agreed-upon separate "identifiers" under HIPAA. Note that the presence of just one identifier classifies the information as PHI. The U.S. Department of Health and Human Services discusses the 18 identifiers on its website, but finding them can be a chore. For a more concise discussion, the HIPPA E-Tool site is a useful resource.

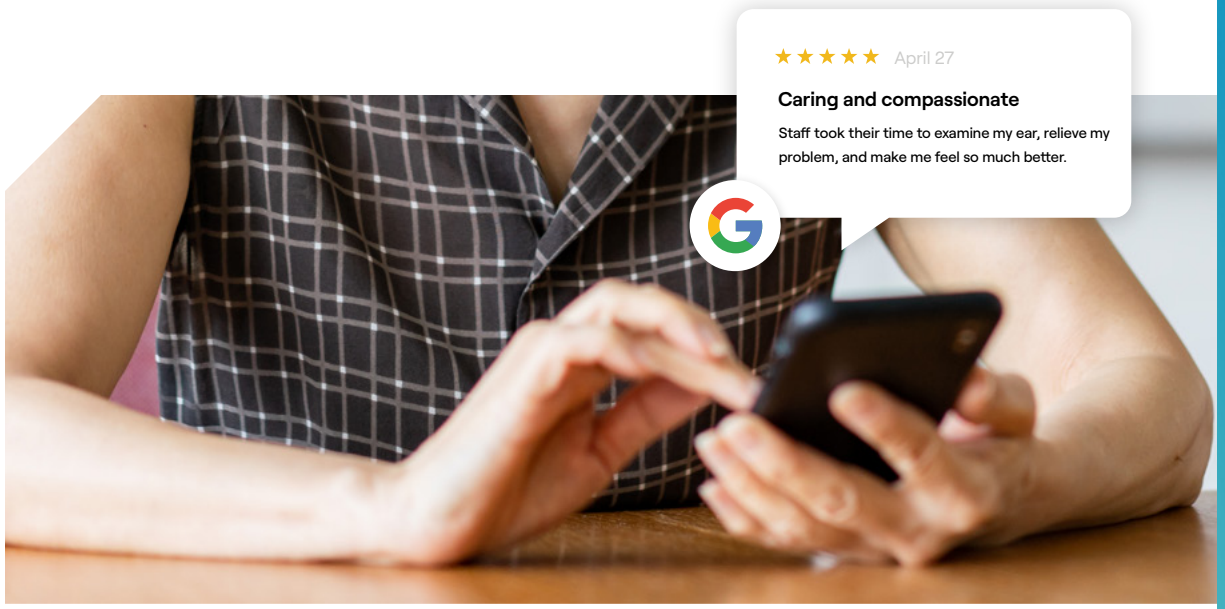


2

Patient PHI in Reviews

The general rule of thumb for avoiding HIPAA violations is this: patients may disclose their own PHI, but a healthcare organization or a provider may not.

If a patient discloses PHI in their review, they have not waived their rights under HIPAA. The responder needs to be very careful not to disclose any PHI in their reply even if a patient has divulged these details. This is where some healthcare organizations and providers run afoul with HIPAA regulations.



Here are two examples:

→ In 2022, a dental practice impermissibly disclosed a patient's PHI on a webpage in response to a negative online review. **The practice suffered a $50,000 HIPAA fine.**

→ **In June 2023, a New Jersey psychiatry practice paid $30,000 to settle a complaint** about impermissible disclosure of protected health information by disclosing this information in response to an online review.

More examples can be found on the U.S. Department of Health and Human Services Website.

But it's not always easy to realize that you've run afoul of HIPAA regulations. In fact, even acknowledging that a patient received care in your reply is a violation.

3 Examples of Good and Bad Responses

Example 1

I had to wait in the waiting room for 45 minutes before seeing the doctor. When I asked someone at the front desk how longer the wait would be, they ignored me. And after all that, my doctor rushed me out the door and didn't listen to me!

Non-HIPAA-compliant response

We're sorry your appointment experience was unsatisfactory. Please let us know how we can make it right.

HIPAA-compliant response

We are always working to improve our patient experience and appreciate your feedback. We strive to deliver the best care possible to all our patients, but we occasionally fall behind schedule because of emergencies. **Because of privacy regulations, we can't discuss any specifics about your comments on this forum. Please contact our Office Manager, Janice, at [email address] if you have any further comments or suggestions.**

Example 2

I am impressed with the outstanding service I received from Doctor Smith for my skin rash! She answered all my questions thoroughly and with compassion.

Non-HIPAA-compliant response

Thank you! We are so pleased that you had a good experience with Dr. Smith. **We are glad that we were able to treat your dermatitis.**

HIPAA-compliant response

Thank you for your feedback! We're always striving to provide the best possible care to our patients, and your review is tremendously helpful.

Example 3

Dr. Jones and their staff were not clear in the instructions they gave me for how I should treat my shin splints, which added stress to my physical pain.

Non-HIPAA-compliant response

We are sorry you did not feel as though our instructions to you were unclear. **Did you mention this to us at the time?** We would have patiently explained next steps.

HIPAA-compliant response

Our goal is always to be extremely clear with our patients. That's why we offer detailed instructions, print take-home instructions, and even text after appointments if necessary. **Because of privacy regulations, we can't discuss any specifics about your comments on this forum.**

What the HIPAA-Compliant Reviews Get Right

In all the above examples, the non-HIPAA-compliant replies sought to be helpful and even encouraging. But all those replies could be costly in more ways than one. They all gave away information that confirmed that the reviewer was a patient. On the other hand, the HIPAA-compliant responses:

- **Remove phrases such as** "your appointment experience" to avoid acknowledging that the reviewer is a patient.
- **Focus on improving the patient experience in general,** rather than specifically addressing the reviewer's complaints.
- **Provides a direct contact method** for the reviewer to share their feedback offline, where it can be addressed more fully.

TAKEAWAY:

Now, it's important to reply to reviews. Doing so is a best practice that shows you listen to feedback.

- It's crucial to follow the "minimum necessary standard" and only disclose the minimum amount of information required for the intended purpose.
- In all the examples of HIPAA-compliant replies, they are short and, while professional and courteous, not personal.

4 General Tips

What are some reliable ways to avoid landing in HIPAA hot water? Here are some good rules of thumb.

1. **Never respond with a patient's personal information.** As noted, here is resource with examples of the 18 identifiers to avoid.
2. **Speak in general terms.** Don't respond directly to a patient. Address the issue being raised by the patient in general terms.
3. **Don't respond personally.** Even if someone identifies themselves in a review, don't respond to them by name. Demonstrating familiarity could imply knowledge that the reviewer is a patient.
4. **Discuss your practice's policies and goals to reinforce your brand messaging.**
5. **Be brief.** The more you say, the more likely you are going to say the wrong thing.
6. **Explain that you are honoring privacy regulations when necessary.** This is especially important when someone shares a negative review. You don't want to sound callous by sharing a terse reply. Be upfront and explain, "Because of privacy regulations, we can't discuss any specifics about your comments on this forum." Doing so sends a message that you care about patient privacy.

7. **Direct reviewers to a resource for an offline conversation if remedial action is required.**

8. **Be positive; never go on the defensive.** Responding with an explanation will increase the risks that you violate HIPAA regulations, and you'll simply look bad. Be brief. Discuss your commitment to providing great service.

9. **Don't apologize for a bad experience.** This sounds counterintuitive – after all, if a reviewer is upset, won't apologizing defuse the situation? Unfortunately, apologizing for a bad experience confirms that a person did in fact have an experience at your provider's location, which could result in a HIPAA violation. This is where a safe harbor explanation comes into play: "Because of privacy regulations, we can't discuss any specifics about your comments on this forum." And this is also where referring the reviewer to a person can be especially helpful to show compassion without acknowledging the reviewer received service at your location.

10. **Thank reviewers for feedback.** Thanking someone for their feedback is a courtesy that shows you value input. And thanking someone for providing feedback does not mean you're acknowledging that they are a patient.

11. **Don't alter content.** If a review from a patient includes protected health information, you don't need to delete it. However, as noted, don't repeat or disclose additional information in your response, and never acknowledge the reviewer is a past or present patient.

12. **Use templates.** Create approved responses that address various common scenarios. Work with your legal and compliance team to develop 15-20 approved responses to common patient scenarios. Then, load them into your online reputation management platform, so that anyone responsible for responding to patient comments can easily pick a response from a drop-down menu.

13. **Train your team.** Anyone who responds to reviews should receive training first. Document your processes and rules. Make sure new team members understand what and what not to do.

Take the next step to HIPAA compliant review response

You might find it helpful to work with an outside partner to do the heavy lifting of review management. The Reputation healthcare team consists of industry experts and our online reputation management platform that handles all aspects of review management.

Learn more about our expertise on our website.

About Reputation

Reputation is the only platform that manages consumer feedback from acquisition to loyalty. Functioning as a business' eyes and ears in the spaces where customers talk, post, review, and recommend, Reputation analyzes vast amounts of public and private feedback data to uncover predictive insights for companies to act on and improve the customer experience. Backed by Marlin Equity Partners, Bessemer Ventures, and Kleiner Perkins, Reputation turns consumer feedback into fuel to grow businesses around the world.
Visit reputation.com to learn more.

Reputation