The Computer & Internet Lawyer

Volume 42 ▲ Number 1 ▲ January 2025

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Can Healthcare Providers Respond to Online Patient Reviews Without Violating HIPAA?

By Steffie Rosene, Elizabeth S. Warren and Roy Wyman

Current and potential patients are taking to the internet to share opinions and make decisions about healthcare providers. Good reviews can convert prospective healthcare consumers into patients, while bad reviews, particularly if poorly handled, can damage a provider's reputation. Because reviews are inevitable, providers should develop a strategy to curate a strong professional reputation online to attract new patients and maintain existing patients. A critical part of this strategy is developing a plan for responding to both positive and negative reviews without violating patient confidentiality.

Responding to patient reviews is more complicated than responding to a regular consumer's review. For example, if a restaurant patron leaves a scathing review, the restaurant can respond by citing the patron's own boorish behavior and poor tipping. On the other hand, should the patron leave a glowing review, the restaurant can thank the reviewer by name with added context related to their experience, meal, and/or interactions with employees. However, a healthcare provider that responds to a review risks violating the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA).

The authors, attorneys with Bass, Berry & Sims PLC, may be contacted at steffie.rosene@bassberry.com, ewarren@bassberry.com and roy.wyman@bassberry.com, respectively.

HIPAA

HIPAA protects the privacy and security of health information that identifies an individual, which is referred to as Protected Health Information (PHI). HIPAA prohibits covered healthcare providers from sharing any PHI about a person unless an exception applies or the patient signs an authorization. PHI is broadly defined. The term includes not just medical records but also information that simply confirms that a person is or was a patient or has requested healthcare services.

HIPAA applies to patients even in a non-medical context. The fact that an individual leaves an online review, good or bad, does not waive the individual's rights to privacy or the provider's obligations to keep PHI confidential. This can be frustrating for healthcare providers, as it creates a situation where they

cannot defend themselves against damaging patient reviews, and even misinformation, without violating HIPAA.

DISCLOSING PHI IN RESPONSE TO AN ONLINE REVIEW CAN HAVE SERIOUS CONSEQUENCES

If a provider discovers that its employee has wrongly disclosed PHI (such as by posting PHI as part of a response to an online review), the provider must determine whether the incident constitutes a breach under HIPAA and, if so, notify the patient in writing as well as the U.S. Department of Health and Human Services, Office for Civil Rights (OCR), which enforces HIPAA. Patients can also file complaints with OCR when they feel their privacy rights have been violated. Consider the following examples of healthcare providers incurring monetary penalties for violating HIPAA:

- OCR imposed a $50,000 penalty against a dental practice[1] that disclosed a patient's PHI in response to an online review. In response[2] to a patient complaint on the practice's Google page, the dental practice posted anecdotal information about an interaction between the patient and the practice. The patient subsequently filed a complaint with OCR.

- OCR imposed a $10,000 penalty against a healthcare provider[3] for various instances of disclosing PHI on the provider's review page. The healthcare provider also agreed to enter into a Corrective Action Plan, requiring the provider to develop policies and procedures, train its workforce, and report certain events to OCR.

- A plastic surgery provider[4] received a letter from OCR alerting the provider of a complaint filed by a patient's mother alleging that the provider posted the patient's PHI in its response to an online review.

Even if OCR does not enforce monetary penalties against a healthcare provider, an OCR investigation into the issue can still cost a healthcare provider time and money. In addition, an OCR investigation could uncover unrelated HIPAA violations and expose the provider to additional scrutiny.

Even a well-meaning response to a positive review is technically a HIPAA violation if the response confirms or implies the reviewer's status as a patient. Crafting a response to a patient review that acknowledges the sentiments expressed while neither confirming nor denying the reviewer's status as a current or former patient can be a challenge. Not responding to patient reviews, however, also risks creating the perception that the healthcare provider is not interested in rectifying concerns and complaints expressed by reviewers online.

A HEALTHCARE PROVIDER CAN RESPOND TO ONLINE PATIENT REVIEWS WITHOUT VIOLATING HIPAA

Responses should be drafted to generically describe the provider's processes without confirming or denying that the reviewer is or has been a patient and without otherwise disclosing PHI. There are a number of ways to capitalize on patient reviews while minimizing risk of violating HIPAA:

- A healthcare provider can work with legal counsel or its privacy officer to develop a procedure for responding to patient reviews as well as pre-approved responses.

- When in doubt on whether a proposed response would violate HIPAA, a healthcare provider should consult with its legal counsel or privacy officer before posting the response.

- A healthcare provider can train its social media manager (or whoever responds to patient reviews on the healthcare provider's behalf) on HIPAA with a focus on preserving patient confidentiality during online interactions.

- A healthcare provider can use an artificial intelligence (AI) tool that does not have access to PHI and is trained to respond to patient reviews in a HIPAA-compliant manner; any AI vendor should be assessed to make sure that the vendor is monitoring the quality of responses and is willing to stand behind its compliance with HIPAA.

Notes

1. https://www.hhs.gov/sites/default/files/upi-nfd.pdf.
2. https://www.hhs.gov/sites/default/files/upi-npd.pdf.
3. https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https:/www.hhs.gov/sites/default/files/elite-dental-ra-cap.pdf.
4. https://www.documentcloud.org/documents/2843212-North-Valley-Plastic-Surgery.html.