Hashtags and HIPPA: A Guide to Social Media for Healthcare Practices

By Lanchi Bombalier, JD/MPH, PT
Arnall Golden Gregory LLP

For businesses large and small, social media is a powerful tool for connecting with consumers and building a brand. For healthcare practices, however, a single misguided post, blurry photograph, or casual comment on a public platform can lead to a potential violation of the Health Insurance Portability and Accountability Act (HIPAA). The U.S. Department of Health and Human Services' Office for Civil Rights (OCR)-the agency that enforces HIPAA-actively investigates potential violations. These investigations can stem from provider self-reports, patient or competitor complaints, or the agency's own compliance reviews. As a result, a single error on social media can set in motion a series of regulatory enforcement actions, leading to significant financial penalties and reputational harm.

By understanding HIPAA's key risks and taking practical steps, healthcare practices can ensure their social media presence is both effective and compliant. The core of social media HIPAA compliance is protecting patient privacy and all categories of Protected Health Information (PHI). PHI is broadly defined under the HIPAA Privacy Rule to capture most types of individually identifiable health information that can be used to identify a patient, including not-so-obvious subsets of health information. As OCR's enforcement actions have repeatedly shown time and time again, PHI may include photos (even cropped or blurred), appointment dates, locations, and descriptions of unique characteristics (like tattoos or a distinctive assistive device) that could on their own, or collectively, identify a patient. Even if a patient initiates contact on social media or voices "verbal" consent, unless the healthcare practice obtains **a valid, written HIPAA authorization** from the patient, it risks violating HIPAA by posting the patient's PHI on a public platform without a valid, written authorization.

Hotspot #1: Responding to Online Reviews

It's tempting to thank a patient for a glowing review or apologize for a bad one, but even a harmless-sounding public response can be a HIPAA compliance trap. Simply confirming that someone is (or was) a patient is a disclosure of PHI. In a notable 2019 case, OCR investigated a dental practice for impermissibly disclosing patient information in its Yelp review responses. Although patients can share their own PHI, their posts don't give a provider the green light to do the same. That dental practice paid a $10,000 settlement and agreed to two years of monitoring. The best practice is to use a generic, neutral response for all online reviews, without acknowledging patient status, and invite the reviewer to discuss their feedback privately.

Hotspot #2: Patient Photos, Videos, and Testimonials

Sharing patient "success stories," before-and-after photos, or feel-good videos can be compelling marketing tools, but healthcare practices should obtain a specific, HIPAA-compliant written authorization before such items are posted – and under certain circumstances, before such content is captured. The written authorization signed by the patient should be tailored to confirm the type of information to be shared, the purpose, the duration of the posting (e.g., if there is any expiration date), and ideally, the social media platforms to be used.

In April 2025, a healthcare provider paid a settlement of $182,000 and agreed to be monitored for two years after a patient complained about their photo being posted on the provider's social media page as part of a "success story" program. The OCR investigation revealed the provider had disclosed the PHI of 150 individuals in similar posts without first obtaining valid authorizations. Although the provider quickly removed the posts, OCR made it clear that a breach cannot be "fixed" after the fact and also cited the provider for failing to notify the 150 individuals about the impermissible disclosure of their PHI online.

Hotspot #3: Policies, Procedures and Protocols

Every healthcare practice needs to address social media risks, even those without an official social media presence. Risks can come from anyone connected to the practice - employees, patients, vendors, or competitors. All practices should develop and implement a formal social media policy that includes a "takedown" protocol for accidental PHI posts and other follow-up measures to mitigate harm. Since social media operates 24/7, robust employee HIPAA training is essential and should also cover posting, responding to comments, sharing media, and direct messaging. Finally, practices must have technical and procedural safeguards to ensure written authorizations are obtained when needed and to monitor compliance with social media use.

In today's digital era, social media offers immense opportunities for healthcare providers to engage with patients and promote their practice to a wide audience. However, as with all areas of rapid growth in healthcare, practices must take a thoughtful and proactive approach to social media to ensure they reap the benefits without compromising patient privacy and HIPAA compliance.

Contact Lanchi Bombalier, JD/MPH, PT
Email: lanchi.bombalier@agg.com
Office Phone: (404) 873-8520

Lanchi is a partner in the Healthcare practice at Arnall Golden Gregory LLP. She has over 25 years of experience working in the healthcare industry and has distinguished herself as a healthcare lawyer who provides full-service regulatory counsel to providers across the healthcare continuum. Her clients appreciate her deep knowledge and multifaceted experience in the healthcare industry, which is the result of her degrees in law and public health and her prior experience as a practicing physical therapist specializing in traumatic brain injury treatment.

She represents providers before state and federal agencies and is known for her technical acuity and comprehensive understanding of payor and reimbursement issues, Medicare/Medicaid certification, voluntary disclosures, state licensure, and emerging health care models. She counsels providers dealing with government audits (UPIC, SMRC, MAC, TPE) to negotiate the administrative appeals process, including challenging the use of statistical sampling and extrapolation. She also defends providers in actions under the federal False Claims Act and serves as healthcare regulatory counsel in the acquisition, merger, and restructuring of large national healthcare organizations. She actively participates in APTA and previously served as an appointee on APTA's Public Policy and Advocacy Committee and the APTA Private Practice Section's Payment Policy Committee.