

Why Posting Patient Photographs on Social Media Accounts May Violate HIPAA and FTC Advertising Regulations

February 22, 2024

By Michael H. Cohen

Many doctors seek to use patient photos as testimonials for their medical practices. The photos are often before and after pictures to show how a patient looked before the medical care was provided and after the treatments were provided. Photos can also be used along with text to state that the patient recommends a doctor due to the care that was provided. Medical practices and organizations also may want to use patient photos to announce when certain services are available, to promote healthy lifestyles, and to discuss current health issues – and for many other reasons.

Doctors and medical practices that provide plastic surgery, beauty, or anti-aging services are among the practices most likely to want to post patient pictures – but almost any medical practice could promote its practice through patient photos.

Healthcare providers need to understand the ethical requirements and federal and state laws that govern the use of patient photos. For starters, the posting of patient photos must comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and with the Federal Trade Commission's (FTC's) social media rules.

The HIPAA Journal states that medical practices and healthcare organizations do need to comply with HIPAA even though HIPAA was enacted before most social media platforms came into existence. These practices and organizations also need to comply with the FTC rules on advertising.

GOT HIPAA? GET HIPAA? JOYCE EXPLAINS WHY AND HOW

Interview with an expert in healthcare privacy and security, both on the federal side with HIPAA, and the state side, especially California law.

FTC ENFORCES FALSE ADVERTISING RULES AGAINST 'CELL REPAIR' PRODUCTS

In today's video, we discuss the dangers of marketing products without proper legal review—in this case, not just FDA enforcement, but even more significantly, FTC (Federal Trade Commission) [...]

The FTC rules on social media

The Federal Trade Commission Act applies to all types of advertising and marketing including social media. The FTC has the authority to review online and offline advertising. The agency can file warning letters and seek injunctive relief to stop any

improper advertising. In addition, the FTC can seek civil penalties.

Advertising and marketing are considered deceptive if:

- *“A representation, omission, or practice misleads or is likely to mislead the consumer;*
- *A consumer’s interpretation of the representation, omission, or practice is considered reasonable under the circumstances;*
and
- *The misleading representation, omission, or practice is material.”*

FTC REGULATIONS YOU MUST KNOW FOR HEALTHCARE ADVERTISING

Lots of physicians and healthcare companies have had us reviewed their marketing materials, and inevitably, we’ve quickly spotted gaping holes where they’ve left themselves vulnerable to [...]

The HIPAA Social Media Rules?

Covered entities and business associates can use social media to promote their practices and products – provided the HIPAA and FTC requirements are met.

Covered entities are:

- *“Healthcare providers, like doctors, dentists, and pharmacies.*
- *Health plans, like HMOs and employer health plans.*
- *Healthcare clearinghouses, which process health information.”*

Business associates are partners of the covered entities that need access to health information to perform certain services.

HIPAA applies to Protected Health Information (PHI) by “covered entities and business associates.” The PHI must comply with HIPAA’s privacy and security rules.

“Protected health information (PHI) is individually identifiable health information transmitted or maintained in any form or medium by a Covered Entity or its Business Associate. Individually identifiable health information is information, including demographic data that relates to an individual’s physical or mental health or the provision of or payment of health care, which identifies the individual.”

Patient authorization and HIPAA (HIPAA’s privacy rules)

Any PHI that is disclosed requires the individual consent of the patient. The HIPAA authorization rules can be found in §164.508 of the HIPAA Privacy Rule. Valid authorizations must include the following core elements:

- *“A meaningful description of the information to be used or disclosed*
- *A meaningful description of the purpose of the use or disclosure*
- *An explanation that the information may be further disclosed*
- *The individual’s right to revoke the authorization*
- *An expiration date for the authorization”*

The patient should be informed that the social media post with their PHA may be widely shared, published, and republished.

This means that even if the patient does request a revocation of the authorization, the medical practice/organization may not be able to comply because the PHI has already moved quickly across the various social media platforms.

What steps can medical practices and organizations take to comply with HIPAA?

The consequences for violation of HIPAA's privacy rule can include large fines and even possible imprisonment. Medical practices and medical organizations that use social media should consult with experienced healthcare providers to understand the do's and don'ts of posting medical information (including patient) photos online.

The practice/organization should establish social media policies, train the staff on permissible and impermissible uses, enforce policy violations, and create safeguards to protect against inadvertent disclosures. Access to social media accounts within the medical office should be limited to specific staff members.

A few FAQs about social media postings and HIPAA

The HIPAA Journal provides a few commonly asked questions about social media and HIPAA.

What is one reason that social media increases the risk for HIPAA violations?

Photographs are a large driver of social media content. The staff in medical offices can take someone's picture and load the picture to the Internet almost immediately. The posting of the photograph will likely violate HIPAA unless the medical practice has the patient's consent.

Is the posting of a photograph of a patient a HIPAA violation if the patient's name is not provided?

Generally, the posting of the photograph will be a violation if the patient's identity can be determined from the image. Medical practices should expect that patients can identify themselves in a social media photo. The medical practice should obtain the patient's permission before posting a photograph online.

Do the HIPAA social media rules apply to all accounts or just corporate accounts?

HIPAA applies to business and personal social media accounts. In fact, posting a patient's photo from a corporate account onto a private account will likely violate both HIPAA's privacy rule and security rule.

Practical suggestions for medical practices regarding social media

Medical practices should train their staff about HIPAA's privacy and security requirements, what information constitutes patient health information, and what the consequences will be for violating these requirements.

The medical practice should also establish protocols, with the help of experienced healthcare lawyers, for obtaining permission from patients to use their patient health information. The patients should understand what information is being disclosed, where it's being disclosed, why it's being disclosed, who may see the information, and the other consequences for seeing their photo on social media accounts. The written consent form should be drafted to address the patient's legal rights and ethical concerns.

American Medical Association Guidelines for social media posts

The American Medical Association (AMA) reviewed a case study of a woman who consented to having her images posted on social media. She broke down in tears when she discovered that images of her breast (the doctor performed breast reduction surgery) were posted online. While the doctor emphasized that the images were for educational purposes, the woman complained that the images were not respectful.

The AMA analysis stated that informed consent may not be enough to protect a doctor in the age of social media. The AMA recommended that the plastic surgeon *change "his social media practices for future patients,"* and share his specific plans for

change so the patient could feel *“like she is making a difference and thus ease the tension.”* The AMA stated that there must be:

- (1) Fully informed consent
- (2) A commitment to professional content
- (3) Avoidance of abusing the patient-physician power differential.

The AMA summarized the basic principles for using patient images on social media as follows:

- *“Complying with the Health Insurance Portability and Accountability Act (HIPAA)*
- *Maintenance of separate private and personal social media accounts*
- *Minimal online interactions with patients*
- *Familiarity with hospital policies on social media.*
- *Patient confidentiality must be protected at all times, as HIPAA’s security rule protecting identifiable health information that a provider creates, receives, maintains, or transmits electronically applies to social media as well.”*

This means that the images should be “deidentified” – though some images cannot be completely deidentified. Online communications between the doctor and patient should not be a substitute for the patient-physician relationship. Doctors, such as plastic surgeons, should understand any hospital policies or medical practice policies in addition to the applicable social media laws.

The AMA states that some entities, like the Social Media Task Force of the American Society of Plastic Surgeons (ASPS) are still in the process of developing applicable policies. Both the physician and the patient should understand that many social media viewers are under 25 years of age.

A practical suggestion is to show the patient the pictures that are going to be posted BEFORE the pictures are posted.

HIPAA Violations – Civil and Criminal Penalties

HIPAA violations are classified as follows:

- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Tier 3:** A violation suffered as a direct result of “willful neglect” of HIPAA Rules, in cases where an attempt has been made to correct the violation
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days.

The penalties for HIPAA violations, by tier, are as follows:

- Tier 1: Minimum fine of \$100 per violation up to \$50,000
- Tier 2: Minimum fine of \$1,000 per violation up to \$50,000
- Tier 3: Minimum fine of \$10,000 per violation up to \$50,000

- Tier 4: Minimum fine of \$50,000 per violation

The penalties increase based on an inflationary index.

"If healthcare professionals knowingly obtain or use protected health information for reasons that are not permitted by the HIPAA Privacy Rule, they may be found to be criminally liable for the HIPAA violation under the criminal enforcement provision of the Social Security Act." [Emphasis added].

Doctors and medical practices also need to understand that obtaining consent near the time of the actual procedure is problematic since the patient is focused primarily on their health – patients may not dissent because patients don't want to upset their doctor when he/she is about to perform a medical procedure.

Another concern raised by the AMA is that posting images online may be detrimental to the medical practice in addition to the patient because photos that seem inappropriate may suggest that the plastic surgeon or other type of physician does not respect the physician-patient relationship.

Doctors and medical practices need to understand how HIPAA, the FTC social media rules, and state and local ethics rules govern the posting of photographs on corporate and personal social media sites. At a minimum, health professionals and practices should obtain a proper written consent to post photographs online for marketing purposes, education, and other reasons. The consequences for violating HIPAA, the FTC rules, and doctor-patient confidentiality can be quite severe.

Physicians and medical practices should contact Cohen Healthcare Law Group to discuss the requirements for posting patient photographs on social media accounts. Our experienced healthcare attorneys advise physicians and medical practices about healthcare compliance laws and regulations.

[Book Your Legal Strategy Session Today](#)

Contact our healthcare law and FDA attorneys for legal advice relevant to your healthcare venture.