Whose Photos Are They, Anyway?

An investigation of the complexities of using patient photos.

BY WENDY LEWIS

>> Look at your phone. Are there any patient photos in your camera roll? Maybe it's just a few of your most prized results, or a case that you want to show to a learned colleague at the watercooler, or a patient you need to call from home. Newsflash: These all may constitute HIPAA violations!

Most practitioners would be lying if they said they didn't have some patient photos on their cell phones or tablets. After all, for aesthetic practitioners, your results are your calling card. But the regulations that govern how photographs should be stored and used by healthcare professionals are often misconstrued.

The first thing you need to know, which may seem obvious but bears repeating, is to never disclose protected health information without written patient consent. Period. Therefore, everyone involved in the medical field needs to get up to speed on HIPAA, and the rules for protecting patient PHI (protected health information). This includes administrative staff, medical staff, aestheticians, marketing teams, social media managers, etc. When it comes to photos, this concept may seem counterintuitive to the under 35 set who do not really value their privacy like their parents did. Younger people may be very comfortable (over)sharing in an open forum because that is how they grew up and it seems quite natural. However, for a healthcare practitioner, it can be deadly.

Regrettably, the laws that govern this space for healthcare professionals are a minefield. Lines can get blurry on the topic of best practices for securing patient photos and regulations for how you can use them. For starters, they are not *your* photos, even though you are treating the patient and took the photos and are storing them in the patient's file, whether in an old-fashioned manila envelope or electronic format.

HIPAA & PHI DEFINITIONS

Healthcare providers are required to identify what is called a "Designated Record Set" that defines all documents that create a medical record, including paper and electronic patient records. Therefore, photos need to be identified as part of the designated record set. When obtaining photos, you need to get a signed consent prior to taking the photograph. Make sure you are aware of your state laws, relevant guidance from the Joint Commission or your hospital, and clinic and surgical suite policies, as these may differ.

Not all patient photos contain PHI, but all patients' photos would be considered health information according to the regulations. A patient photo is considered to contain PHI if it has any of the following patient identifiers:

- Any portion of the face (not just the eyes…)
- Tattoos
- Name or Initials
- Birth Date
- Social Security Number

Never disclose protected health information without written patient consent. Lines can get blurry on the topic of best practices for securing patient photos and regulations for how you can use them. Note: they are not your photos, even though you are treating the patient and took the photos and are storing them in the patient's file.

Set policies that preserve privacy, be sure to avoid publicly sharing PHI, obtain appropriate releases, protect images against misuse, and store images properly.

thebottomline

> "Shockingly, some practitioners and their representatives do not even realize that another physician's patient photos are not to be shared."

- Address
- Date of service
- Medical Record Number

For patient photos containing PHI, HIPAA does not require a patient release if the photos are used only for training and teaching. Photographs used in external settings, such as at conferences, lectures, workshops, seminars, or websites, require patient consent to be used. Patient photos that do not contain any identifiers may not always require approval, but you should cover yourself by getting a consent, anyway.

USE OF CELL PHONES, TABLETS, LAPTOPS, AND DIGITAL CAMERAS

All patient photos are required to be stored and secured properly. Repeat: all. This technically means that photos containing PHI (refer to above) need to be deleted from your devices "in a timely manner," which is open to interpretation. Most digital camera memory cards are not encrypted. If your iPhone or iPad stores these images in the cloud and they appear on your other devices, that is a hard no also.

PERMISSION FORMS

Model release forms should be obtained from patients whom you are photographing or videotaping. These forms are required in order to grant permission to use the subject's image in any medium for educational, promotional, advertising, or other purposes. For public events, which could technically include a patient seminar or lecture, releases are not necessarily required but it is recommended that anyone who appears in a photograph that you intend to use should sign a release. Note that for minors, forms must be completed by a parent or guardian to be considered valid.

When capturing images or obtaining other personal information from patients, HIPAA requires medical professionals to obtain permission to use the information or images by completing the HIPAA Authorization form.

Basically, healthcare professionals are expected to get a completed HIPAA Authorization for Use/Disclosure of Information and Consent/Use of Photographs and Audio/Video Images form from patients who disclose health information to you in any form (written, electronic, photographs, videos, reports, x-rays, lab results, and verbal) that you intend to use in communications (news releases, media, website content, brochures, advertisements, social media, videos, presentations, etc.). These forms should be kept in the patient's record and a copy given to them for their own records. For an example, see legalzoom.com/forms/model-release

HIPAA VS. SOCIAL MEDIA

The HIPAA Privacy Rule prohibits the use of PHI on social media networks. That includes any text about specific patients as well as images or videos that could result in a patient being identified. PHI can only be included in social media posts if a patient has given their consent, in writing, to allow their PHI to be used, and only for the purpose specifically listed in the consent form.[1]

COMMON SOCIAL MEDIA HIPAA VIOLATIONS[2]

- Posting of images and videos of patients without written consent
- Posting of gossip about patients
- Posting of any information that could allow an individual to be identified
- Sharing of photographs or images taken inside a healthcare facility in which patients or PHI are visible
- Sharing of photos, videos, or text on social media platforms within a private group

WHAT GOES INTO A ROCK-SOLID PHOTO CONSENT?

According to Patrick O'Brien, Legal Coordinator for the American Med Spa Association, "While there are many variables that go into making a good photo consent form as a guiding principle you want to very clearly spell out your rights, the patient's rights, and the permitted uses for the photos. Did the patient consent to allowing you to use their photos in a Facebook ad campaign or did they only agree to using them in a portfolio that you show to other patients? You want this kind of question to be very clearly covered in your consent forms, so no one is surprised."

It is wise to consult with an attorney and/or direct your questions to your malpractice carrier to make sure you are covering yourself for any situations that may arise. Laws governing the use of patient photos differ between states and fluctuate even more widely from country to country. "At the national level you have patient privacy concerns from HIPAA,

Tips for **Protecting Your Practice**

If you're hoping to come up with a bulletproof strategy for protecting your photos online, you may be sadly disappointed. Basically, anything posted in a public forum is subject to being copied, since the image or content is there for the taking. However, you should make your ownership clear to scare off would-be photo thieves, and to make it harder for anyone to copy or reuse your images.

Try these strategies to show that you are serious and won't stand for your photos being copied:

- Watermarks that are positioned to deter anyone from cropping around them
- Practice logo on post
- Use a branded treatment of photos on social platforms (colors, backgrounds, format)
- Avoid posting high resolution images—low resolution won't copy well
- Review terms of websites you upload any photos to
- Disable right clicks on the image where possible
- Frame your image and include copyright details
- Use sites that will track where your photos end up, such as tineye.com/
- Secure permission to share, repost, or regram any images posted by your patients to your social channels or website

and most states have their own version, as well, which may differ from HIPAA. Then separate from patient concerns for regular privacy, online data, and advertising rules, states such as California have specific advertising rules when you are using a person's likeness for business purposes," said Mr. O'Brien.

It should be noted that the patient basically has the right to revoke their consent for you to use their photos at any time. Mr. O'Brien weighs in, "Whether or not your consent form has a revocation provision it is probably a good idea from a business perspective to promptly honor their request anyway. At the end of the day what is going to hurt your practice more: losing a nice before and after photo or creating a vocal and unhappy former patient who is talking about how terrible you are to anyone who will listen?"

> "Basically, anything posted in a public forum is subject to being copied, since the image or content is there for the taking."

STAYING SAFE

To stay out of legal trouble and avoid misunderstandings with patients, you should have a written policy in place that all staff should read and sign. To be clear, the physician is responsible for the behavior of all staff who may come into contact with patients and their photographs and personal information. It's your name on the door, and if or when patients take legal action, they will be coming for you, not your receptionist or medical assistant.

Dermatologist Todd E. Schlesinger, MD of Dermatology & Laser Center of Charleston, recommends asking for a comprehensive, unlimited media release from your office staff. "It is likely that their images they will end up in many posts or other media outlets as a normal course of business. The release helps to cover any complaints that may arise during or after the termination of their employment. You may wish to have a social media policy in place at your practice that all staff sign so they understand their responsibility to represent your practice online in the way you prefer or not at all."

Mr. O'Brien offers more advice on how to protect your photos online. "Realistically once a photo has been posted online, there isn't a way to keep someone from downloading it. But you can provide some protection to your photos by adding watermarks. You want to use a watermark design that is difficult to remove, crop, or edit out. This won't stop people downloading your photos, but it will make it more difficult for others to steal them and pass them off as their own."

If you do find that your patient photos have been lifted, rather than seek legal action right out of the gate, start by reaching out directly to the owner of the site or social channel to request that the photos be removed. Shockingly, some practitioners and their representatives do not even realize that another physician's patient photos are not to be shared. In many cases, it can be an innocent, albeit stupid, mistake. Photo borrowing may be undertaken by a naïve marketing assistant, a sloppy web developer, or newbie blogger. If you ask nicely, you may be rewarded with an apology and the photos taken down. If a simple request is ineffective, you may have to escalate it to the next level, which can involve lawyers and a protracted battle.

Common Photo Snafus Explained

With Dermatologist David J. Goldberg, MD, JD

You post a patient's facial laser treatment B/As on Instagram and have a signed consent that includes Instagram as a platform that photos can be posted on, but the photos get lifted and show up on another practice's Instagram channel.

Now what?

"Although you may be sued for this, you are not likely to lose such a lawsuit. Having said that, your patient's release for you to use such photos is not a release for the other person to use them."

Your social media manager takes a photo from a patient's Instagram account of her having a laser treatment that tags your channel, and regrams it without specifically asking the patient for permission and getting a sign off.

Now what?

"Such behavior may be in violation of that person's privacy and ownership. The regram should be immediately removed. Instruct your social media manager not to do this going forward."

A patient agrees to let you post her body sculpting B/A photos but asked for them to be cropped so she is not identifiable. Her pics get posted on your Facebook page with a "Forever Ray" tattoo showing, and her boyfriend Ray recognizes her tattoo.

Now what?

"There is already precedent for such a lawsuit (See finance.yahoo.com/news/plastic-surgery-client-sues-clinic-073729793.html). Expect to be sued if your patient can prove that anybody will recognize this as her tattoo."

You post a set of B/A photos of a thread lift procedure on RealSelf®, but the patient signed a consent that did not include RealSelf in the language. Then, her facial photos end up on a PDO thread company's website. She finds out and demands that her photos be taken down from everywhere.

Now what?

"It all depends on the wording of the consent (release). You are not required to describe virtually every form of social media/internet exposure. If a general release is signed by the patient for such purposes, she will have no claim against you."

STAY VIGILANT

Dr. Schlesinger points out that the issues surrounding patient photos are more complex and confusing than ever before in light of social media's meteoric rise and the pressure physicians face to be visible on these channels. "My best advice is to stay vigilant about how your marketing team uses patient photos online and get into the habit of asking for signed consents from everyone to avoid any problems down the road. As physicians, we have to protect ourselves from the trolls online, because we are ultimately responsible for implementing patient privacy regulations. In the near future, technology will catch up with consumers' online behavior and there will be more systems and programs available to police this for busy physicians." ■

For more insider tips for how to deal with patient photos, consider attending 5CC in Barcelona, and visit the Business Session to be held on Saturday, August 31. The session, Patient Photos: Best Practices for Taking, Posting & Protecting Your Images, will feature a panel of doctors and industry on this important topic. To register, visit http://www.5-CC.com

Wendy Lewis is Founder/President of Wendy Lewis & Co. Ltd., a marketing communication and social media boutique in New York City. She is the author of 12 books including Aesthetic Clinic Marketing in the Digital Age. WL@wendylewisco.com

1. https://www.hhs.gov/hipaa/index.html
2. https://www.hipaajournal.com/hipaa-compliance-checklist/