THINK TWICE BEFORE OVERSHARING

New EU regulations on data protection are coming.

BY LAURA STRAUB, EDITOR-IN-CHIEF

Social media are ever-present in our daily lives. We tweet, post, and blog, and we retweet, like, and respond to an exorbitant amount of material. Sometimes we do so without taking a second to think about the nature of our posts—and, sometimes, the lines between personal and professional become blurry.

Take, for instance, the following three scenarios.

SCENARIO NO. 1

After examining the cutest baby in the neonatal intensive care unit for a retinopathy of prematurity screening, a retinal physician in Italy posts a picture of the child on her Facebook wall with no mention of the patient's name.

SCENARIO NO. 2

While visiting a practice in the United Kingdom to observe laser-assisted cataract surgery cases, a cataract surgeon from Germany snaps a selfie in the operating room and posts it on Instagram, not realizing that the patient's information is visible on the computer screen in the background.

SCENARIO NO. 3

A nurse working in a Spanish hospital who helped save the eye of an alleged rapist blogs about the experience, using caution not to mention her employer, the patient, or the victim by name.

These three seemingly innocent scenarios are not so innocent. They are all intrusions on patient privacy that, in fact, can lead to serious repercussions, including the fining or firing of the health care professionals involved, regardless of where those persons live. Patient privacy laws of some type are in effect in every country. In the European Union (EU), the Directive on Data Protection (DDP) prohibits disclosure of any personal details, including health care data, to any foreign entities not meeting the EU's data safeguard guidelines.[1]

But, since the DDP was adopted in 1998, many changes have been made to privacy acts, and many more are coming. The EU's General Data Protection Regulation (GDPR), adopted in April 2016, will go into effect in May 2018 and replace the DDP. This new regulation is an attempt by the European Parliament, the Council of the European Union, and the European Commission to strengthen and unify data protection for individuals within the EU and to address the exporting of personal data outside the EU. Once this regulation is in effect, data protection regulations will be the same throughout the EU, and fines for noncompliance will increase by up to 5%.[3]

Under the GDPR, four basic sanctions can be imposed if an individual is found guilty of noncompliance:[4]

- A written warning for first-time offenders and unintentional noncompliance;
- Regular periodic data protection audits;
- A fine of up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater; and
- A fine of up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

What personal data is protected under the GDPR? According to the European Commission, "personal data is any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."[5]

In today's digital age, one in which oversharing on social media is so commonplace, health care professionals need to be especially careful to uphold patient privacy. In the accompanying article, Michael Sopher, the president and cofounder of Rendia, shares some do's and don'ts that health care professionals should keep in mind when participating in social media. ■

1. Guiliano S. Beyond HIPAA: International health data protection. *Atlantic Net*. May 5, 2014. www.atlantic.net/blog/beyond-hipaa-international-health-data-protection/. Accessed January 31, 2017.
2. Commission proposes reform of data protection rules to increase users' control of their data and to cut costs for businesses [press release]. European Commission. January 25, 2012. http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en. Accessed January 31, 2017.
3. Albrecht JP. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). October 22, 2013. http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf. Accessed January 31, 2017.
4. [no authors listed] Regulation (EU) 2016/679 of the European Parliament and of the Council. Journal of the European Union. April 27, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1. Accessed January 31, 2017.
5. Interinstitutional File: 2012/0011 (COD). Council of the European Union. June 11, 2015. http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf. Accessed January 31, 2017.

THE DO'S AND DON'TS OF PATIENT PRIVACY ON SOCIAL MEDIA

Remembering these five tips could help you to avoid costly mistakes.

By Michael Sopher

Thanks to high-tech devices such as smartphones and tablets, thanks to the Internet, and thanks to social media, we live in an age of constant connection. People can share anything at the press of a button, and, just the same, they can access endless material shared by others.

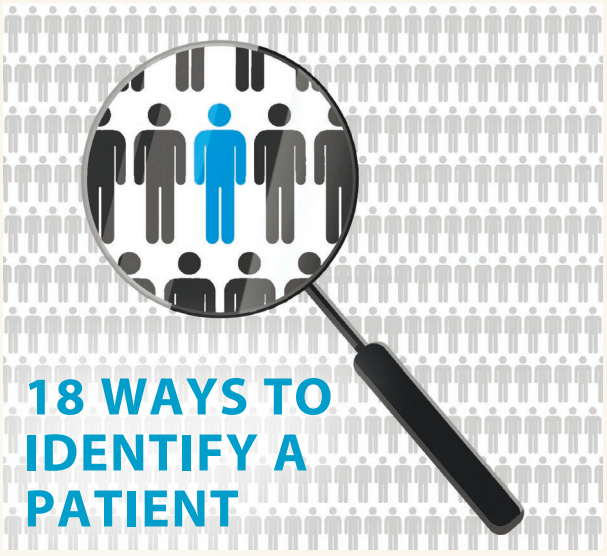
With all this widespread sharing, it is important for physicians to monitor their own use of social media, upholding the security of their patients' protected health information (PHI), and, thereby, saving themselves and their practices from breeches in patient privacy. As much as physicians are aware that they must store and send sensitive PHI securely, sometimes it is inadvertently shared with others.

FIVE EASY TIPS

The truth is, with so many social media platforms available, and with more emerging all the time, it can be daunting to figure out what is acceptable to post and what is not. The five easy tips I offer here are what you need to know about protecting your patients and your practice.

Tip No. 1: Do decode patient identifiers. Most health care professionals know to avoid impermissible use or disclosure that compromises the security or privacy of a patient's PHI. But what, exactly, constitutes PHI? In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) defined PHI as any information that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service.[1] This includes 18 distinct identifiers (see *18 Ways to Identify a Patient*).[2] The bottom line is that, if the patient can be identified in something you are considering posting, do not post it.

One common example of a HIPAA violation is when a staff member shares his or her excitement about treating a professional athlete or well-known TV personality on social media. According to a blog by the compliance consultant organization Healthcare Compliance Pros, "posting verbal 'gossip' about a patient to unauthorized individuals, even if



18 WAYS TO IDENTIFY A PATIENT

1. Patient's name
2. Any geographical subdivision smaller than a state (eg, street address, city, county, precinct, zip code) and their equivalent geocodes
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voice prints
17. Full face photographic images and comparable images
18. Any other unique identifying number, characteristic, or code (not including the unique code assigned by the investigator to code the data)

Adapted from: HIPAA PHI: List of 18 identifiers and definition of PHI. Berkeley Human Research Program Protection. http://cphs.berkeley.edu/hipaa/hipaa18.html. Accessed January 31, 2017.

the name is not disclosed" is enough to get medical practices into trouble with HIPAA laws.[2]

Tip No. 2: Do keep your personal social media accounts and those of your employees separate from the practice's accounts. Creating a personal social media account using a pseudonym that only friends and family know can help to keep a health care professional's patients from searching for him or her and sending friend requests. Furthermore, it is important to avoid connecting with patients on personal or practice accounts and to advise your employees to do the same.

Tip No. 3: Do speak up when patients are asking for medical advice online. Crowdsourcing your medical care on social media is never a good idea, but, unfortunately, people do it all the time.[3] Instead of making comments that are specific to one patient, speak to patients on social media collectively and offer general advice only. One tactic is to share a patient education video. If an unknown patient reaches out and asks a personal health question on social media, however, the most appropriate course of action is to take the conversation offline. In these situations, use a standard response that asks the patient to call the office and make an appointment, or, if in an emergency, to call his or her local emergency number or go to the emergency room of a hospital.

Tip No. 4: Don't make the mistake of thinking that posts are private or that they disappear once they have been deleted. Search engines and screenshots can make even deleted posts permanent. As a general rule, do not post anything you would not be comfortable sharing in public.

Tip No. 5: Don't overlook staff training. Educate the staff in your practice on social media security, and have a solid social media policy in place. In the policy, social media should be defined and specific sites mentioned, and the type of information employees are and are not allowed to post on both the practice's pages and on their personal pages should be covered.

1. HIPAA PHI: List of 18 identifiers and definition of PHI. Berkeley Human Research Program Protection. http://cphs.berkeley.edu/hipaa/hipaa18.html. Accessed January 31, 2017.
2. Posting with caution: The Do's and Don'ts of social media and HIPAA compliance. Healthcare Compliance Pros. April 7, 2015. https://www.healthcarecompliancepros.com/blog/posting-with-caution-the-dos-and-donts-of-social-media-and-hipaa-compliance-2/. Accessed January 31, 2017.
3. McCullar E. A warning against crowdsourcing your medical care on social media. KevinMD.com. April 18, 2016. http://www.kevinmd.com/blog/2016/04/a-warning-against-crowdsourcing-your-medical-care-on-social-media.html. Accessed January 31, 2017.

Michael Sopher
- President and Cofounder, Rendia
- michael@rendia.com