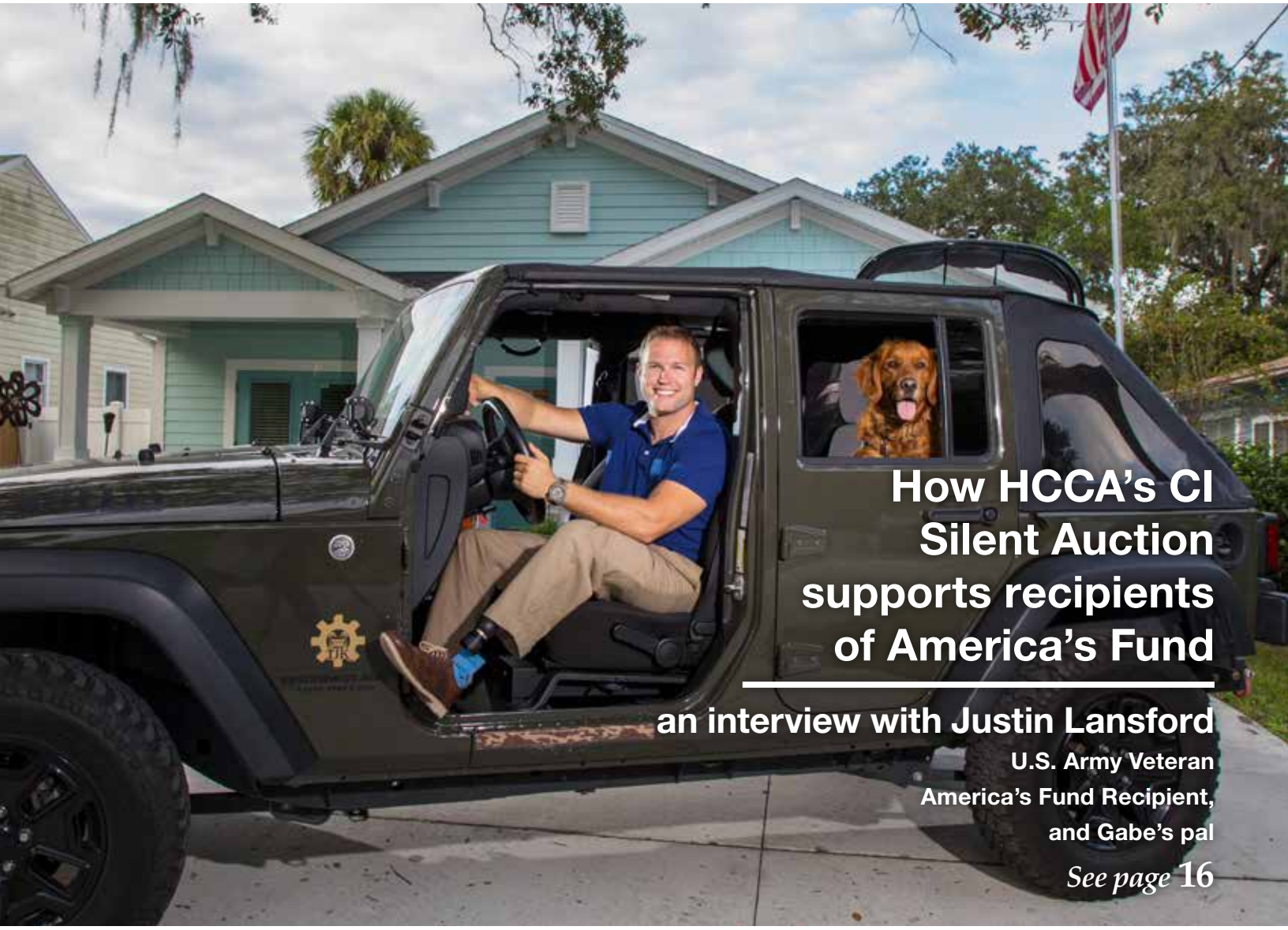
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

December 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



How HCCA's CI Silent Auction supports recipients of America's Fund

an interview with Justin Lansford

U.S. Army Veteran
America's Fund Recipient,
and Gabe's pal

See page 16

22

How to respond when ransomware catches you off guard

Theresamarie Mantese, Jordan Segal, and Paul Mantese

28

Embracing patient payment preferences, Part 2: Records and documentation requirements

Rozanne M. Andersen

35

Helping new physicians learn to improve billing and coding

Duncan Norton

39

Addressing compliance issues in reimbursement and licensing for telemedicine

Max Reiboldt

> America's Fund is by far the greatest wounded veteran-based nonprofit out there...they're also one of (if not the most) efficient—97 cents on the dollar goes directly to their programs.

See page 18

ARTICLES

46 [CEU] **Physicians, social media, and "BYOD": HIPAA risks and compliance**
by Daniel F. Shay
A security risk assessment and social media policy are essential before you let providers and employees bring their smartphones, tablets, and other devices to work.

53 **Billing compliance for oncology clinical trials in a community cancer center**
by Christina Head and Alaina Underberg
Ensuring timely and accurate billing and record keeping for clinical trials requires coordinating with staff across multiple areas of a medical facility.

56 [CEU] **Ethics in research**
by Juanita Rendon
The increasing scope of international clinical research puts a spotlight on the importance of ethical behavior, not just in the United States, but throughout the world.

61 **Act now, LTC facilities: Phase 2 is upon us**
by Dayna C. LaPlante and Brian D. Bewley
Recommended steps for long-term care facilities to ensure they are ready in eleven areas for the November 28, 2017 deadline for Phase 2 compliance.

66 **Certifying Medicaid program data, Part 1: What it entails and why you do it**
by Jay Davis
To combat fraud, CMS published a final rule that makes Medicare managed care entities responsible for the accuracy, completeness, and truthfulness of data submitted.

70 **Reframing compliance training by a well-formed incentives plan**
by Misty Bridwell
Promote enthusiasm around compliance training with the constructive use of creative communication, rewards and recognition, and elevated status.

72 **Santa Claus: The compliance interview**
by Adam Turteltaub
A light-hearted look at the compliance program at the North Pole.

Compliance TODAY

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance Today*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

VOLUME 19, ISSUE 12

by Daniel F. Shay

Physicians, social media, and "BYOD": HIPAA risks and compliance

» Social media and "bring your own device" (BYOD) require the establishment of effective policies and procedures, including employee training.

» A security risk assessment that takes social media and BYOD into account is essential to ensuring HIPAA compliance.

» Policies and procedures drafted without having conducted a security risk assessment are insufficient to meet HIPAA requirements.

» Effective HIPAA compliance training for social media should include examples of how PHI can be incorrectly shared and spread.f

» BYOD policies should consider whether to limit the type of devices that may be used and whether to require the use of specific apps.

Daniel F. Shay *(dshay@gosfield.com) is an Attorney with the Alice G. Gosfield & Associates PC law firm in Philadelphia, PA.*

In just short of ten years, adult usage of social media in the United States has exploded, increasing from a mere 8% in 2005 to 69% by 2016.[1] Given the prevalence of social media, it is no surprise that healthcare providers have seized upon its usefulness in communicating with their patients and potentially delivering more responsive care. At the same time, smartphones, tablets, and personal digital assistants (PDAs) are ubiquitous, and offer potential cost-saving to those physician practices that permit their physicians to utilize their own devices for work purposes, a practice known as "bring your own device" (BYOD). However, using social media and personal devices for work purposes brings with it risks, especially with respect to Health Insurance Portability and Accountability Act (HIPAA) compliance.

Shay

Background information

Social media's functionality makes it naturally attractive to physician practices as a method of communicating with patients.[2] Most social media platforms permit the sharing of content such as images, video, text, links to other websites, etc. Social media platforms also may offer a range of demographic data on those user accounts to which the practice connects. In addition, social media creates a kind of "six degrees of separation" effect. If an individual connects to a friend, depending on the individual's account settings, other accounts connected to the individual's account may be able to see and connect to that friend. Likewise, the friend may be able to see information posted by those other accounts, without ever having connected to them. All of this means that a physician practice's communications may be able to reach beyond just the individuals to whom the physician

practice connects on social media, and may allow the practice to grow its patient base and online influence.

With respect to BYOD policies, the underlying theory is that such a policy allows the company to reduce overhead by shifting the expense of maintaining such devices to the company's workforce. Employees often prefer to carry around only a single device. In addition, while a company might seek to limit the functionality of its own devices, it does not necessarily need the same degree of control over the functionality of the employee's device.

HIPAA concerns

Social media provides several ways in which physician practices may run afoul of the HIPAA regulations. Although most physician practices have effectively taught their physicians basic HIPAA compliance principles relating to the HIPAA Privacy Rule,[3] they may not have effectively educated their staff with respect to both HIPAA's Security Rule and Breach Notification Rule.[4] The HIPAA Security Rule in particular represents a blind spot for physician practices, with many physicians believing, "Our EHR is certified. Isn't that enough?" It is not.

Although the full range and implications of both the Security and Breach Notification Rules' requirements are beyond the scope of this article, some basics must be conveyed to understand how the Security Rule relates to social media use and BYOD policies. First, the Security Rule applies to protected health information (PHI) contained in electronic form (ePHI).[5] All PHI that is stored on computer systems, communicated by electronic messages, or otherwise rendered into an electronic format is considered ePHI. In addition, the Breach Notification Rule specifically applies to "unsecured PHI" (uPHI).[6] This generally means PHI that has not been encrypted in accordance with HIPAA standards. When uPHI is improperly disclosed, it requires the disclosing entity to determine whether a breach has occurred. By contrast, secured PHI (i.e., PHI that has been appropriately encrypted) is not subject to the Breach Notification Rule. The same also applies to text messages, unless those texts are sent through appropriately encrypted secure texting applications; most text applications that come standard on smartphones do not use this level of encryption.

Within the social media context, all posts or messages sent through social media are ePHI, and are almost certainly also uPHI; social media posts are not generally encrypted at all. As a result, an improper disclosure of PHI on a social media network will necessarily require an analysis under the Breach Notification Rule, meaning the practice will have to determine whether there is a low probability that the PHI was compromised, based on an analysis of the following factors:

- the nature and extent of the PHI involved, including the type of information contained in the PHI;
- the unauthorized person who used the PHI or to whom disclosure was made;
- whether PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.[7]

Employees may post PHI on social media both intentionally and unintentionally. For example, in our practice, we represented a physician clinic where a front-desk staff member was given an apple from a patient's orchard. She was so pleased that she posted a photograph of the apple to a social media account, with a comment about how she loved the patients at her job. Unfortunately, the apple itself was sitting atop a charge sheet for the day, which listed partial names, telephone numbers, and medical ID numbers for

patients, the disclosure of which required the client to conduct a breach analysis.

Other scenarios in which a physician or staff member might disclose PHI could involve colleagues who are friends on a social media network communicating through the network about a particular patient. In some instances, physicians have intentionally posted information about patients online. For example, Northwestern University Medical Center found itself sued for the actions of a physician who posted photographs of an intoxicated emergency room patient online.[8]

Within the BYOD context, if a physician practice allows its clinicians to use their own devices, improper disclosures could be made when one clinician, for example, takes a photograph of a patient's signs and symptoms and sends them by unsecured text to another physician for a consultation. This may not be an improper disclosure in and of itself, depending on the physician's settings on their smartphone, but the photo could end up incorporated into the physician's own "camera roll," with it sitting among family vacation photos. If those photos are then backed up to a cloud server for the physician's phone (e.g., the Apple iCloud, which is not secure for HIPAA purposes), then the physician and practice would be in violation, because Apple will not sign a business associate agreement with either the physician or the practice to store the photos on either's behalf.

The adoption of BYOD policies also necessarily raises the risk of loss or theft of devices that either grant access to ePHI or store ePHI on them. This issue has served as the basis for multiple multi-million dollar settlements with the Department of Health and Human Services' Office for Civil Rights (OCR), the government entity responsible for enforcing HIPAA.[9,10,11] Each case involved the loss or theft of an unencrypted laptop or thumb drive containing ePHI.

These settlements also raise an additional consideration under the HIPAA Security Rule. The Security Rule requires that covered entities conduct a security risk assessment (SRA). The SRA has been described by the OCR as a "foundational" document. The results of the SRA help a covered entity to determine where its security is deficient, which in turn informs how the covered entity will develop appropriate policies and procedures to address the other requirements of the Security Rule. Without an SRA, any policies and procedures developed by the covered entity will likely be viewed as insufficient to satisfy HIPAA's requirements.

The adoption of BYOD policies also necessarily raises the risk of loss or theft of devices that either grant access to ePHI or store ePHI on them.

In several of the settlements described above, the OCR found that the covered entity in question either had not conducted an SRA, or had conducted an ineffective one (e.g., a SRA conducted many years ago, addressing security considerations which have subsequently changed). The SRA does not need to be conducted on a regular basis, but must be conducted when the security considerations for the covered entity change. For example, if new computers are purchased, a new electronic health record (EHR) system is implemented, or even if the layout of desks within the practice is altered (e.g., so that passersby might be able to view computer monitors), it may require revisiting and updating the SRA.

If the practice intends to implement a BYOD policy, it will need to revise its SRA

to account for the new policy. Similarly, if the practice intends to create a social media presence for itself, it will need to address this under the SRA. Naturally, this will lead to the development of policies and procedures to address the risks posed by both social media usage and BYOD.

Practical guidance

As a general rule, physician practices should (after having conducted an appropriate SRA) develop clear, firm policies and procedures addressing the use of electronic media and personal devices both on and off the job, as well as how social media may be used both on the practice's behalf and in the employee's private usage. If the practice intends to have an official social media presence, it is advisable to limit the number of people authorized to post online on the practice's behalf. In addition to limiting the possibility of improper HIPAA disclosures through the practice's own social media accounts, having specific social media duties assigned to a limited number of staff will help the practice to maintain a uniform message when communicating online.

When training employees on HIPAA compliance, consider using a sample post with information that looks like PHI, but obviously is not actual PHI.

With respect to personal usage of social media by employees, an absolute ban on use during work hours is unlikely to be enforceable. Even without a BYOD policy, employees will still be able to use smartphones to post on social media while in the bathroom or on lunch break. Instead, a better approach is to educate employees on what constitutes improper use of social media and how quickly improper postings can spread.

When training employees on HIPAA compliance, consider using a sample post with information that looks like PHI, but obviously is not *actual* PHI. This could take the form of a photograph where employees try to find where the PHI is in the image (or if there even is any), or a post containing nothing but text. Demonstrating how the "six degrees of separation" nature of social media can lead to the widespread dissemination of information may provide a sobering reminder of the risks of discussing patient information online.

With respect to BYOD issues, it is essential to establish clear policies regarding the use of such devices. The practice may want to specify which apps may be used for work functions, which types of devices may be used, and which security features must be enabled to use a personal device for work.

Restricting the types of devices may help the practice's IT team to create uniform guidelines for the technical aspects of ensuring security. In addition, depending on the practice's technical infrastructure, it may want to require that employees use specific apps that store no data on the device itself, and instead back up to a cloud account that the practice itself controls. Lastly, the practice may want to investigate whether it can install remote "kill switch" technology on the BYOD device so that it may be completely locked or wiped of all data in the event that it is lost or stolen.

Whatever a practice decides to do, however, it should be certain that it has addressed the new security considerations in its SRA, and developed its policies and procedures in response to what the SRA itself has uncovered. Simply adopting policies and procedures that sound like a good idea, or adopting a compliance program from a "kit" provided by a

specialty society or consultant without tailoring it to the practice's own realities, will not satisfy the Security Rule requirements.

Conclusion

It is unlikely that social media usage will abate anytime soon, nor will people stop using smartphones or tablets. Patients find the use of such devices increasingly convenient and want to be better connected with the healthcare providers who treat them. Physician practices must decide how to cope with these new realities. Those practices that want to ensure compliance with HIPAA's requirements will need to carefully consider how to develop effective policies and procedures to govern the use of social media and to address the use of personal devices for work purposes. Knowledgeable healthcare counsel can help with this.

1. Pew Research Center, Internet & Technology: Social Media Fact Sheet. Available at http://pewrsr.ch/2z2Jaus
2. Daniel Shay: "Physicians and Social Media: Untangling the Web" *Health Law Handbook*, 2014 Ed., pp.34-69.
3. 45 CFR § 164.500, et seq. (Privacy of Individually Identifiable Health Information)
4. 45 CFR §§ 164.300, et seq.(Security Standards for the Protection of ePHI) and 164.400 (Notification in the Case of Breach of Unsecured PHI). Available at http://bit.ly/2i00Hs8
5. 45 CFR § 160.103 (Definitions)
6. 45 CFR § 164.402 (Definitions)
7. Idem.
8. Alana Abramson: "Chicago Doctor Accused of Posting Photos of Intoxicated Patient" *Good Morning America*, August 20, 2013. Available at http://abcn.ws/2zJorc6.
9. HHS.gov: "Massachusetts provider settles HIPAA case for $1.5 million" (Mass. Eye and Ear Infirmary). September 17, 2012. http://bit.ly/2yDENW9
10. HHS.gov: "Lack of timely action risks security and costs money" (Children's Medical Center of Dallas, $3.2 million settlement). February 1, 2017. http://bit.ly/2zJn7WC;
11. HHS.gov: "$2.5 million settlement shows that not understanding HIPAA requirements creates risk" (CardioNet settlement) April 24, 2017. Available at http://bit.ly/2yEt6hS,