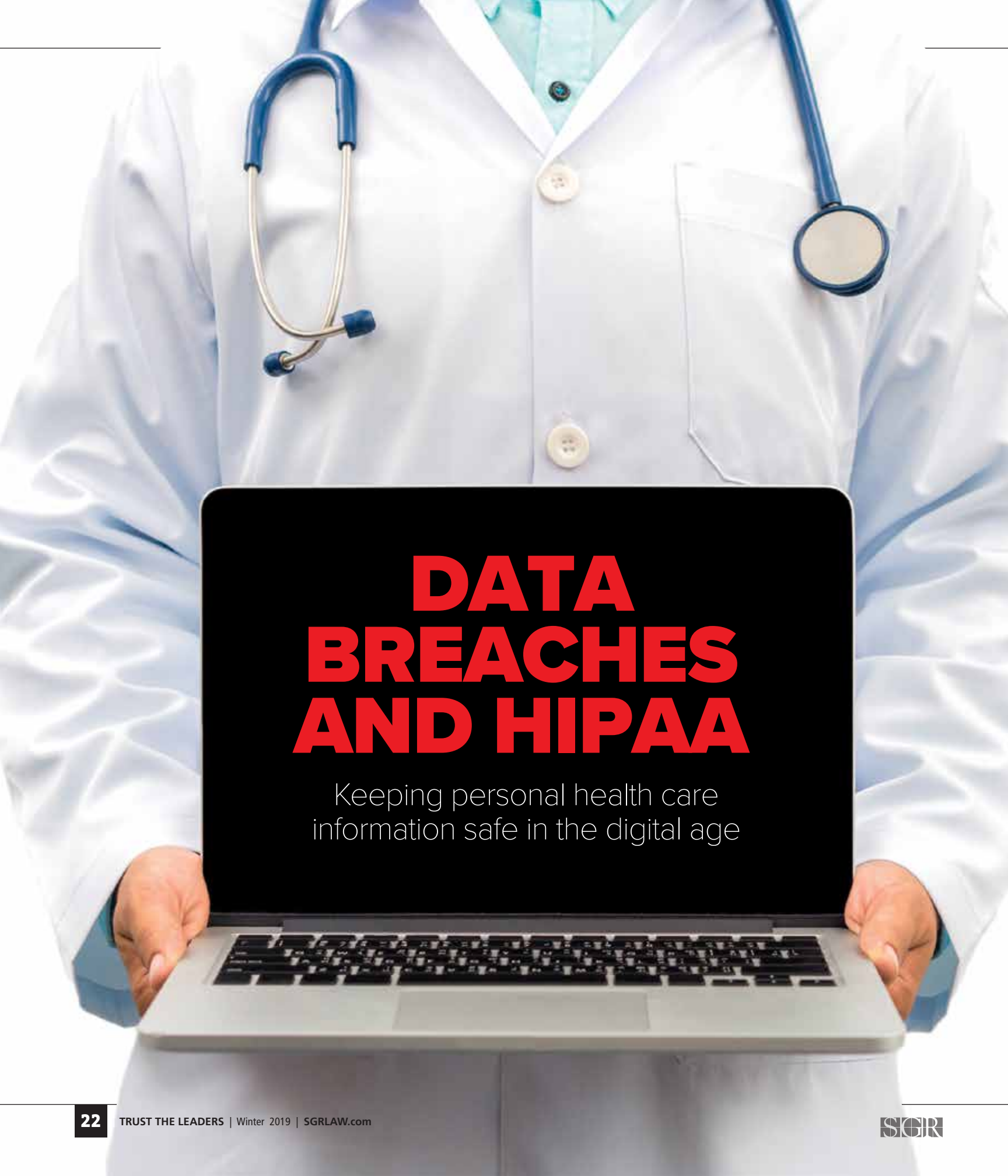

DATA BREACHES AND HIPAA

Keeping personal health care information safe in the digital age

BY LAURA ANDREW

IF YOU HAVE ever lost your laptop, you have something in common with one of the most frequent violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, among other provisions, protects the privacy and security of certain individually identifiable health information considered to be "protected health information," or PHI. Organizations that have access to, create or transport such information are "covered entities." Covered entities include hospitals, physicians, health insurance companies and employer group health plans. These covered entities are subject to stringent regulations and requirements related to the privacy and security of PHI. They are only allowed to use PHI in specified ways. Companies that provide services to these covered entities, called "business associates," are also subject to these requirements. The United States Department of Health and Human Services (HHS) Office of Civil Rights (OCR) is charged with overseeing compliance with and enforcing the HIPAA Privacy Rule and Security Rule.

OCR has been very active in auditing and assessing penalties and fines to covered entities and business associates that fail to safeguard PHI. It investigates complaints that have been filed with it and conducts compliance audits to determine if covered entities are in compliance with the HIPAA Privacy and Security rules. As noted in its report of July 31, 2018, since HIPAA's Privacy and Security rules were first effective in April 2003, OCR has received over 186,450 HIPAA complaints and has initiated over 900 compliance reviews. According to OCR, it has resolved almost 96 percent of these cases.[1]

HIPAA sanctions in 2018

In 2018, OCR imposed two major HIPAA penalties and won a case before an HHS administrative law judge (ALJ). The three outcomes amount to an estimated $7.9 million in fines. In 2017, OCR imposed 10 penalties totaling $19.4 million, and in 2016, the office instituted actions resulting in 13 penalties totaling $23.5 million.[2]

On February 1, 2018, OCR announced the first HIPAA settlement of the year, with Fresenius Medical Care North America (FMCNA), a nationwide dialysis provider.[3] In this settlement, FMCNA agreed to pay $3.5 million and adopt an extensive corrective action plan to settle potential HIPAA violations based on five data breaches that occurred at separate FMCNA-owned entities over a five-month period in 2012.[4] These breaches included two desktop computers stolen during a break-in at one company facility, with another three desktops and one laptop stolen from another company location. All of these devices contained PHI not protected by password or encryption. At another FMCNA location, an unencrypted USB drive was stolen from a company employee's car parked at the company's work location. A similar theft happened at an employee's home, where an unencrypted laptop and its computer bag (which contained the employee's list of passwords) were stolen from the employee's car. Lastly, a hard drive ▶

containing unprotected PHI was reported missing from another office location. These data breaches impacted 521 individuals. "The number of breaches, involving a variety of locations and vulnerabilities, highlights why there is no substitute for an enterprise-wide risk analysis for a covered entity," said OCR Director Roger Severino. "Covered entities must take a thorough look at their internal policies and procedures to ensure they are protecting their patients' health information in accordance with the law." OCR found that FMCNA "failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of" its electronic PHI, or "ePHI."[5] A corrective action plan requires FMCNA to complete a risk analysis and risk management plan, revise policies and procedures, develop an encryption report, and provide employee education on policies and procedure.[6]

Failing to properly secure and handle PHI was at the root of the second large settlement of 2018. An anonymous tipster alleged that an individual took papers out of an unlocked dumpster outside of a company location and attempted to sell the paper as recyclable material to a paper shredding office. The only problem was that the company that originally disposed of the papers stored and delivered medical information.

The settlement of $100,000 between OCR and Filefax, Inc. resulted from an OCR audit based on this anonymous tip. The investigation concluded that "Filefax impermissibly disclosed the PHI of 2,150 individuals by leaving the PHI in an unlocked truck in the Filefax parking lot, or by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unsecured outside the Filefax facility."[7] Filefax dissolved during the course of the investigation, but the receiver appointed to liquidate the assets of Filefax agreed to pay the $100,000 and properly

An anonymous tipster alleged that an individual took papers out of an unlocked dumpster and attempted to sell them as recyclable material to a shredding office.

store and dispose of the remaining medical records in a HIPAA-compliant manner.[8] This is a good reminder that HIPAA responsibility does not end when a company goes out of business. The company must still dispose of or protect the PHI in accordance with HIPAA's requirements.

Lastly, in June of 2018, an HHS ALJ ruled that MD Anderson Cancer Center violated HIPAA and granted summary judgment to OCR on all issues, requiring MD Anderson to pay $4,383,000 in civil money penalties.[9] In this case, unencrypted laptops and thumb drives were stolen or lost. While MD Anderson's HIPAA policy required that devices containing ePHI must be encrypted, it was slow to implement its policy, and did not begin mass encryption until 2012, even though its annual risk analysis identified failure to encrypt as a high risk concern. In April of 2012, a laptop was stolen from the home of an MD Anderson employee who had purchased

the laptop using the organization's funds. This employee was "teleworking" and the computer was not encrypted or password protected. Three months later, in July of 2012, another MD Anderson employee lost a USB thumb drive while riding in one of the Center's shuttle buses. Again, as with the other situations cited, the thumb drive was not encrypted and contained ePHI of more than 2,200 individuals. Then, in November of 2013, a visiting researcher lost an unencrypted thumb drive containing ePHI of about 3,600 patients.[10]

While stating that HIPAA gives flexibility to covered entities in how to protect their ePHI, the judge held that the protection must be effective. It does not matter whether a laptop or thumb drive is lost or stolen; the violation is the failure to protect ePHI from disclosure, including from theft. The ALJ held that the penalties assessed – $1.5 million per year – were modest given the gravity of MD Anderson's noncompliance. The takeaway from this case is that, once a strategy for protecting PHI and ePHI is determined, it must be implemented with diligence or the organization risks an OCR audit or investigation and possibly substantial penalties.

Conclusion

The examples cited above reinforce the importance of vigilance regarding a company's HIPAA policies and procedures. Complacency with the handling of PHI and ePHI can lead a company's employees to compliance failure. Neglecting to implement passwords or encryption on portable devices, then losing such devices, is just one example of the carelessness that can lead to HIPAA breaches. Companies can protect themselves and their PHI and ePHI by instituting self-audits and providing refresher training to employees to reduce the likelihood of such breaches.

Laura Andrew is a partner in SGR's Executive Compensation and Employee Benefits and Health Care practices in Jacksonville. She concentrates her practice in health care related matters, including compliance with HIPAA and federal and state health care anti-fraud laws. **landrew@sgrlaw.com**.

Endnotes

1. U.S. Dep't of Health & Human Servs., Health Information Privacy, Enforcement Highlights as of May 31, 2018 (last updated June 13, 2018), www.hhs.gov/hipaa/for-professionals/complianceenforcement/data/enforcement-highlights/index.html.
2. *Id.*
3. www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlemen-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.
4. www.hhs.gov/sites/default/files/fresenius-racap.pdf.
5. *Id.* n.3.
6. *Id.* n.4.
7. Press Release, U.S. Dep't of Health & Human Servs., "Consequences for HIPAA violations don't stop when a business closes" (Feb. 13, 2018), www.hhs.gov/about/news/2018/02/13/ consequences-hipaa-violations-dont-stop-when-business-closes.html.
8. www.hhs.gov/sites/default/files/filefax-receiver-racap.pdf.
9. www.hhs.gov/sites/default/files/alj-cr5111.pdf.
10. *Id.*