COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 6. June 11, 2020 Privacy Briefs: June 2020

By Jane Anderson

◆ **A divided Indiana Court of Appeals has reinstated a patient's claim that a hospital is vicariously liable for the actions of a medical assistant who accessed the patient's medical records and then shared details with her husband, according to *The Indiana Lawyer*.**[1] The patient, Haley SoderVick, sued Fort Wayne-based Parkview Health System Inc. after Parkview notified her in May 2018 of the disclosure of her protected health information (PHI). SoderVick had gone to an appointment with an obstetrician-gynecologist on Parkview's campus in Wabash in October 2017, and while she was there, medical assistant Alexis Christian accessed her medical records for one minute, the court record shows. "Christian then immediately texted information about SoderVick to Christian's then-husband, Caleb Thomas," Judge John Baker wrote for the majority. "In these texts, Christian disclosed SoderVick's name, the fact that she was a patient, a potential diagnosis, and that she worked as a dispatcher. Christian also texted Thomas that SoderVick was HIV-positive and had had more than fifty sexual partners, although this information was not included in her chart and was ultimately false," Baker wrote. "Christian testified that she had been checking Facebook on her phone during her lunch break earlier that day and had seen that SoderVick had liked a photo of Thomas. Later that afternoon, when Christian was 'inputting chart information and came across all of that information' about SoderVick, she claims she felt 'concerned' and therefore texted her husband asking if and how he knew SoderVick, curious as to whether they might have had a sexual history together." According to the court record, Thomas' sister saw the texts on his phone and notified Parkview, which investigated the potential HIPAA violation, ultimately firing Christian and notifying SoderVick. The case was remanded to the trial court for further proceedings.

◆ **Based in Phoenix, Arizona, District Medical Group (DMG), which includes more than 650 providers in health and medical specialties, said it suffered a breach in February that exposed PHI for more than 10,100 patients.**[2] "On March 11, 2020, we learned that an unauthorized person may have gained access to some DMG employee email accounts through an email phishing incident," the group said in its breach notification statement. The investigation indicates the unauthorized access occurred sometime between Feb. 4 and Feb. 10, the group said. Information that was accessed included patient names, medical record numbers, health insurance information, medical information, and Social Security numbers in some instances, the medical group said, adding that it would offer free credit monitoring for patients whose Social Security numbers were involved.

◆ **In a breach involving a business associate stemming from 2019, Ohio-based Management and Network Services (MNS) has begun notifying**[3] **more than 30,000 patients that their data may have been compromised.** The company provides administrative support services to post-acute providers and, in connection with these services, may receive information belonging to patients or individuals who were referred by, but did not receive services from, a provider. "On or about August 21, 2019, MNS confirmed that several employee email accounts may have been accessed without authorization at various times between April and July of 2019," the company said in a statement. "Five of the impacted email accounts were believed to contain personal or protected health information." MNS said it took steps to secure the email system and began analyzing the email accounts to determine what information may have been affected, and that the analysis "recently revealed" PHI in those accounts. The PHI may have included names, diagnosis and medical treatment information, information on medications, dates of service, insurance information, dates of birth and Social Security numbers. For a small

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

number of individuals, affected information may have included driver's license numbers, state identification card numbers and financial account information, the company said.

◆ **States—for example, California, Nevada and Maine—are becoming more active in the data privacy arena, enacting various new privacy laws. Other state governments are considering similar measures.** However, these state-level mandates "can create confusion and compliance issues," according to a new white paper from Clearwater Compliance.[4] "That's why there is a growing push among some for more unified, possibly even federalized, data privacy standards" similar to HIPAA. But as a health care organization that handles PHI or personally identifiable information, "how do you develop a data privacy and protection program that meets all of the emerging and changing standards and regulations, especially if you have limited resources or highly trained staff?" The answer, according to Clearwater, is to set the foundation of your program in an existing cybersecurity framework. Possible frameworks include free recommendations from the National Institute of Standards and Technology and more complex standards that entail certifications from the International Organization for Standardization, Clearwater said. Developing a basic program and then building forward will become more important as more states adopt new privacy statutes, the white paper said.

◆ **Oklahoma lawmakers are moving to modify the state's privacy laws so that health records necessary to protect the public health may be released, assuming HIPAA also allows release of the records.** The proposed legislation is aimed at informing first responders when they should use scarce personal protective equipment in responding to a call, and when that equipment might not be necessary. "While law enforcement and other first responders have been able to get this information during Oklahoma's catastrophic health emergency, HB 2938 makes sure this can continue once the emergency order ends," said bill sponsor Sen. Greg McCortney.[5]

◆ **The Federal Trade Commission (FTC) is seeking public comment on its health breach notification rule,[6] which took effect in 2009 and mandates the disclosure of data breaches by vendors that handle personal health data but are not covered by HIPAA.** The agency is seeking comment on a variety of issues, including whether the rule has resulted in overnotification or undernotification; whether the rule's definitions should be modified to reflect legal, economic and technological changes; whether the timing requirements and methods for reporting a breach should be altered; the implications for enforcement raised by direct-to-consumer technologies; and whether and how the rule should address developments in health care products and services related to COVID-19. As currently written, the rule requires covered companies to notify the FTC within 10 days after discovering a breach if more than 500 people are affected, and within 60 days if fewer individuals are affected. However, there have been no enforcement actions over the last decade, and only two companies have notified the FTC about breaches affecting more than 500 people.

◆ **Experts warned that entities performing contact tracing for patients who have COVID-19 need to abide by HIPAA in some instances.** Digital contact tracing in particular falls into a grey area, according to a report in *Health Affairs*, and this becomes important because contact tracing apps are an increasingly popular tool to combat the coronavirus.[7] Google and Apple recently announced they are jointly developing a contact tracing app that's based on Bluetooth proximity detection. They also designed the app to hold most information on users' phones rather than servers to address privacy issues. However, because neither Google nor Apple meet the definition of a covered entity under HIPAA, the law's privacy-enforcing requirements do not apply to the companies' contact tracing efforts, although some state laws, such as those in California, may provide some protections. Policymakers are seeking to close this loophole. Several U.S. senators are considering legislation that would govern contact-tracing apps operated by organizations not subject to HIPAA. However, other privacy experts are urging a consistent approach that would group all contact-tracing apps together.

◆ **Ohio's attorney general is warning that thieves posing as COVID-19 contact tracers are trying to trick state**

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

residents into handing over personal information.[8] Health departments are conducting contact tracing, said Ohio Attorney General Dave Yost, but will never ask for sensitive data, including Social Security numbers or bank account information, by phone.

1 Dave Stafford, "COA reinstates patient's claims against hospital in HIPAA-related suit," *The Indiana Lawyer*, May 15, 2020, https://bit.ly/3e8n4aa.
2 District Medical Group, "Notice to our Patients About an Email Phishing Incident," May 8, 2020, https://bit.ly/3bV6bhM.
3 Management and Network Services, "Management and Network Services, LLC Notifies Patients of Data Security Incident," accessed June 8, 2020, https://bit.ly/3bNMkRL.
4 Clearwater Compliance, "Building Frameworks to Manage Healthcare Data Within the Changing U.S. Privacy Landscape," accessed June 8, 2020, https://bit.ly/2AIaksq.
5 Destiny Washington, "Updated protection for first responders moves to Governor," KOKH Fox 25, https://bit.ly/36kafH5.
6 David F. Katz, "Amid Telemedicine's Rise, FTC Seeks Public Comment on Health Breach Notification Rule," Lexology, accessed June 6, 2020, https://bit.ly/2ziW5tS.
7 Carmel Shachar, "Protecting Privacy In Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork," *Health Affairs* (blog), May 19, 2020, https://bit.ly/2WOLqQG.
8 "Be wary as thieves posing as contact tracers, Ohio Attorney General says," WHO TV 7, updated May 20, 2020, https://bit.ly/2AdY7fk.

This publication is only available to subscribers. To view all documents, please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.