COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 11. November 05, 2020 Privacy Briefs: November 2020

By Jane Anderson

◆ **HHS Office of the National Coordinator (ONC) for Health Information Technology (ONC) is giving health care organizations more time to meet new rules on information blocking and conditions and maintenance of certification requirements.**[1] The 21st Century Cures Act mandated the new requirements, and ONC released the final rule on March 9. However, health care organizations have lobbied for an extension, saying the COVID-19 pandemic has complicated their implementation. An interim final rule, which ONC released Oct. 29, extends compliance dates until April 5, 2021, for most parts of the regulations, and for more than a year for certain sections. Don Rucker, national coordinator for health information technology, said "there is strong support for advancing patient access and clinician coordination through the provisions in the final rule, [but] stakeholders also must manage the needs being experienced during the current pandemic…To be clear, ONC is *not* removing the requirements advancing patient access to their health information that are outlined in the Cures Act Final Rule. Rather, we are providing additional time to allow everyone in the health care ecosystem to focus on COVID-19 response."

◆ **Sonoma Valley Hospital in California said a security incident on Oct. 11 knocked out its computer systems and "triggered a significant downtime event."**[2] The hospitals computer systems had not been fully restored nearly two weeks later, and some patients awaiting test results were repeatedly told to check back. The hospital did not provide any details about the incident, but on Oct. 22, it posted a notice about the systems failure and said it was able to care for patients using its "business continuity plan."[3] The patient portal is accessible to patients, but no new results have been posted since the incident.

◆ **The inspector general in Montgomery County, Maryland, is raising concerns for the second time in 2020 about personal information, including protected health information, being at risk of a security breach.**[4] Inspector General Megan Davey Limarzi released a report on Oct. 27 "concerning at least 529 child victims of sexual or physical abuse or neglect at the Tree House Child Advocacy Center in Rockville." Their names, biographical data, medical information, clinician notes and details of their abuse were accessible to any county employee or contractor that had access to a shared platform as of late September. The inspector general didn't say whether the data were accessed by unauthorized users. Limarzi had "reported on another set of unsecured documents in May. That case involved Medicare benefits applications stored on a shared platform at the county's Department of Health and Human Services," and it involved Social Security numbers, dates of birth, "Medicare numbers, bank checking account numbers, and applicants' addresses." Limarzi said that county agencies aren't taking seriously recommendations to either delete the sensitive information or restrict access to personal documents on the shared platforms.

◆ **California lawmakers have clarified and harmonized the applicability of the California Consumer Privacy Act (CCPA) to patient information.**[5] According to Brandon Reilly, partner with Manatt, Phelps & Phillips LLP, California lawmakers have approved a "little-noticed amendment" that expands the CCPA's exemptions of patient information to include research data and more information handled by business associates. The amendment also harmonized the law's de-identification exemption with HIPAA, Reilly said. However, in doing so, the amendment created "a novel restriction on re-identification and introduced public disclosure and

contract obligations that may be surprising to health care entities unaccustomed to CCPA compliance," Reilly said. Many health care companies erroneously believe they are exempt at the entity level from the CCPA, when in fact the CCPA employs "a clutter of exemptions targeting health-related data sets," he said. Under the new CCPA amendment, "California law now explicitly bans any re-identification of de-identified patient information (DPI) unless certain exceptions apply." The law also requires public disclosure of any sale or sharing of de-identified patient information and new contractual restrictions covering the sale or license of such information, Reilly said. The new law also contains other provisions that could affect California health care companies, he said, noting that health care companies are "well advised to revisit their CCPA compliance efforts to ensure they are meeting these new obligations."

◆ **Centerstone of Tennessee Inc., a nonprofit health system that provides mental health and substance use disorder treatments, is notifying current and former patients and employees that their personal and protected health information could have been accessed without their authorization during a data breach.**[6] The investigation started after an employee noticed "unusual activity" involving their email account, according to WSMV in Nashville. Centerstone said personal information from some current and former Centerstone patients had been "accessed without authorization."[7] The incident occurred between Dec. 12 and Dec. 16, 2019, and the information included names, dates of birth, Social Security numbers, driver's license or state identification card numbers, medical diagnosis or treatment information, Medicaid information, Medicare information, and health insurance information. Centerstone said, "We have no evidence that any personal or protected information was misused," and added that it is "immediately investing more than $800,000 dollars to upgrade IT security infrastructure, including new software applications and security appliances." Centerstone is offering "potentially impacted individuals" complimentary credit monitoring and identity theft restoration services.

◆ **At least 2,219 patients at McLaren Oakland hospital in Pontiac, Michigan, have been notified that their personal data might have been accessed.**[8] According to *Crain's Detroit Business*, officials at the nonprofit hospital "became aware of a computer desktop file containing an unauthorized and unsecured link to a file containing patients' protected health information…The link was accidentally left open by an employee, but an investigation found no evidence of fraudulent or criminal activity." McLaren has implemented additional employee training and is offering free identity theft monitoring and protection services.

◆ **Patients of a large psychotherapy clinic in Finland were blackmailed after their data were stolen, according to a Finnish news report.**[9] The data appear to have included personal identification records and notes about what was discussed in therapy sessions. The psychotherapy clinic, Vastaamo, is a nationwide practice with around 20 branches. The clinic said it believed the data were stolen in November 2018, with a second potential breach in March 2019. Approximately 300 records already have been published on the dark web, according to the report.

◆ **The health care industry tops the list of most expensive data breaches with a $7.13 million average data breach cost, 84% more than the global average, according to London-based investment firm AksjeBloggen.**[10] Overall, "the global average cost of a data breach has fluctuated between $3.5 million and $4 million in recent years. In 2020, it hit $3.86 million, a 1.5% drop" from 2019 levels, according to the firm, and the health care industry also led in another category: the longest average time to identify a violation. It takes a health care company an average of 329 days to identify a data breach. Malicious attacks caused 52% of all breaches, the study showed, while human error and system glitches followed, causing 23% and 25%, respectively. "Statistics also show that around 20% of companies that had been victims of a malicious breach were hacked by using stolen or compromised credentials."

1 HHS, "HHS Extends Compliance Dates for Information Blocking and Health IT Certification Requirements in

21st Century Cures Act Final Rule," news release, October 29, 2020, https://bit.ly/34PyspD.
2 Anne Ward Ernst, "Sonoma Valley Hospital computer systems shut down by 'security incident,'" *Sonoma Index-Tribune*, October 22, 2020. https://bit.ly/34D0i8r.
3 Sonoma Valley Hospital, "Notice to Hospital Patients About Computer Systems Disruption," news release, updated October 30, 2020, https://bit.ly/30PBQJm.
4 Dominique Maria Bonessi, "Montgomery County Inspector General Again Raises The Alarm On Data Security Breaches," *DCist*, October 27, 2020, https://bit.ly/3jEX1df.
5 Brandon Reilly, "California Harmonizes CCPA, HIPAA But Providers Still Face Obligations," *Bloomberg Law*, October 27, 2020, https://bit.ly/31UBF5y.
6 Joseph Wenzel, "Centerstone patients, employees impacted by data breach," WSMV, October 24, 2020, https://bit.ly/2TDkRvq.
7 Centerstone, "Notice of Security Incident," news release, accessed November 2, 2020, https://bit.ly/3jNPhWs.
8 Jay Greene, "Possible data breach exposes 2,219 patient files at McLaren Oakland hospital," *Crain's Detroit Business*, October 15, 2020, https://bit.ly/30H2VOw.
9 Zoe Kleinman, "Therapy patients blackmailed for cash after clinic data breach," BBC News, October 26, 2020, https://bbc.in/3e69BBb.
10 Jastra Kranjec, "Average Cost of Data Breach in Healthcare Industry Hit $7.13 Million in 2020, 84% More Than Global Average," AksjeBloggen, September 23, 2020, https://bit.ly/3mrhrrY.