COSMOS
Navigate the Compliance Universe

# Report on Patient Privacy Volume 20, Number 7. July 09, 2020 Privacy Briefs: July 2020

By Jane Anderson

◆ **Concerns about hacking and online security have fallen since the onset of the COVID-19 pandemic, despite the fact that the actual risks have risen, according to the 2020 Unisys Security Index report.**[1] The World Health Organization (WHO) and Interpol have warned of increased cyberattack risk during the pandemic, and estimates indicate there have been as many as 192,000 coronavirus-related cyberattacks globally per week in May 2020 alone, a 30% increase compared to April. Google's Gmail service reported that it saw more than 18 million daily malware and phishing emails related to COVID-19 scams in just one week, and more than 240 million daily spam messages related to COVID-19. However, only 45% of respondents to the global survey said they are concerned about the risk of being scammed during or about a health crisis. "This is worrying given that the vast majority of cyberattacks—98%, by some estimates—deploy social engineering methods (such as phishing), with the WHO reporting a fivefold increase in attacks since the start of the pandemic," the report said. "This blind spot is likely the result of an overconfidence in online protection, and an urgent need to prioritize the most immediate and tangible concerns—namely, instincts toward health and survival—in a situation that shows signs of being 'peak concern' for consumers globally," the report said.

◆ **An Illinois appeal court has ruled that a county in the state no longer must release the names of COVID-19 patients to emergency dispatchers.**[2] The ruling by the "2nd District Appellate Court of Illinois reversed an April 10 ruling by McHenry County Judge Michael Chmiel that gave the McHenry County Emergency Telephone System Board access to names and addresses of those who" have tested positive for COVID-19. It "was beyond question that plaintiffs had no right to the information" sought, the names and addresses, Appellate Justice Joseph Birkett wrote in his opinion. He said the health information that was released fell within an exception to HIPAA that permitted but did not require the health department to release it. The health department no longer is providing the patient information to the emergency board system.

◆ **Canadian laboratory testing company LifeLabs "failed to protect the personal health information of millions of Canadians, resulting in a 'significant privacy breach,'** according to a joint investigation by Ontario and [British Columbia's] information and privacy commissioners."[3] In December, the company revealed it had been the target of a cyberattack that affected the private information of 15 million Canadians. The joint investigation, which concluded last month, found the company failed to implement reasonable safeguards to protect the personal health information. This violated British Columbia's personal information protection law, Ontario's health privacy law and the Personal Health Information Protection Act. "'LifeLabs' failure to properly protect the personal health information of British Columbians and Canadians is unacceptable,' [British Columbia] information and privacy commissioner Michael McEvoy said in a statement. LifeLabs exposed British Columbians, along with millions of other Canadians, to potential identity theft, financial loss and reputational harm." The results of the investigation also found that LifeLabs failed to have adequate technology security policies and collected more personal information than necessary.

◆ **American Medical Technologies said it has suffered a data breach that may have affected nearly 50,000 patients.** The company, based in Irvine, California, said the cyberattack occurred in December 2019, when it discovered suspicious activity on an employee's email account.[4] AMT provides long-term care programs for

seniors. The company hired a third-party forensic team, which established that a breach had taken place. The inquiry, which was conducted in May, found that protected health information and other personal information may have been visible and available to the hacker. Potentially compromised information includes: patient names, Social Security numbers, medical record numbers, diagnosis information, health insurance policy information, medical history information and driver's license or state identification card information. American Medical Technologies states that it is unaware of any misuse of this information. The company has established a toll-free call center to answer questions about the incident and to help those affected enroll in free credit monitoring services.

◆ **Miami-based population health company Cano Health LLC reports that "three employee email accounts were accessed by an unknown perpetrator," leading to a breach that exposed more than 28,000 patients' personal information.**[5] "The unauthorized access may have occurred between May 18, 2018, and April 13, 2020. The information in the compromised email accounts during that time included patient names, dates of birth, contact information, healthcare information, insurance information, [S]ocial [S]ecurity numbers, government identification numbers and/or financial account" information. "Based on its investigation, Cano Health cannot confirm that any emails were accessed by the unknown perpetrator, but because some emails contained documents or messages with personal information, it is notifying all potentially affected individuals out of an abundance of caution," the company said in its breach notification. Cano Health also said it is offering complimentary credit monitoring services for the 28,268 individuals affected.

◆ **A Missouri county "has opened a health privacy investigation after revealing the possibility of a problem with information contained on the county's COVID-19 dashboard."**[6] Clay County revealed the investigation after an individual contacted a local media outlet, saying they were able to access a spreadsheet of personally identifiable information on the public dashboard of the Clay County Public Health Center. The information listed positive COVID-19 cases, with personally identifiable information that included names, addresses, age group, ethnicity, phone numbers and addresses. At least 16 of the entries on the spreadsheet included the names of individuals with an address that matches the Pleasant Valley Manor Care Center, a local facility with a known outbreak of COVID-19. The information no longer is available on the website, and the health center released a statement saying it is investigating.

◆ **Choice Health Management Services, based in Claremont, North Carolina, said hackers were able to gain access to email accounts last year.**[7] The company, which provides IT, payroll, billing and compliance functions for independent living, assisted living and skilled nursing facilities, said it was unable to determine whether individual emails or attachments in the affected email accounts were subject to unauthorized access. However, information that potentially was affected by the breach included first and last names, along with dates of birth, Social Security numbers, driver's license numbers, passport numbers, credit card information, financial account information, employer identification numbers, usernames with password or associated security questions, email addresses with passwords or associated security questions, dates of service, provider names, medical record numbers, patient numbers, medical information, diagnostic or treatment information, surgical information, medications, and health insurance information. The company said it was "unaware of any actual misuse of personal information relating to this event."

◆ **CHI St. Luke's Health-Memorial, based in Lufkin, Texas, said late last month that an unauthorized third party had gained access to patient information.**[8] An internal investigation indicated that the breach occurred on April 23 through two employee email accounts. Potentially compromised information includes names, diagnoses, dates of services and facility account numbers. "Though we have no evidence to confirm that information was actually viewed or obtained by the individual, we cannot totally rule it out as a possibility," the hospital said in a release. "We discovered the potential exposure as we were investigating a security event involving one of our

servers, which we learned about on March 25." The hospital's "investigation included engaging forensic experts, interviewing employees, reviewing data and access logs, conducting threat intelligence analysis and reviewing various data file types," the hospital said, adding that electronic health records were not involved. Some of the individuals affected by the event may be eligible for free credit monitoring, the hospital said.

◆ **The Central California Alliance for Health said it recently became aware of a data security breach that may have resulted in the unintentional disclosure of member health information.**[9] The Alliance is the Medi-Cal managed care plan for three California counties: Merced, Santa Cruz and Monterey. The health plan, which has more than 330,000 members in those three counties, said an unauthorized third party accessed three employees' email accounts during a brief period on May 7 in an attempt to obtain the credentials of several individuals. After potentially suspicious activity, Alliance staff began an investigation to determine what information may have been accessed. The plan determined that limited member health information may have been accessed, but that the information would not have included financial information or Social Security numbers. Potentially affected members have been notified, according to the plan.


**1** Unisys, 2020 Unisys Security Index: Global Edition, last accessed July 6, 2020, https://bit.ly/2Vsc0xG.
**2** Sam Borcia, "Appellate court rules in favor of health department in battle over releasing COVID-19 patient data," Lake & McHenry County Scanner, June 28, 2020, https://bit.ly/31rPrNF.
**3** Joel Ballard, "LifeLabs failed to protect personal health information of millions, commissioners say," CBC News, June 25, 2020, https://bit.ly/3ifvPlG.
**4** American Medical Technologies, "American Medical Technologies Notifies Consumers of Data Security Incident," June 18, 2020, https://bit.ly/2VubZt4.
**5** "Cano Health Advises Patients of Potential Data Security Issue," Cano Health Blog, June 12, 2020, https://bit.ly/3eFcs3n.
**6** Matt Flener, "Clay County Health Center opens privacy investigation into its COVID-19 dashboard," KMBC News, June 23, 2020, https://bit.ly/2AiVysu.
**7** Choice Health Management Services, "Choice Health Management Services, LLC Provides Notice of a Data Breach," PR Newswire, June 23, 2020, https://prn.to/2ZiD6Zv.
**8** Grace Juarez, "CHI St. Luke's Health-Memorial reports patient information data breach," The Lufkin Daily News, June 24, 2020, https://bit.ly/2BTbv9i.
**9** Shawn Jansen, "Data breach reported for Merced County's Medi-Cal managed healthcare plan,"Merced Sun-Star, June 30, 2020, https://bit.ly/2YLKflY.