COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 12. December 09, 2021 Privacy Briefs: December 2021

By Jane Anderson

◆ **Huntington Hospital in New York has sent notices to approximately 13,000 patients about an incident that happened in late 2018 and early 2019 involving a night shift employee who improperly accessed electronic medical records.**[1] The employee was immediately suspended and subsequently fired, and a law enforcement investigation resulted in the former employee being charged with a criminal HIPAA violation. "The hospital cooperated with the law enforcement investigation, which included following instructions to delay notifying any patients who were potentially impacted by this incident through November 2021," Huntington Hospital said in a statement. "There is no evidence that the former employee accessed Social Security numbers, insurance information, credit card numbers or other payment-related information. The patient information accessed by the former employee may have included demographic-type information such as name, date of birth, telephone number, address, internal account number and medical record number; and clinical information such as diagnoses, medications, laboratory results, course of treatment, the names of health care providers, and/or other treatment-related information." In addition to its "robust compliance program that includes ongoing training of its employees, implementation of security tools to monitor access to medical record applications, and audits of medical record access," the hospital said it has "taken additional steps to prevent this type of incident from occurring in the future, including bolstering access controls and targeted re-training of staff on the importance of protecting patient confidentiality." Huntington Hospital is offering all affected patients complimentary identity theft protection services.

◆ **Southern Ohio Medical Center (SOMC) in Portsmouth, Ohio, was forced to reschedule some procedures and divert ambulances to other hospitals after it was hit with a cyberattack.**[2] "This morning, an unauthorized third-party gained access to SOMC's computer servers in what appears to be a targeted cyber attack," the hospital said in a statement. "We are working with federal law enforcement and internet security firms to investigate this incident. Patient care and safety remain our top priority as we work to resolve this situation as quickly as possible. While this does not impact our ability to provide care to current inpatients, we are presently diverting ambulances to other hospitals." The hospital canceled appointments for medical imaging, cancer services, cardiovascular testing, cardiac catheterization, outpatient surgery and outpatient physical and occupational rehabilitation following the Nov. 11 attack.

◆ **True Health of New Mexico said it identified and addressed a data security incident and notified the affected patients.**[3] True Health did not say how many patients were affected by the incident, which occurred on Oct. 5. The incident was caused by an unauthorized third party who gained access to the organization's information technology system in early October. "Security professionals determined that impacted data may have included a person's name, date of birth, age, home address, email address, insurance information, medical information, Social Security number, health account member ID, provider information, dates of service, and provider identification number and dates of service," True Health said in a statement. "At this time, we have no evidence that any personal information has been misused." The organization is mailing letters directly to those individuals whose information may have been involved and is offering free credit monitoring and identity theft protection.

◆ **Indianapolis-based Eskenazi Health is beginning to notify some of the nearly 1,516,000 patients whose personal information was affected in a data breach earlier this year.**[4] Local news organization FOX59 obtained a copy of the letter, dated Nov. 11, sent to some patients, which claimed that "sophisticated cyber criminals had gained access to its network on or about May 19, 2021, using a malicious internet protocol address." Information potentially compromised included names, dates of birth, ages, addresses, phone numbers, email addresses, medical record numbers, patient account numbers, diagnoses and clinical information, physician names, insurance information, prescriptions, dates of service, driver's license numbers, passport numbers, face photos, Social Security numbers and credit card information. Eskenazi is offering free credit monitoring and identity theft protection services for one year.

◆ **The personal data of 2,347 clients of three Sonoma County, California, agencies may have been exposed during a breach of a county contractor's network, county officials said.**[5] "An August ransomware attack on the network of Seneca Family of Agencies may have exposed" personal information, including names, Social Security numbers, addresses and phone numbers, along with diagnosis and treatment information, the county said. "Seneca provides mental health, counseling and family engagement services for the county Human Services Department, Health Services Department and Probation Department. The county said there is no evidence that clients' personal data has been misused as a result of the breach but, as a precaution, Seneca is notifying county clients whose data was stored on its network....Seneca is providing potentially impacted individuals with 12 months of free credit monitoring and identity protection services."

◆ **A former patient at Northwestern Memorial HealthCare has filed a class-action lawsuit against Northwestern Medicine and Swedish company Elekta over an April data breach that involved cancer patients' records.**[6] Elekta, which provides radiation services for cancer and brain disorders, experienced a data breach in spring 2021 that affected 170 health care systems, including Northwestern Medicine. The data breach jeopardized the personal health information of more than 200,000 patients at Northwestern Memorial HealthCare, including Deborah Harrington, who filed the lawsuit. Information that was particularly at risk included names, dates of birth, Social Security numbers and other private health information and data. The suit, which claims the defendants "acted negligently and did not adequately protect patients' information," is seeking damages for the patients whose data was potentially breached.

◆ **A former employee benefits plan administrator has notified Southern Illinois Healthcare (SIH) of a possible data breach dating from nearly eight years ago and involving nearly 1,000 current and former employees and covered family members.**[7] SIH said it received notification on Oct. 15 of the security incident following the conclusion of Consociate Health's 10-month investigation. Some 982 individuals were affected, according to SIH. Consociate Health's analysis said the risk included personally identifiable information that could have been compromised between Jan. 1, 2014, and Dec. 31, 2015. The information potentially breached may have included names, addresses, dates of birth, Social Security numbers, diagnosis codes, medical record numbers, health insurance policy numbers and medical record information. Consociate Health said there is no evidence the information was misused, but it will offer one year of free identity monitoring services to affected individuals.

◆ **Cybersecurity & Infrastructure Security Agency (CISA) and the FBI have warned critical infrastructure partners, including health care entities, that cyberattacks may ramp up over the holiday period.**[8] "Malicious cyber actors aren't making the same holiday plans as you," the two agencies said in a combined statement. "Recent history tells us that this could be a time when these persistent cyber actors halfway across the world are looking for ways —big and small—to disrupt the critical networks and systems belonging to organizations, businesses, and critical infrastructure." Although neither CISA nor the FBI have identified any specific threats, "recent 2021 trends show malicious cyber actors launching serious and impactful ransomware attacks during holidays and weekends, including Independence Day and Mother's Day weekends." The agencies urged organizations to

identify information technology security employees "for weekends and holidays who would be available…in the event of an incident or ransomware attack." In addition, they recommended implementing "multi-factor authentication for remote access and administrative accounts" and mandating strong passwords that are not reused across multiple accounts. "If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored," the warning said. "Remind employees not to click on suspicious links, and conduct exercises to raise awareness." The two agencies also recommended maintaining vigilance against "phishing scams, such as unsolicited emails posing as charitable organizations"; "fraudulent sites spoofing reputable businesses," such as holiday shopping sites; and "unencrypted financial transactions."

1 Huntington Hospital Northwell Health, "Huntington Hospital – Notice of Unauthorized Access to Personal Information," news release, November 24, 2021, https://bit.ly/30dKpzc.
2 WSYX Staff, "Southern Ohio Medical Center canceling some appointments after cyberattack," WSYX ABC 6, November 11, 2021, https://bit.ly/3d7mYBp.
3 Carla Amundaray, "True Health New Mexico Informs Individuals of Data Security Incident and Offers Support," Business Wire, news release, November 15, 2021, https://bwnews.pr/3d9hCW9.
4 Bianca Reyes, "Eskenazi patients receive letter in the mail alerting them of cyber security breach 6 months ago," FOX59, November 17, 2021, https://bit.ly/3rGVqeL.
5 KPIX 5, "Personal Data of Thousands of Sonoma County Agencies' Clients Possibly Hacked," November 25, 2021, https://cbsloc.al/30ch20h.
6 Catherine Odom, "Northwestern faces cheer team, retirement, tuition and data breach lawsuits," *The Daily Northwestern*, November 16, 2021, https://bit.ly/3Dd8Ot0.
7 The Southern staff, "SIH notified of potential data breach involving ex-benefit plan administrator," *The Southern Illinoisan*, November 23, 2021, https://bit.ly/3pizcwz.
8 Cybersecurity & Infrastructure Security Agency, "Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends," November 22, 2021, https://bit.ly/3IdlNi8.