HARVARD | BUSINESS | SCHOOL

9-123-065

FEBRUARY 17, 2023

SURAJ SRINIVASAN

LI-KUAN (JASON) NI

Ransomware Attack at Springhill Medical Center

In July, 2019, Springhill Medical Center ("SMC") in Mobile, Alabama fell prey to a malicious ransomware attack that crippled the hospital's internal network systems and public-facing web page. While the hospital rushed to securely restore the network, medical personnel scrambled workarounds to continue medical services. Amidst the chaos, a baby was born in the hospital with umbilical cord wrapped around her neck that had resulted in severe brain injury and died nine months later. The mother and family sued SMC, alleging the hospital failed to inform her of the cyber incident, which she believed had compromised the quality of care and led to an otherwise preventable tragedy.

The alleged association between the ransomware attack and infant death received nationwide attention as likely being the first documented case of death directly linked to a ransomware attack.[1] The case raised important questions of how SMC had responded to the ransomware attack. Had it done enough to respond to the attack and inform staff, doctors and patients? And how should hospitals and other organizations manage the ever-increasing threat of ransomware breaches.

Springhill Medical Center

SMC's predecessor Springhill Memorial Hospital was founded in 1975 with the founder's vision to "rewrite the traditional and make the most advanced a common occurrence" and to "build a medical center second to none." The hospital's mission was "to be the best health care provider in Mobile where patients, physicians, and payers can rely on our outstanding staff to efficiently provide health care that is unmatched in quality, convenience, and benefit of use in a courteous and family-oriented manner."[2]

As Mobile's first private hospital, SMC had more than quadrupled in size throughout the years and had become a major player among Mobile's local healthcare providers. The full-service hospital's featured areas included cardiovascular, thoracic, primary care, orthopedics, structural heart, surgery, emergency department, heart center, hyperbaric medicine, and birthing suites. Among the 89 hospitals in Alabama in 2019, SMC ranked 26th in staffed beds (209), 20th in total discharges (11,527), 17th in total patient days[a] (59,522), and 24th in total patient revenue ($689 millions). In 2021, SMC ranked 26th in

[a] Total patient days measured the total number of days for all patients who were admitted for an episode of care and who separated during a specified reference period.

Professor Suraj Srinivasan and Research Associate Li-Kuan (Jason) Ni prepared this case. This case was developed from published sources. Funding for the development of this case was provided by Harvard Business School and not by the company. HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management.

staffed beds (200), 22nd in total discharges (9,602), 18th in total patient days (56,458), and 26th in total patient revenue ($679 millions).[3]

The hospital's leadership team was led by President/CEO Jeffery M. St. Clair who was a SMC veteran of more than 35 years. Systems and Data were led by Chief Information Officer Mark Kilborn who had also been with SMC for over 20 years (see **Exhibit 1** for the leadership team bios). In 2011, Kilborn led SMC to become one of the first Gulf Coast hospitals to successfully implement the Electronic Health Record technology (called Sunrise) that automated clinical tasks and connected healthcare providers to coordinate among themselves. When asked during a 2015 interview with a healthcare journalist, Kilborn admitted that IT security was the biggest challenge that "[kept him] awake all night." Acknowledging the big cybersecurity incidents at Anthem Inc. and Community Health Systems just months earlier, Kilborn said,

> We are taking [cybersecurity] very seriously. Part of meaningful use requires that you do an external security audit, which we have done. Security is a 24-hour, 7-day-a-week endeavor. The threat is out there, it's real. We have the FBI coming later this month to meet with the department heads to talk about cybersecurity both here in the workplace, as well as at home. It's important to educate and re-educate end users on making good decisions on what they put in the system, as well as what they do at home and how it all ties together.[4]

Ransomware

Ransomware was a type of malware[b] that prevented users from accessing their data by locking the system's screen or files until a ransom was paid. To do so, hackers first exploited system vulnerabilities through phishing emails[c], stolen or guessed employee login credentials, direct network intrusion, or the like. After the malware had gained access to a system, attackers began to encrypt files with an attacker-controlled key, effectively locking the files. Skilled ransomware perpetrators were cautious in their selection of files to encrypt to avoid quick detection, and some variants would also delete backup files to make recovery without the decryption key more difficult. The more files the extortionists encrypted the more effective they were in paralyzing the system for normal users. Once the encryption was complete, the ransom demand was made, often by changing a display background to a ransom note or placing the note as a text file in each encrypted directory. Typically, these notes demanded a set amount of cryptocurrency in exchange for access to the victim's files. If the ransom was paid, the ransomware operator would provide the keys and methods to unlock the files and restore user access.[5]

Since around 2015 ransomware had become a major source of cyber risk. Cybersecurity experts estimated that annual ransomware attacks had risen from 183 million attempts in 2016 to 623 million by 2021 (see **Exhibit 2** for global ransomware rates and total ransom paid from 2016 to 2021). Ransomware amounted to about 11% of all data breaches incidents in 2022, and the average cost to the victim of the attack was about $4.54 million. These costs included detection, notification, crisis management, post-breach restitution, and lost business costs.

Data breach costs varied by industry. An IBM study concluded that healthcare industry had experienced the highest average breach costs for at least 12 consecutive years. The average cost of a

[b] Malware was a software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

[c] Phishing email was a form of social engineering where attackers sent emails to deceive the recipient into revealing sensitive information or installing malware.

breach in healthcare increased from 2019's estimate of $6.45 million to 2022's $10.10 million. Hackers' propensity to target the healthcare industry was largely due to the critical nature of its services and hence the low affordability of downtime.[6]

Further, ransomware on average took 326 days to identify and contain, or 49 days longer than the global average across different types of cyber breaches of 277 days. Victim organizations also experienced an average of 20 days in post-attack system downtime. Perhaps due to its disruptive potential, a 2022 survey of corporate executives ranked ransomware as the second highest cyberbreach concerns (closely behind targeted phishing attacks).[7]

Also, paying ransom did not always guarantee a full recovery of data and function. IT consulting firm Gartner estimated in 2021 that organizations that paid the ransom were only able to recover 65% of their data, and only 8% of organizations recovered all the encrypted files. Cost wise, IBM estimated in 2022 that organizations that paid ransom incurred an average total cost of $4.49 million while those that did not pay incurred $5.12 million.[8]

The Ransomware Attack at SMC and Kidd's Delivery

SMC detected the ransomware on July 8, 2019 and refused to pay an undisclosed amount of ransom demand. The hospital rushed to shut down the network, including the Sunrise electronic health record system, and attempted to securely regain control of its systems.[9]

Press reports suggest that much confusion and uncertainty existed throughout the incident. At first, many front-line staffers were oblivious about the cyber-attack. One nurse recalled finding vague notes taped to their computers saying the medical records system was down until further notice. A local news station inquired with the hospital but only learned that it was experiencing a "network event" and that patient care was not affected. Another news station was told that "the system had a virus but wouldn't [call it] a cyber attack." An anonymous employee was later said, "We've all been told, basically, keep Springhill Medical Center's name out your mouth, don't talk about what's going on inside or you'll be terminated."[10]

Inside the hospital, routine tasks typically carried out with modern technologies suddenly became arduous and difficult, especially for younger staff who had not worked without modern technology. A *Wall Street Journal* article described the situation:

> In the medical imaging departments, radiologists peered into the cramped screens attached to scanning equipment because the dedicated workstations with high-resolution monitors they normally used to examine CT scans and MRIs were down. In anesthesiology, the absence of medical records "put lives at risk," [according to] an anesthesiologist. …[N]urses in the second-floor maternity ward had to start keeping handwritten paper records. Older staffers tutored their younger colleagues on paper charting, including hand-drawing graphs showing patients' vital signs. ...[D]octors and nurses…texted each other with updates. "We have no computer charting for I don't know how long," one manager informed a nurse…. "They are printing out the labs in the laboratory and sending them by paper," another worker wrote. One overwhelmed nurse texted, "I want to run away." [11]

An employee also reported, "[The cyberattack] effected everything in the hospital, payroll, nothing works, no computers work[,] everything is confusing. You can't read anybody's writing, it's terrible, everything is haywire." Another inside source also claimed that the attack had caused a department to

shut down, with some employees told to not come to work for several days while others pulled to jobs they were never trained on.[12]

Then-CEO Jeffrey St. Clair later stated, "We stayed open and our dedicated healthcare workers continued to care for our patients because the patients needed us and we, along with the independent treating physicians who exercised their privileges at the hospital, concluded it was safe to do so."[13]

A week went by and SMC's IT system remained unserviceable. As staffs and patients grew increasingly worried that their personal information might be compromised, SMC released a statement in the morning of July 16:

> We are currently addressing a security incident affecting our internal network. After learning of this issue, we immediately shut down our network to contain the incident and protect all data, notified law enforcement, and engaged leading outside forensic experts to support our investigation. As we have worked diligently to investigate and remediate the incident, our staff has continued to safely care for our patients and will continue to provide the high quality of service that our patients deserve and expect.[14]

Hours later, SMC provided an additional statement:

> Our staff has implemented standard downtime procedures to mitigate the impact to our patients, and we are working diligently to maintain the same high quality of care as when our systems are operating normally. We have continued seeing our normal volume of patients over the past week.[15]

On that same morning of July 16, Teiranni Kidd checked in to the hospital to be induced due to gestational hypertension. According to medical records, Kidd had "routine prenatal care and an uneventful pregnancy." An ultrasound a week prior to her admission had confirmed that the fetus was healthy. According to the lawsuit complaint, Kidd "had no knowledge of the effect that the cyberattack was having on [SMC], on hospital operations, or the quality of patient care."[16]

In the birthing suite where Kidd was administered synthetic oxytocin to induce her labor, all vital-tracing monitors would normally be linked to a large screen at the nurse station for central monitoring; however, due to the ransomware incident the large screen was nonfunctional, and nurses had to rely on bedside monitors that gave out sound alert when attention was needed. These monitors also spooled out paper strips showing the rate of heart beat. Nurses put patients in the rooms closest to the nurses station and tuned up the volume of the bedside fetal heart monitors. They were also instructed to stay in or near patients' rooms at all times.[17]

On the morning of July 17, the strip in machine recording Kidd's condition recorded fetal distress signal, which the later lawsuit brought by Kidd claimed that the medical personnel failed to respond to or intervene in an appropriate manner. About an hour later Kidd was fully dilated and nurses called down attending obstetrician Katelyn Parnell for the delivery. Kidd's daughter was born near noon with umbilical cord wrapped around her neck. A lack of oxygen and blood had led to severe brain damage and other serious ailments. A "code blue" was called and a neonatologist arrived to resuscitate the newborn before transferring her to the nearby USA Women & Children's Hospital where the infant spent months in the neonatal intensive care unit.[18]

On July 22 – two weeks after the initial attack – the systems were still down and the hospital website still showed "page not found" or "down for maintenance." However, the nature of the attack started to leak. "[T]here is a ransom, this is what I have been hearing from people in high places at the hospital. There is ransom in return for money then they will leave the hospital alone," an anonymous employee

said to a reporter, "We don't deserve to be going through this. We don't deserve to be frustrated. We deserve to have equipment up and running. Patients deserve the treatment they deserve. This can be life threatening."[19]

Rumors of a second cyberattack also surfaced from the same source but it was quickly refuted by the hospital through a statement made on July 23:

> We'd like to assure our patients and the community that patient safety is always our top priority and we would never allow our staff to operate in an unsafe environment. After learning of the security incident, we promptly shut down our network to contain the incident and protect data. We continue to bring our network back up carefully to ensure our systems are operating normally and securely, and there is no truth to the claim that we have experienced a second incident. We have provided employees with consistent updates about the status of our computer systems and we greatly appreciate their diligence in maintaining excellent care while utilizing downtime procedures.[20]

The following day on July 24th, news media reported that investigators had confirmed that the the attack was indeed in the form of a ransomware, possibly introduced into the system through an email. It also reported that Mobile Police took the initial report of the incident but later turned the case to the FBI since most attacks originated internationally.[21]

SMC eventually returned its systems to services without paying the ransom about three weeks after the initial attack. Although the hospital never disclosed the identify of the perpetrator, third-party IT experts suspected the attack to be the work of the Russian-based Ryuk gang that had attacked at least 235 hospitals and healthcare facilities in the United States between 2018 and 2019. It was estimated that Ryuk had collected over $100 million in ransom payment in 2018, with a typical ransom demand of about $700,000. [22]

In April, 2020, Kidd's infant girl died. She was nine months old.[23]

Medical Malpractice Lawsuit

Kidd filed a civil lawsuit against SMC and Dr. Parnell in January, 2020. An amended complaint was filed in June, 2020 after the death of her infant.

The complaint accused the hospital and Dr. Parnell of fraudulent non-disclosure as they failed to inform Kidd of the nature, scope, and impact of the cyberattack. The complaint stated that SMC "planned, orchestrated, and implemented a scheme by hospital management and ownership in which they conspiratorially hid, suppressed, and failed to disclose critical patient safety-related information, and further created a false, misleading, and deceptive narrative concerning the July 2019 cyberattack," and that "had the above disclosure been made, Plaintiff Teiranni Kidd would have gone to a different and safer hospital for labor and delivery."

The complaint also alleged wrongful death, negligence, and breach of implied contract by the hospital and Dr. Parnell as they failed to use a fetal scalp monitor during the labor, recognize the presence of life-threatening nuchal cord, seek timely treatment for Kidd and infant, and respond promptly when fetal distress was exhibited during labor, among other allegations. The complaint stated,

> Because numerous electronic systems were compromised by the cyberattack, fetal tracing information was not accessible at the nurses' station or by any physician or other

> healthcare provider who was not physically present in Teiranni's labor and delivery room…. As a result the number of healthcare providers who would normally monitor her labor and delivery was substantially reduced and important safety-critical layers of redundancy were eliminated.[24]

The complaint did not, however, accuse the hospital for the failure to prevent a cyberattack.

SMC denied any wrongdoing. The hospital asserted that under Alabama law hospitals did not have any legal duty to provide details of a cyberattack. As such SMC requested a judge to dismiss part of the lawsuit that suggested the "deceptive narrative" conspired by the hospital had made the child's delivery unsafe. The hospital claimed Dr. Parnell should be the one responsible to notify the patient of the cyber incident since she "was fully aware of the inaccessibility of the relevant systems, including those in the labor and delivery unit, and yet determined that (Kidd) could safely deliver her at Springhill."[25]

In a court filing, Dr. Parnell said that she was aware of the cyberattack, but "believed Ms. Kidd could safely delivery her baby at Springhill" when Kidd presented to the hospital. Dr. Parnell and her medical group denied she did anything that hurt or caused the child's injuries and death. Still, in a text conversation reported by the press, Dr. Parnell maintained if she had seen the monitor printout then she would have "100%" performed a caesarian section on Kidd. "I need u to help me understand why I was not notified," Dr. Parnell wrote to ask the nurse manager. In a separate text with another colleague, Dr. Parnell was reported to have written, "This was preventable."[26]

Conclusion

SMC was one of the 764 American healthcare providers that fell prey to ransomware in 2019. This number was 560 in 2020 and a whopping 1,203 in 2021 (see **Exhibit 3** for statistics on U.S. healthcare providers data breaches and **Exhibit 4** for examples of other hospital cyber breaches). Numbers aside, these attacks caused significant and sometimes life-threatening disruption: ambulances redirected, cancer treatments delayed, lab test results blocked, hospital employees furloughed, and 911 services interrupted.[27]

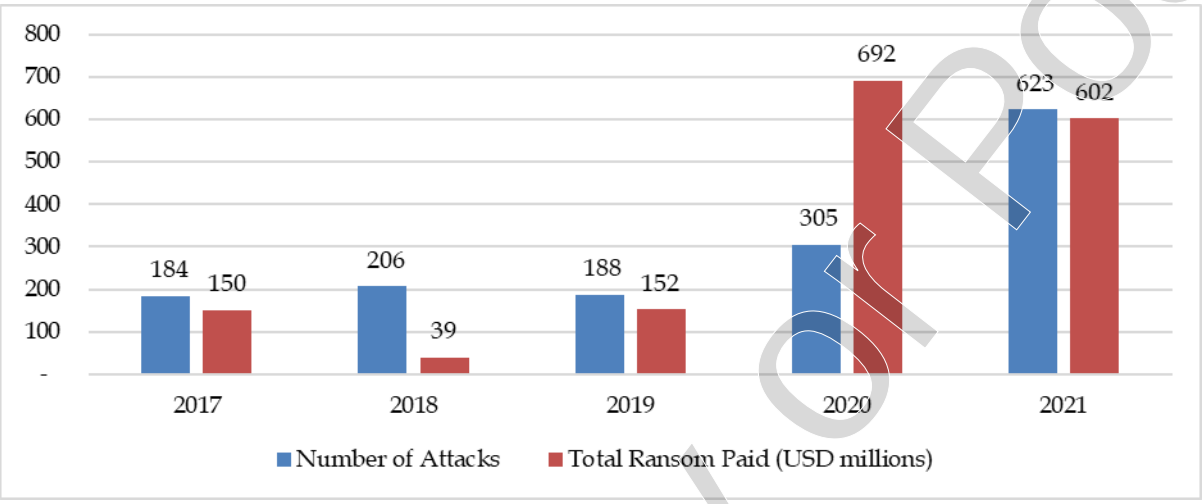
As of February 2023, the trial related to the death of Kidd's child had not commenced. With the ever present threat of ransomware and other cyberattacks on hospitals, how healthcare providers should respond to these attacks remained an open yet pressing challenge.

Exhibit 1 Springhill Medical Center Leadership Summary

Title	Name	Notable Experience
President/CEO	Jeffery M. St. Clair, MHA	• CEO at SMC since 2009; COO/Hospital Administrator for 15 years and VP of Operation for 8 years
VP/COO	Rene J. Areaux, FACHE	• SMC VP/COO since 2009 • Fellow of the American College of Healthcare Executive • Former president of the Southeast Louisiana Chapter of the American College of Healthcare Executives • Registered respiratory therapist
Chief Nursing Executive	Paul Read, RN, MSN	• Chief Nursing Executive at SMC since 2002 • Had worked at SMC since graduation from nursing school in 1998 • US Navy Executive Officer of a Forward Resuscitative Surgical Company supporting USMC Forces
VP/CFO	Stephen "Jan" Grigsby, MHA, FHFMA	• Former Senior VP/CFO of Memorial University Medical Center • Former CFO of Jupiter Medical Center • Former CFO of Methodist Hospital North • Former CFO/COO of Mizell Meorial Hospital
VP/Chief Information Officer	Mark Kilborn	• SMC CIO since 2000 • Various leadership positions at Mobile Infirmary Medical Center for 26 years

Source: Compiled by casewriters with data from LinkedIn and Springhill Medical Center, "Our Leadership," https://www.springhillmedicalcenter.com/who-we-are/our-leadership, accessed February, 2023.

Exhibit 2 Global Ransomware Attack Count and Total Ransom Paid Estimates



Source: Casewriters with data from SonicWall, "Annual number of ransomware attacks worldwide from 2016 to first half 2022 (in millions) [Graph]," *Statista*, June 22, 2022, https://www-statista-com.ezp-prod1.hul.harvard.edu/statistics/494947/ransomware-attacks-per-year-worldwide/, accessed January, 2023; see also Chainalysis, "As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict," February 10, 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/, accessed February, 2023.

Exhibit 3 U.S. Healthcare Industry Breaches Affecting 500 Individuals or More

Year	Number of Breaches Affecting 500+ Individuals	Total Individuals Affected	Average of Individuals Affected
2009	18	134,773	7,487
2010	199	5,932,276	29,810
2011	200	13,162,158	65,811
2012	217	2,853,985	13,152
2013	277	7,018,839	25,431
2014	314	19,073,551	60,744
2015	270	112,466,720	416,543
2016	328	16,711,004	50,948
2017	357	5,305,045	14,860
2018	368	14,230,522	38,670
2019	511	44,963,289	87,991
2020	663	34,541,474	52,099
2021	715	55,619,405	77,789
2022	713	52,127,518	73,110
Total	5,180	385,120,128	74,362

Source: Casewriters with data from U.S. Department of Health and Human Services, Office for Civil Rights, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, accessed February 2023.

Note: Two breaches in 2015 at Anthem Inc. and Premera Blue Cross affected a combined 89.8 million individuals.

Exhibit 4 Other Hospital Data Incidents

Data breach incidents at hospitals had become common. Besides ransomware, data breaches could happen from other supply chain attack, brute force attack (e.g. guessed credentials), physical theft, distributed denial of services ("DDoS") attack, among others. Below are three illustrative examples.

Ransomware: University Hospital Düsseldorf

On September 10, 2020, University Hospital in Düsseldorf ("UHD"), Germany experienced disrupted email and telephone services, and soon ransomware was detected. The ransomware invaded 30 servers, compromised the digital infrastructure that the hospital relied on to coordinate doctors, beds, and treatment, forcing the cancellation of hundreds of operations and other procedures. As such it cut the hospital's capacity by half. The hospital had to de-register from providing emergency care, alongside of having to reschedule planned surgeries.

On the night of September 11, paramedics were alerted to the deteriorating condition of a 78-year-old woman suffering from an aortic aneurysm. When they called UHD – the closest hospital – they were told to divert the patient to another hospital 32 kilometers away, which delayed the patient's treatment by an hour. The patient died shortly after.

Germany's Federal Agency for Security in Information Technology later concluded that the attackers breached the hospital using a hole in Citrix software that was patched in January, 2020. It was likely that the ransomware had furtively invaded the hospital before the vulnerability was fully patched. Perplexingly, the ransom note was addressed to the Heinrich Heine University and not UHD. As a result, the police contacted the hackers and informed them that they had hit the "wrong target" and that lives were in danger. In return, the ransom demand was withdrawn and decryption keys were provided. Still, it took the hospital almost two weeks to restore essential services and allow emergency care to re-open, and longer to become fully operational again.

Supply Chain Attack: Trinity Health

Trinity Health ("Trinity") system was one of the largest healthcare providers in the U.S. with over 88 hospitals, 135 continuing care locations, 136 urgent care locations, and 27,000 physicians and clinicians in 26 states.

On July 16, 2020, Trinity's philanthropy database cloud vendor Blackbaud notified Trinity of a cyber-attack that included ransomware that had impacted Trinity and other companies' donor database back-up files maintained by Blackbaud. More than 10 million records were compromised, of which more than 3.32 million records belonged to Trinity, including dates of birth, physical and email addresses, social security numbers, treatment information, and financial payment data. In a security notice, Blackbaud said that it had paid an undisclosed amount of ransom to have the data copy destroyed, and that it had subsequently fixed the vulnerability.

Less than six months later on January 29, 2021, Accellion, another third-party vendor that provided Trinity large file transfer services, notified Trinity of a security issue: hackers had exploited four known, unpatched vulnerabilities in Accellion's File Transfer Appliance platform. Trinity later confirmed that over 586 thousand patients were affected by this data breach and terminated the use of Accellion's platform.

Internal IT Failure: Advocate Aurora Health

With 26 hospitals across Wisconsin and Illinois, Advocate Aurora Health ("Aurora") was one of the largest healthcare providers in the Midwest.

Meta Pixel was a common snippet JavaScript codes to track visitors on websites, recording vital information on how they interacted, how long they stayed on the site, and where they dropped off. It was a useful tool that helped web designers and organizations make their sites more user-friendly. However, in the case of Advocate Aurora Health, the use of Meta Pixel on patient portals — where patients enter sensitive information caused private health information to be disclosed, especially if users were logged into Facebook or Google at the same time.

In July, 2022, Aurora sent out a statement that the company's improper use of pixels might have exposed patient information to various third-party providers:

> These pixels or similar technologies were designed to gather information that we review in aggregate so that we can better understand patient needs and preferences to provide needed care to our patient population….We learned that pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of our scheduling widgets, transmitted certain patient information to the third-party vendors that provided us with the pixel technology.

Aurora had since disabled the use of pixels from its platforms. The healthcare provider maintained that these pixels would be "very unlikely" to result in identity theft or any financial harm.

Source: Melissa Eddy and Nicole Perlroth, "Cyber Attack Suspected in German Woman's Death," *The New York Times*, September 18, 2020, https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html, accessed February, 2023; see also, William Ralston, "The Untold Story of a Cyberattack, a Hospital and a Dying Woman," *Wired*, November, 11, 2020, https://www.wired.co.uk/article/ransomware-hospital-death-germany, accessed February, 2023; see also Jantje Silomon, "The Düsseldorf Cyber Incident," *Institute for Peace Research and Security Policy at the University of Hamburg*, September 30, 2020, https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident, accessed February, 2023; see also Emma Contreras, "Over Half a Million Trinity Health Patients Affected in Data Breach," May 18, 2021, https://www.paubox.com/resources/over-half-million-trinity-health-patients-affected-data-breach/, accessed February, 2023; see also, Trinity Health, "Trinity Health Announces Response to Accellion Data Event," April 5, 2021, https://www.prnewswire.com/news-releases/trinity-health-announces-response-to-accellion-data-event-301262364.html, accessed February, 202; see also Gaby Vinick, "Data Breach in Advocate Aurora Health System May Have Exposed up to 3M Patients' Information," *Wisconsin Public Radio*, October 21, 2022, https://www.wpr.org/data-breach-advocate-aurora-health-system-may-have-exposed-3m-patients-information, accessed February, 2023; see also Annie Burky, "Advocate Aurora Says 3M patients' Health Data Possibly Exposed through Tracking Technologies," *Fierce Healthcare*, October 20, 2022, https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3, accessed February, 2023.

Endnotes

[1] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[2] Springhill Medical Center, "Who We Are," https://springhillmedicalcenter.com/who-we-are, accessed January 2023; see also Springhill Medical Center, "Our Mission," https://springhillmedicalcenter.com/who-we-are/our-mission, accessed January 2023; see also Springhill Medical Center, "Words From Our Founder," https://www.springhillmedicalcenter.com/who-we-are/words-our-founder, accessed January 2023.

[3] Springhill Medical Center, "Who We Are," https://springhillmedicalcenter.com/who-we-are, accessed January 2023; see also Springhill Medical Center, "Home Page," https://springhillmedicalcenter.com/, accessed January 2023; see also American Hospital Directory, "Individual Hospital Statistics for Alabama," compiled from each hospital's most recent cost report and other sources, https://www.ahd.com/states/hospital_AL.html, accessed February 2023; see also American Hospital Directory, "Individual Hospital Statistics for Alabama," compiled from each hospital's most recent cost report up and other sources up to March 26, 2020, https://web.archive.org/web/20200326083320/https://www.ahd.com/states/hospital_AL.html, accessed February 2023.

[4] Katie Dvorak, "CIO Spotlight: Cybersecurity keeps Springhill's Mark Kilborn 'awake all night' [Q&A]," *Fierce Healthcare*, March 16, 2015, https://www.fiercehealthcare.com/it/cio-spotlight-cybersecurity-keeps-springhill-s-mark-kilborn-awake-all-night-q-a, accessed February, 2023.

[5] Checkpoint.com, "How Ransomware Works," https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=After%20ransomware%20has%20gained%20access,originals%20with%20the%20encrypted%20versions., accessed February, 2023.

[6] SonicWall, "Annual number of ransomware attacks worldwide from 2016 to first half 2022 (in millions) [Graph]," In Statista, June 22, 2022, https://www-statista-com.ezp-prod1.hul.harvard.edu/statistics/494947/ransomware-attacks-per-year-worldwide/, accessed January, 2023; see also IBM Security, "Cost of a Data Breach Report 2022," July, 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ, accessed February, 2023; see also SonicWall, "2022 SonicWall Cyber Threat Report," 2022, https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf, accessed February, 2023; see also IBM Security, "Cost of a Data Breach Report 2019," July, 2019, https://www.ibm.com/downloads/cas/RDEQK07R, accessed February, 2023.

[7] IBM Security, "Cost of a Data Breach Report 2022," July, 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ, accessed February, 2023; see also SonicWall, "2022 SonicWall Cyber Threat Report," 2022, https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf, accessed February, 2023; see also Coveware, "Average Duration of Downtime after a Ransomware Attack from 1st Quarter 2020 to 4th Quarter 2021 [Graph]," In *Statista,* February 3, 2022, https://www-statista-com.ezp-prod1.hul.harvard.edu/statistics/1275029/length-of-downtime-after-ransomware-attack/, accessed February, 2023.

[8] Edward Segal, "Why Experts Disagree On Whether Businesses Should Pay Ransomware Demands," *Forbes*, July 29, 2022, https://www.forbes.com/sites/edwardsegal/2022/07/29/why-experts-disagree-on-whether-businesses-should-pay-ransomware-demands/?sh=17ab27a74fca, accessed February, 2023; see also Sally Adam, "The State of Ransomware 2021," April 27, 2021, https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/, accessed February, 2023; see also, IBM Security, "Cost of a Data Breach Report 2022," July, 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ, accessed February, 2023.

[9] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[10] *Ibid;* see also WKRG News, "Springhill Medical Center Releases Statement on 'Network Security Incident'," July 16, 2019, https://www.wkrg.com/mobile-county/only-on-news-5-springhill-medical-center-releases-statement-on-network-security-incident/, accessed January, 2023; see also Rachel Wilkerson, "Computer Issues Continue at Springhill Medical Center," *NBC 15 News*, July 22, 2019, https://mynbc15.com/news/local/springhill-medical-center-allegedly-hacked-again, accessed January, 2023; see also Nicole Fierro, "Additional Inside Sources Come Forward about Springhill Medical Center Cyber Attack," *NBC 15 News,* July 26, 2019, https://mynbc15.com/news/local/additional-inside-sources-come-forward-about-springhill-medical-center-cyber-attack#, accessed January, 2023.

[11] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[12] Rachel Wilkerson, "Computer Issues Continue at Springhill Medical Center," *NBC 15 News*, July 22, 2019, https://mynbc15.com/news/local/springhill-medical-center-allegedly-hacked-again, accessed January, 2023; see also Nicole Fierro, "Additional Inside Sources Come Forward about Springhill Medical Center Cyber Attack," *NBC 15 News*, July 26, 2019, https://mynbc15.com/news/local/additional-inside-sources-come-forward-about-springhill-medical-center-cyber-attack#, accessed January, 2023.

[13] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[14] WKRG News, "Springhill Medical Center Releases Statement on 'Network Security Incident'," July 16, 2019, https://www.wkrg.com/mobile-county/only-on-news-5-springhill-medical-center-releases-statement-on-network-security-incident/, accessed January, 2023.

[15] *Ibid.*

[16] Teiranni Kidd v. Springhill Hospitals, First Amended Complaint, Circuit Court of Mobile County, Alabama, Civil Action NO. 02-CV-2020-900171, Filed June 4, 2020, https://www.documentcloud.org/documents/21072978-kidd-amended-complaint, p.3-8, accessed January 2023.

[17] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023; see also Teiranni Kidd v. Springhill Hospitals, First Amended Complaint, Circuit Court of Mobile County, Alabama, Civil Action NO. 02-CV-2020-900171, Filed June 4, 2020, https://www.documentcloud.org/documents/21072978-kidd-amended-complaint, p.3-8, accessed January 2023.

[18] *Ibid.*

[19] Rachel Wilkerson, "Computer Issues Continue at Springhill Medical Center," *NBC 15 News*, July 22, 2019, https://mynbc15.com/news/local/springhill-medical-center-allegedly-hacked-again, accessed January, 2023.

[20] Brad Gunther, "Springhill Medical Center Victim of Ransomware Attack," *NBC 15 News*, July 24, 2019, https://mynbc15.com/news/local/mobile-police-springhill-medical-center-was-victim-of-cyber-attack, accessed January, 2023.

[21] *Ibid.*

[22] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[23] *Ibid.*

[24] Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023; see also Teiranni Kidd v. Springhill Hospitals, First Amended Complaint, Circuit Court of Mobile County, Alabama, Civil Action NO. 02-CV-2020-900171, Filed June 4, 2020, https://www.documentcloud.org/documents/21072978-kidd-amended-complaint, p.3-8, accessed January 2023.

[25] Associated Press Staff, "Suit Blames Baby's Death on Cyberattack at Alabama Hospital," *AP*, October 1, 2021, https://apnews.com/article/technology-business-health-alabama-lawsuits-68c78e9d6af359842c0e9645b4577b50, accessed January, 2023.

[26] *Ibid.*; see also Kevin Poulsen, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death," *The Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116, accessed January, 2023.

[27] Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2019," December 12, 2019, https://www.emsisoft.com/en/blog/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/, accessed February, 2023; see also Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, https://www.emsisoft.com/en/blog/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/, accessed February, 2023; see also Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2021," January 18, 2022, https://www.emsisoft.com/en/blog/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/, accessed February, 2023.