Healthcare Delivery Under Attack: Healthcare Industry Cybersecurity at the Close of 2023

Just imagine: your loved one needs an emergency room, right away, but the ER is closed due to a cyberattack. This is not a scary dream, but, unfortunately, a reality of healthcare delivery, today. Just earlier this fall, a hospital in the Hudson Valley of the New York region temporarily was forced to divert patients due to a full-stop cyberattack. The healthcare industry – all across the care continuum, from hospitals to physician practices – is a major target for cyberattacks because of its dependence on complex information technology systems and its storage of personal information. This piece will touch on the scope of the risk, and the regulatory response, underway.

Recent Cyberattacks

This fall, two major cyberattacks made national headlines. On Thanksgiving, Ardent Health Services (Ardent) experienced a ransomware attack that disrupted 30 of its hospitals and shut down emergency rooms in at least three states. Ardent was unable to restore access to its electronic medical record system and other core clinical and business systems until December 6.

Coincidentally on the 6th, a German dialysis group, Fresenius Medical Care, reported a breach at one of its U.S. subsidiaries, Cardiovascular Consultants, Ltd. The attacker was able to gain access to the medical records and personal information of 500,000 current and former patients and guarantors. Additionally, 200 staff members' personal information was compromised, affecting constituents across the United States and in several other countries.

This is all part of a larger trend: the Office for Civil Rights (OCR) has recorded a 93% increase in data breaches from 2018 to 2022, and healthcare companies reported 536 data breaches during 2023 to OCR. According to a 2021 study conducted by Proofpoint and the Ponemon Institute, during a ransomware attack there is an increase in the mortality rate for admitted patients. Additionally, cyberattacks force hospitals to cancel elective procedures and disrupt critical emergency care operations.

Looking Ahead

Regulators will begin to impose additional cybersecurity requirements on the healthcare sector. In keeping with this trend, the U.S. Department of Health and Human Services (HHS) recently published a concept paper telegraphing its position on the importance of cybersecurity requirements within the healthcare sector; if HHS has its way, organizations' reimbursement would be conditioned on the development of their cybersecurity posture. The plan is part of the broader effort to implement a Federal Cybersecurity Strategy.[1] The concept paper focused on four main goals:

---

1 *It should be noted that Mr. Oberfield, one of this piece's co-authors, is a member of the HHS 405(d) Task Group, part of the HHS 405(d) Program. That Program "is focused on providing organizations across the nation with useful and impactful Healthcare and Public Health (HPH) focused resources, products and tools that help educate, raise awareness and provide vetted cybersecurity best practices which drive behavioral change and strengthen the sector's cybersecurity posture against cyber threats" (see, https://405d.hhs.gov/, last accessed December 19, 2023).*

Establish voluntary cybersecurity performance goals for the healthcare sector. Cybersecurity Performance Goals (CPGs) would include foundational cybersecurity practices and encourage the implementation of advanced practices.

Provide resources to incentivize and implement these cybersecurity practices. HHS would implement an up-front investments program and an incentives program.

Implement an HHS-wide strategy to support greater enforcement and accountability. Ultimately, HHS would fold CPGs into existing regulations and programs, including through the Centers for Medicare and Medicaid Services (CMS). Additionally, OCR would enhance the Health Insurance Portability and Accountability Act (HIPAA) Security Rule with additional cybersecurity requirements.

Expand and mature the one-stop shop within cybersecurity. Overlaying all this would be a greater connection between healthcare delivery organizations and HHS's Administration of Strategic Preparedness and Response (ASPR), an agency equipped with healthcare emergency preparedness expertise.

Federal Enforcement Efforts

Shortly after the release of the concept paper, HHS entered into a settlement agreement with a Louisiana medical group, Lafourche Medical Group (LMG), regarding a phishing attack that led to violations of HIPAA. In 2021, LMG experienced a phishing attack that exposed the electronic health information of nearly 35,000 individuals. After the breach, OCR launched an investigation and determined that LMG did not have any policies or procedures in place to safeguard protected health information against cyberattacks. As part of the settlement, LMG agreed to pay $480,000 to OCR and take steps to improve its security measures, such as addressing security risks and vulnerabilities, implementing compliant HIPAA policies and providing cyber training to staff.

Additionally, in October 2023, the HHS entered into a settlement with Doctors' Management Services (DMS) for a ransomware attack that compromised the data of nearly 207,000 individuals. In April 2017, DMS's network was infected with GandCrab ransomware, but it was not detected until it was used to encrypt DMS files during December 2018. DMS filed a breach report with HHS in April 2019 and OCR began its investigation. OCR concluded that DMS failed to implement required policies and procedures under the HIPAA Security Rule, had insufficient monitoring of its information systems and failed to have a risk analysis in place to detect potential risks and vulnerabilities within its environment. DMS has agreed to pay $100,000 to OCR, take steps to resolve the HIPAA violation and improve its security measures.

NYS Enforcement Efforts

Similarly, in the financial sector, the New York Department of Financial Services (DFS) has amended its cybersecurity regulation. The amendment expands cybersecurity requirements that financial institutions must comply with, which includes implementing safeguards to prevent unauthorized access to its networks and conducting additional risk assessments. The regulation applies to any entity operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law. Therefore, insurance companies, pharmacy benefit managers and other similar entities

are subject to the regulations. (Healthcare delivery organizations without a financial product may not be; any entity with questions thereon should consult with counsel.)

Further demonstrating the increased desire for increased cybersecurity regulations in the healthcare industry, proposed cybersecurity regulations in New York would require hospitals to implement cybersecurity safeguards to better protect its systems and networks used to provide patient care. The proposed regulations were reviewed by the Public Health and Health Planning Council (PHHPC) and published in the State Register on December 6. Public comment is open through February 5, 2024, and if ultimately finalized, hospitals would have one year to comply with the regulations.

Some are not waiting for regulation: instead, they are jumping into upstream preventative work. For instance, in Florida, CommunityHealth IT, Inc. (CommHIT) has begun to administer two federal grants for heath and public health (HPH) sector facilities in rural, underserved and other remote areas. The grants (referenced here) are aimed to assist these facilities with implementing cybersecurity safeguards. Additionally, through the grants, CommHIT is providing educational resources to aid in protecting Florida's critical access hospitals (CAHs), Emergency Medical Services (EMS) agencies and communities from cyberattacks. Further, CommHIT is training workers in healthcare occupations in the use of technology and cybersecurity best practices.

Takeaways

The LMG and DMS settlements constituted the first instances of HHS entering into settlements with healthcare institutions resulting from reports of exploited phishing attacks. These settlements demonstrate that HHS is expanding its enforcement powers and emphasizing its effort to ensure the healthcare industry has robust and effective cybersecurity programs.

With the increased attention to cybersecurity, healthcare institutions should review and strengthen cybersecurity policies and procedures.

Bond attorneys regularly assist and advise clients on an array of healthcare, data privacy and cybersecurity matters. For more information regarding healthcare and data privacy, please contact Gabriel Oberfield, Shannon Knapp, CIPP/US & CIPP/A, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to associate trainee Victoria Okraszewski for her assistance in the preparation of this publication. Victoria is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS