KEEPING UP WITH CLINICAL RISK MANAGEMENT

A QUARTERLY PUBLICATION

LESSONS LEARNED FROM 2020 HEALTHCARE BREACHES

Danielle Donovan | Clinical Risk Manager

2020 has been a remarkable year full of challenges never before faced, testing our persistence and endurance to carry onward. It has also been a year full of cybercrime, with nearly 1 million health records breached in November, targeting healthcare organizations and testing their internal network security. Not only can these cybercrimes be a huge disruptor and financial liability, but Office for Civil Rights (OCR) fines, settlements, and legal fees can be devastating as well. Here is a look back on some of the biggest trends in data breaches and settlements of 2020 and the hard lessons learned.

PHISHING CAMPAIGNS AND RANSOMWARE/ MALWARE ATTACKS

Blackbaud – The non-profit software company faced a ransomware attack in February on its self-hosted environment that compromised the data of more than 10 million individuals, with almost a million of those victims from healthcare entities. Although a ransom demand was paid and data was returned, it's unclear whether those cybercriminals actually destroyed the data or still maintain a copy today. The breach was allegedly caused by Blackbaud's failure to implement adequate cybersecurity measures and protocols necessary to protect individuals' personal health information (PHI) stored in the cloud.

Magellan Health – In April, hackers accessed nearly 365,000 patients' and employees' data by leveraging a social engineering phishing scheme that impersonated a Magellan Health client.

BJC Healthcare – In May, over 287,876 patients' PHI was exposed after hackers were successful with a phishing attack, gaining access through three separate employee's emails.

Premera Blue Cross – In September, Premera agreed to pay OCR $6.85 million to settle potential violations related to a HIPAA breach that affected more than 10.4 million people. The settlement is the second largest payment to resolve a HIPAA investigation to date, which centered on a 2014 email phishing attack on Premera's systems that lasted for nine months.

Metropolitan Community Health Services – In July, Metropolitan agreed to pay OCR $25,000 to settle potential HIPAA violations stemming from a June 2011 data breach. OCR found that Metropolitan failed to conduct any risk analyses or provide staff security awareness training to prevent security incidents.

PREVENTION STRATEGIES

- Conduct regular security awareness training, education, and phishing email simulations for your workforce. Include cybersecurity terminology and implementation of cybersecurity best practices.
- Secure email gateways and block emails that contain malicious attachments.
- Limit the use of personal emails.
- Leverage email and web browser security settings to protect against modified emails and unsecured webpages.

continued >

- Avoid conducting sensitive activities through public networks.
- Implement effective security tools, such as anti-malware software and intrusion detection/ prevention solutions that can help to prevent, detect, and contain attacks.
- Conduct vulnerability scans monthly and penetration tests at least twice a year.
- Build in redundancy and contingency planning so that data can be recovered quickly and operations can continue. Use a 3-2-1 backup strategy by having a hard copy, remote backup, or both.

STOLEN DEVICES

Health Share of Oregon – In February, Health Share notified over 650,000 members that an unsecured laptop containing individuals' PHI was stolen from its transportation vendor, GridWorks. Although Health Share's policies require business associates to use encryption on all devices with PHI, this laptop was not encrypted for unknown reasons.

Lifespan – Although the breach occurred in 2017, Lifespan agreed to settle a potential HIPAA violation related to a stolen laptop for over $1 million in July 2020. OCR found that the health system had systemic non-compliance with HIPAA rules, including failure to encrypt patients' PHI.

PREVENTION STRATEGIES

- Ensure devices are encrypted
- Require multi-factor authentication (MFA) for accessing your systems whenever possible, especially for remote access users.
- Require regular password changes.
- Maintain inventory of what's on your network, including the hardware, software, and assets, to know what is at risk from an attack or unauthorized access.
- Replace unsupported operating systems, applications, and hardware. Test and deploy patches quickly.

MISHANDLED MEDICAL RECORDS

Elite Emergency Physicians- In June, Elite Emergency Physicians reported that its third-party vendor, Central Files, had improperly disposed of patient medical records, impacting over 550,000 patients.

PREVENTION STRATEGIES:

- Understand business associates' security measures to determine whether their systems could infect your network, disrupt patient care, or put your organization at risk.
- Constantly update and test your organization's incident response plan through mock breach exercises.

UNAUTHORIZED ACCESS:

Mayo Clinic – The clinic is facing multiple lawsuits over an employee who accessed the medical records of 1,600 patients without authorization. The lawsuit alleges that the Mayo Clinic did not implement systems or procedures to ensure patients' health records would be protected and that the former employee accessed those medical records without first obtaining the patients' consent.

The New Haven (Conn.) Health Department – In October, the health department agreed to pay $202,400 for a 2017 breach related to improper termination of a former employee's access to patient medical records. The former employee returned to the health department eight days after being fired and accessed the system using active credentials. PHI, including names, addresses, and dates of birth was downloaded onto a USB drive.

continued >

PREVENTION STRATEGIES

- Ensure policies, procedures, and technologies are aimed at protecting the privacy of individuals' health information.
- Limit PHI access to only those who need it to carry out their job duties.
- Immediately restrict employee login credentials upon termination or change in positions.
- Utilize anti-virus software and endpoint detection and response (EDR).
- Regularly review CISA, FBI, and HHS websites for cybersecurity updates and recommendations.
- Take advantage of training resources available through insurance carriers, professional associations, and academic institutions.

One of the most common ways to mitigate cybercrime losses is by purchasing cyber liability insurance. However, in 2017, only 30% of healthcare organizations purchased cyber insurance, compared to 90% of organizations in the financial sector. Due to dramatic increases in ransomware losses over the past year and the increased cyber exposure from the high number of employees working remotely, obtaining coverage for a competitive price is becoming increasingly difficult. In 2016 and 2017, healthcare data breaches have been reported on an almost daily basis. This will be no different in 2021; breaches and ransomware attacks will continue to occur, thus driving up cyber coverage prices. Those organizations that purchase coverage and work in tandem with their cyber carriers to proactively address potential vulnerabilities will be better positioned as they enter a new year. Healthcare organizations should also work with their brokers to carefully review policy coverage gaps and ensure full liability protection.

For more information on cyber liability insurance, please contact your cyber liability team at Parker, Smith & Feek.

Danielle Donovan is Parker, Smith & Feek's Clinical Risk Manager, dedicated to helping improve our healthcare clients' operations and mitigate risks. She publishes regular articles to support this effort and provide unbiased advice on issues facing all types of healthcare organizations. Stay tuned for her next installment, and contact Parker, Smith & Feek's Healthcare Practice Group if you would like to learn more.

References and Resources

1. Review Policies on Cyberattacks As FBI, HHS Send New Warning Accreditation Insider, https://www.psqh.com/news/review-policies-on-cyberattacks-as-fbi-hhs-send-new-warning/
2. Biggest Healthcare Breaches Of 2020 – The Top 10 and Why They Matter, https://www.govhealthit.com/biggest-healthcare-breaches-of-2020-the-top-10-and-why-they-matter/
3. Update: The 10 Biggest Healthcare Data Breaches Of 2020, So Far, https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far
4. California Medical Center Server Issue Exposed Patient Data For 4.5 Years, https://www.beckershospitalreview.com/cybersecurity/california-medical-center-server-issue-exposed-patient-data-for-4-5-years.html
5. 17 HIPAA settlements in 2020, https://www.beckershospitalreview.com/cybersecurity/18-hipaa-settlements-in-2020.html
6. Kabir, Umar Yusuf. "Trends and Best Practices in Healthcare Cybersecurity." *ASHRM Journal of Healthcare Risk*, vol. 40, no. 2, 12 Nov. 2020, online.fliphtml5.com/byhb/bpuh/?1604431458927#p=3