MCRA

Compliance Flash

Topic: Cyber Criminals Target Healthcare

September 2022

Why should you be paying attention?

According to the IBM Security Cost of a Data Breach Report 2022, the average cost of a data breach is $4.35 million. 11% of the breaches included in the study were related to ransomware attacks, with an average cost of $4.54 million. 19% of the breaches that occur are related to a business partner compromise. The most common cause of a breach is stolen or compromised credentials. Notably, stolen or compromised credential breaches take the longest to identify, with an average of 243 days. Phishing is the second most common type of breach. Lastly, healthcare has had the highest average cost for a breach for the last 12 years, averaging $10.10 million in 2021.

Additionally, according to the FBI Internet Crime Complaint Center 2021 Internet Crime Report, the healthcare sector experienced the most ransomware victim incidents. There were 38% more victim incidents than the second highest sector, which was Financial Services.

Recent Healthcare Breaches

Eye Care Leaders EMR Data Breach

- Detected Unauthorized Access to myCare Integrity system on December 25, 2021.
- Eye Care Leaders is a Business Associate and this breach impacted 16 known organizations and 583,700 individuals.
- Unauthorized party had access and control of individuals’ names, date of birth, social security numbers, and certain treatment information.
- Negotiated its return and offered individuals credit monitoring and identity theft protection.

Allegheny Health Network Data Breach

- Detected malicious phishing email that was sent to an employee on June 1, 2022.
- Unauthorized party had access to protected health information (PHI) for approximately 8,000 patients.
- Offered identity theft protection and monitoring.

Look Out For:

- Social Engineering Scams
  - Phishing Scams
  - Vishing Scams
  - Smishing Scams
  - Whaling Scams
  - Spear Phishing Scams
- Ransomware Tactics
- Stolen or Lost Equipment Containing Protected Health Information

Implement Administrative, Physical and Technical Safeguards

- Policies and Procedures
- Access Controls
- Audit and Monitoring
- Physical Security
- Emergency Preparedness Plan
- Business Continuity
- Workforce Education and Training

HIPAA Breach Reporting Requirements

- Notify impacted individual within 60 days of discovering the breach.
- If breach involved more than 500 individuals, notify media and DHHS within 60 days of discovering the breach.
- If breach involves less than 500 individuals, notify DHHS annually.

We Are Here to Help

Connect With Us to Learn More

✉ info@mcra.com

www.mcra.com/contact-us

☎ 202.552.5800