



STAYING AFLOAT

HOW BUSINESS ASSOCIATE BREACHES THREATEN TO SINK HEALTHCARE ORGANIZATIONS



The volume and magnitude of cyber breaches of business associates has healthcare organizations struggling to stay afloat and maintain patient safety, HIPAA compliance, and operations.

ASSESSING THE THREATS: RECENT HEALTHCARE BUSINESS ASSOCIATE BREACHES

Routinely reviewing the latest business associate breaches can help to create situational awareness to better protect against the next wave of attacks.

Here are details on some of the most recent healthcare vendor breaches.



Kronos was hit with a ransomware attack, revealing that information from many of its high-profile customers may have been accessed. Kronos Private Cloud was forced to shut down operations for weeks. Kronos provides HR software including critical functions for time keeping, payroll, and benefits.

[Read more](#)



Microsoft Exchange Outlook Web Access servers were accessed remotely by threat actors.

An IIS web server module named "Owowa" was installed which allowed attackers to steal credentials.

[Read more](#)



BioPlus's IT network was hacked. An investigation confirmed files containing the protected health information of certain patients had been accessed. 350,000 current and former patients were notified about the breach. BioPlus is also facing a related class-action lawsuit.

[Read more](#)



Onfido, an identification verification (IDV) service, let a major flaw in their security go unchecked, in the form of an exposed admin token that potentially left millions of app users' biometric data exposed. Left millions of app users' biometric data exposed including liveness check videos and/or selfies customers take to prove their identities.

[Read more](#)



The electronic health record vendor QRS has been sued in a new class action lawsuit based on a cyberattack that impacted almost 320,000 current and former patients. Attackers accessed QRS patient portal servers and acquired sensitive information including PHI, SSNs, and treatment information.

[Read more](#)



Marketing giant RR Donnelley (RRD) confirmed that threat actors stole data in a cyberattack. While RRD initially said they were not aware of any client data stolen during the attack, the Conti ransomware gang claimed responsibility and began leaking 2.5GB of data allegedly stolen from RRD.

[Read more](#)



Doxy.me is resolving an issue that gave three third-party companies access to the names of patients' providers. Doxy.me took measures to remove provider names from the URLs it sent to third parties, but the third parties used technical loopholes to view the full URLs.

[Read more](#)



Anthem Inc. alerted 2,003 members that some of their protected health information has potentially been viewed or obtained by an unauthorized individual who gained access to the network of one of its business associates.

[Read more](#)



Ibex announced that the company's IT systems were the target of a malware attack, resulting in the compromise of sensitive consumer data of more than 174,000 individuals.

[Read more](#)



EMI Health suffered a hacking/IT incident to their network server that affected approximately 39,317 individuals.

Details are limited and the breach was reporting to the Department of Health and Human Services.

[Read more](#)








The Medical Review Institute of America was the victim of a cyberattack. After an investigation, PHI was found to be breached, but there was no reported evidence of misuse of the sensitive information. The types of information breached included demographic, clinical, and financial information.

[Read more](#)

STAYING EVEN KEEL: STEADYING THE SHIP IN STORMY WATERS

-  **Update** your business associate inventory
-  **Conduct** a business associate agreement review and update contracts with vendors
-  **Prioritize** and tier vendors for business criticality and compliance risks
-  **Invest** in your third-party risk management program, leadership, and team
-  **Prioritize** vendors for assessment and remediation
-  **Report** on vendor risk across the entire vendor portfolio
-  **Evaluate** and limit privileged access for third parties
-  **Validate** controls and gain assurance via assessment data
-  **Track** KPI, KRI, and SLA metrics on vendor risk program performance
-  **Incorporate** vendors into incident response simulation exercises
-  **Prepare** and practice a communication plan to customers for business associate incidents
-  **Monitor** and adopt emerging supply chain regulations and standards
-  **Explore** managed services for vendor risk and business associate compliance
-  **Automate** third-party risk management processes

Meditology specializes in HIPAA compliance and third-party risk management for healthcare entities. Contact us to learn more about our related services including:

-  Business associate inventory management
-  Vendor risk management program development
-  Vendor risk management managed services
-  Healthcare vendor risk data exchange, powered by [CORL Technologies](#)
-  HIPAA business associate compliance assessments

Meditology Services is a top-ranked cybersecurity, privacy, and risk consulting firm dedicated to the healthcare industry.

Contact us to learn more about how we can help you and your program stay afloat in 2022.