imprivata

Rising data breaches in healthcare: Protect yourself against vendor and third-party cyberattacks

We see data breaches and cyberattacks in the headlines every day – so often that it's easy to become numb to it, or to tune it out like background noise.

Until it happens to your organization.

Now is the right time to tune back in to cyber risk, and in particular, the ways your third parties and vendors might be putting you at risk of a data breach.

Hospitals spend 64% more on advertising after a data breach in an effort to repair their image and minimize patient loss to competitors.

Healthcare's vulnerability to cyberattacks

Healthcare is the most targeted industry for cyberattacks, and it's the industry with the highest costs – up to nearly $11 million in 2023. Attackers want the protected health information (PHI) that providers and business associates have, as it's often worth more than credit card info or other types of personally identifiable information (PII).

The reality is that it only takes one vendor or third party with unsecured network access to open the door for your company to make headlines for all the wrong reasons.

Let's look at a few recent third-party breaches that highlight this risk.

Perry Johnson & Associates

While you may not be familiar with medical transcription vendor PJ&A, you likely have heard of the breach that impacted their customers Northwell Health, Mercy Health, and Cook County Health, among others. To date, almost 9 million patients have been impacted by this vendor breach – the second-largest healthcare data breach in 2023, and the 6th largest ever. Compromised PHI included names, birthdates, Social Security numbers, addresses, medical record numbers, hospital account numbers, admission diagnoses, and times and dates of service.

So, what exactly happened?

PJ&A's investigation discovered that there had been unauthorized access to its network and client data between March 27, 2023, and May 2, 2023. A breach of this size not only impacts customer/patient retention and reputation but also leads to class-action lawsuits against both the vendor and healthcare provider. In the case of PJ&A, over two dozen lawsuits have already been filed against both vendor and healthcare providers.

Broward Health

In 2021, Broward Health in Florida suffered a data breach which compromised the PHI of over 1.35 million patients. So, how did the breach occur?

The bad actor gained access to Broward Health's network through one of their third-party medical providers. The third party had been granted legitimate access to Broward's network to provide services. But through this third party access point, a bad actor was able to steal sensitive employee and patient data like names, birthdays, addresses, banking information, Social Security numbers, drivers' license numbers, patient histories, and treatment and diagnosis records.

Advanced Medical Management

Another recent third-party data breach occurred at Advanced Medical Management, a provider of operational, administrative, and technical healthcare management services. The May 2023 cyberattack resulted in the exposure and possible theft of PHI belonging to 319,485 individuals.

How? Again, Advanced Medical Management was made vulnerable through a third-party vendor.

This vendor worked with Advanced Medical Management to design and maintain parts of its network, and attackers used that legitimate access point to illegally access databases containing PHI. Multiple class-action lawsuits have been filed against Advanced Medical Management, citing the organization's inadequate cybersecurity and failure to notify impacted individuals in a timely manner.

Safeguarding third-party access

These are just three examples among many recent breaches that highlight the risks that third parties and vendors pose to healthcare providers. While third-party services are necessary for business operations and patient care, the privileged access they have poses real security risks if not appropriately secured.

The time to secure your vendor and third-party access is now – not after an incident occurs.

Contact our team to request a demo of Imprivata Vendor Privileged Access Management.

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

1826-2024_VPAM-snippet-rising-data-breaches-healthcare