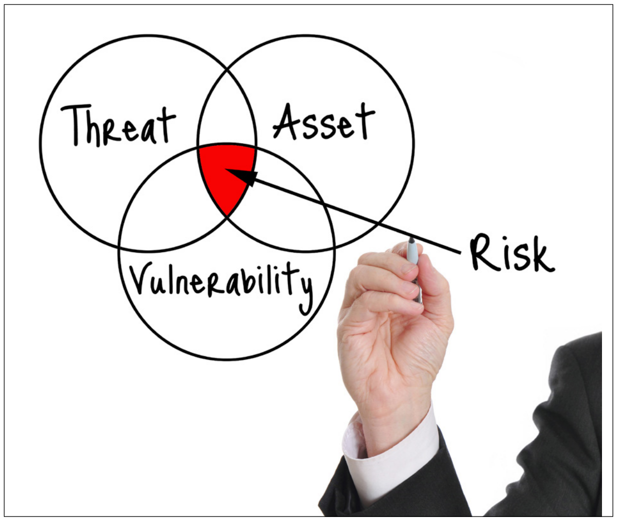
Understanding Your Risks and Exposure When Taking Electronic Payments and Storing Credit Card Data

LabCorp, Quest Diagnostics data breach a wake up call to medical collections industry

The massive data breach experienced by LabCorp and Quest Diagnostics appears to have exposed the personal and financial data of between 8 million and 12 million patients. The aftermath of the breach is certain to draw increased focus on the data security practices of companies that provide billing collection services to healthcare organizations and healthcare providers themselves.



Healthcare providers, medical billing offices, and the vendors providing the collection software and payment applications that take, store and send payment information for processing, all should look at this recent breach as an opportunity to reassess their data security.

Is hosting and managing payment data yourself worth the risk?

The recent data breach took place on an internally developed payment application. Are you currently taking payments through collection software or a payment site you manage, and does it include P2PE certified solutions? If so, have you ever conducted a cost analysis and risk assessment to determine whether maintaining complete data liability exposure makes financial sense?

How confident are you in your payment and software vendors?

If using a third party service, is your collection or billing software storing or passing through credit card data? Is it a P2PE certified solution? In either case, that data must be encrypted.

For example, if you're able to see or export stored credit card data in clear text, that data is not encrypted—which makes you (and your clients) vulnerable to cyber criminials. Capturing, passing, or storing unencrypted credit card data makes a company financially liable in the event of a data breach.

Verifying your payment application or software vendor's compliance to Payment Card Industry (PCI) Standards

As a merchant, you've already completed some version of a PCI Attestation of Compliance (AOC) form where you've declared that you know and have "confirmed" the payment application capturing, transmitting and storing credit card data is PCI compliant. How was this information confirmed?

Can your vendor provide you with proof they've undergone a third-party audit from a PCI Qualified Security Assessor (QSA)? Can they provide a copy of their Report on Compliance (ROC)?

Your payment solution vendor may have never undergone a third-party audit

Third-party audits and penetration testing are only required for Level 1 providers (those who exceed 6 million transactions a year). This means many payment solution providers achieve their PCI-DSS compliance through self-assessments.

A proper risk analysis should consider the level your payment software provider is willing to go to ensure your client or patient's sensitive personal and financial data is secure.

In other words, are you willing to risk the personal and financial data of your patients to a vendor who filled a self-assessment form, or one who has submitted their software and entire network to a third-party audit, penetration testing, and year-long monitoring by a Qualified Security Assessor?

To learn more about our PCI-DSS and HIPAA HiTRUST Certified Payment & Communication Solutions:

Call: 1.800.214.7490

Click: Solutions

hello@intelligentcontacts.com