ACUPUNCTURE Today

YOUR PRACTICE

HIPAA-Compliant Online Payment & Billing

WHICH ONE DO YOU USE (AND HOW COMPLIANT IS IT)?

David Bibbey, Dipl. Ac., LAc

There are countless ways protected health information (PHI) could be exposed during a financial transaction. All health care providers should be mindful that the most valuable consumer data being stolen, shared or sold is found in patients' health care records.

When a company offers a low-cost or free software, applications or services that involve using or storing patients' data, clinic owners need to be extra careful that these companies are HIPAA compliant and willing to sign a Business Associate Agreement (BAA). Companies offering free services often profit from sharing and selling patient data. They want access to your patient data; that's why they provide free services.

The following is a review of the most popular online billing and payment services. Let's see how they compare when it comes to HIPAA compliance.

Square

Square's website states that it uses data encryption within its card reader to protect the "swipe." It also provides 24/7 security monitoring for all payments and boasts PCI compliance.

So, Square meets HIPAA security standards, but this does not guarantee HIPAA compliance. A service provider must also sign a BAA with its users. Square's website specifically addresses HIPAA compliance and includes a link to its HIPAA Business Associate Agreement, so it is reasonable to assume Square signs and provides BAAs for users.

Conclusion: Square is HIPAA compliant, provided that users have a signed BAA with Square before using the service.

Zelle

Zelle requires users to enter their email address and phone number to send payments. Patients' email addresses and phone numbers are HIPAA protected health information (PHI), if connected to treatment, payment or health care operations.

Zelle's website states that it implements user authentication and monitoring features to ensure the security of payments sent through its service. So, Zelle meets HIPAA's requirements for security, but there is no mention of HIPAA Business Associate Agreements. It is reasonable to assume that Zelle does not sign BAAs with its users.

Conclusion: Zelle is not HIPAA compliant. While it does implement security measures to keep user data safe, it does not sign BAAs.

PayPal

PayPal is the world's largest payment processor. In 2021, it processed over a trillion dollars in payments. Its security protections include 24/7 monitoring, fraud detection, firewalls, and encryption.

PayPal collects at least nine of the 18 types of data that are considered PHI. That's a problem

because, while its privacy policy states that it does not sell data, it admits sharing data with "other members of the PayPal corporate family, including our brands such as Venmo and, service providers that help us with processing payments, marketing, research, compliance, audits, corporate governance, communications, and security."

Conclusion: PayPal is not HIPAA compliant. Its security features seem to be sufficient, but health care practitioners have no control over how PHI would be used, and there is no BAA available. Using PayPal is a HIPAA violation just waiting to be discovered in an audit.

Venmo

Venmo is a subsidiary company of PayPal. Both companies share data with each other. This creates gray areas that can cause concern regarding HIPAA compliance. Venmo admits that it uses personal data for internal marketing purposes. It also confirms that it shares data for joint marketing with other financial companies. It also shares date with: "Our parent company, PayPal, Inc., and affiliates and subsidiaries it controls."

Venmo doesn't mention BAAs or HIPAA anywhere on its website. It claims status as a financial institution and therefore does not sign Business Associate Agreements.

Conclusion: Venmo is not HIPAA compliant. Venmo uses data that is considered PHI for marketing purposes. Venmo shares data with PayPal, which also uses data that is considered PHI for marketing purposes. HIPAA compliance standards strictly forbid this practice. It also does not sign BAAs. Any of these three reasons is enough to qualify as noncompliant. That means your clinic would be liable for any breach resulting from Venmo's actions.

Stripe

Stripe is a payment processor and much more. It features a robust suite of applications covering everything from identity verification to help starting a new business online. Its security measures are outstanding, including meeting the standards of the European Union's General Data Protection Regulation (GDPR).

Like PayPal and Venmo, its does use personal data for promotional purposes. It shares this data with its affiliate companies and third-party companies that provide services to Stripe. There is no mention of HIPAA or BAAs on its site. Because of that, it's safe to assume it doesn't sign or offer them.

Conclusion: Stripe is not HIPAA compliant. There are a lot of reasons to like Stripe, but the risks do not appear to outweigh the benefits. Transmitting ePHI without a signed BAA is an automatic violation of HIPAA regulations.

So, Is Your Payment Software HIPAA Compliant?

Of the five best-known online payment processors, only Square clearly and definitively is HIPAA compliant. This is not an exhaustive list of all options available in the marketplace. If you use a processor not listed, make sure you closely review its user and privacy agreements for specifics related to PHI privacy and security.

Author's Note: For more information related to this article, please visit www.patientdataprotection.com or call Matthew Fiorenza, compliance and security specialist, at 352-268-5088, ext. 4.