Storing patients' credit card information: Keep it safe

Kaustubh G. Joshi, MD

Credit cards have made it easier for psychiatrists who work in outpatient settings to collect payment for their services. Accepting credit cards saves time in sessions for clinical matters, leads to higher rates of collecting payments for patients who do not show up for appointments, and avoids having to manage bounced checks and collection agencies.[1] No federal or state laws prohibit businesses from storing consumers' credit card information. However, psychiatric practices are legally obligated to have safeguards in place to protect sensitive information and limit liability exposures.[2] There are several steps to take when storing your patients' credit card information.

Establish a payment policy. Create a policy that outlines your practice's credit card procedures, including when credit cards will be charged and under what circumstances, how patients will be notified, and how credit card information will be stored.[2] Give your patients a copy of this policy and review it with them at their first appointment and any time you change this policy.[2] Get consent from your patients before using and storing their credit card information.[2]

Use secure methods to store this information. Most medical practices photocopy/write down their patients' credit card information and store it in the patient's electronic/paper medical record, or they use an online service to store it electronically.[2] Online services usually provide a higher level of protection than the patient's medical record.[2] Ensure that electronic data that includes credit card numbers is robustly encrypted, or that paper records are locked in a secure place, such as in a safe or file drawer that requires a key/combination lock.[3] Payment Card Industry (PCI) regulations prohibit storing a credit card's security code (a three- or four-digit number on the front or back of the card).[3] This code is used to allow merchants to verify whether a customer authorizing a transaction over the phone or via the internet physically possesses the card.[3] PCI regulations also prohibit storing data contained in the card's magnetic strip.[3] This data contains information about the account that is not displayed on the card, assists with authorizing transactions, and ensures that credit cards cannot be easily counterfeited.[3]

Understand all federal and state laws and regulations. If your practice collects patient billing information, you are considered a "merchant" and are subject to federal and state laws and regulations that protect consumer credit card information.[2] These laws and regulations include (but are not limited to)[2]:

- Health Insurance Portability and Accountability Act (HIPAA) and similar state privacy laws

continued

Dr. Joshi is Associate Professor of Clinical Psychiatry and Associate Director, Forensic Psychiatry Fellowship, Department of Neuropsychiatry and Behavioral Science, University of South Carolina School of Medicine, Columbia, South Carolina. He is one of Current Psychiatry's Department Editors for Pearls.

Disclosure

The author reports no financial relationships with any companies whose products are mentioned in this article, or with manufacturers of competing products.

doi: 10.12788/cp.0134

Psychiatric practices are legally obligated to have safeguards in place to protect sensitive information

- Federal Trade Commission Act (FTCA) and similar state business laws
- Payment Card Industry Data Security Standard (PCI DSS), which was not devised by federal or state government.

HIPAA and state privacy laws require psychiatrists to implement "reasonable" security measures to protect payment information, regardless of how that information is stored.[2,4] Because HIPAA does not define "reasonable," psychiatrists have latitude in determining which security measures to implement.[2,4] Locking the information in a file cabinet and locking the room where the file cabinet is kept (for paper storage) or using HIPAA-compliant encrypted storage programs (for electronic storage) are examples of "reasonable" security measures.[2]

FTCA requires businesses to use "appropriate" and "reasonable" security measures to protect credit card information.[2,5] Because FTCA does not specify these terms,[2,5] psychiatrists have leeway in determining which security measures to implement. Federal law requires all businesses to delete a card's expiration date and shorten the account information to include no more than the last 5 digits of the card number that is printed on all sales receipts.[6] FTCA also requires businesses to get prior authorization from individuals before charging their credit card.[2] For example, if a patient previously used a credit card to pay for a session, the psychiatrist cannot later use the credit card to charge for a missed appointment without notifying the patient and getting their authorization.[2]

PCI DSS applies to entities that store, process, and/or transmit cardholder data.[7] Any business that accepts credit card payments must comply with PCI DSS, which includes 12 requirements.[7] Examples of these requirements include using firewalls to protect cardholder data and restricting access to cardholder data to a "need-to-know" basis. Businesses that do not comply with PCI DSS can be subjected to fines and/or have their contracts terminated by the credit card companies.[2] Fines can range from $5,000 to $100,000 per month for data breaches where you are found negligible.[1]

References

1. Braslow K. Benefits and costs of accepting credit cards in your practice. Current Psychiatry. 2017;16(5):17,29.
2. Wertheimer M. Keeping patient credit card and payment information on file. Psychiatric News. 2019;54(11):8.
3. Hephner L. 5 tips for proper handling of credit card information. Accessed April 22, 2020. https://paysimple.com/blog/5-tips-for-proper-handling-of-customer-credit-card-account-information/
4. Health Insurance Portability and Accountability Act of 1996. Public Law No. 104–191, 110 Stat. 1936 (1996).
5. Federal Trade Commission Act of 1914. 15 U.S.C. §§ 41-58, as amended (1914).
6. Federal Trade Commission. Slip showing? Federal law requires all businesses to truncate credit card information on receipts. Accessed April 22, 2020. https://www.ftc.gov/tips-advice/business-center/guidance/slip-showing-federal-law-requires-all-businesses-truncate
7. PCI Security Standards Council. Accessed April 22, 2020. https://www.pcisecuritystandards.org/

Discuss this article at www.facebook.com/MDedgePsychiatry