

# PCI (Payment Card Industry) Compliance For Healthcare Offices

By Ron Barnett

Dr. Svenson thought he was doing both his patients and his practice a big favor when he started setting up monthly payment arrangements using patient's credit cards. All he had to do was have his staff get the card numbers from patients and then run a payment each month against those cards. It was a great, simple plan UNTIL... someone from his nighttime cleaning crew found the card list.

Now Dr. Svenson is faced with reimbursing \$475,000 in fraudulent credit card charges and paying another \$1,800,000 in court costs, costs associated with reissuing cards, fines and fees- all because one sheet of paper was picked up by a dishonest person. Now he can no longer accept credit cards of any type and has lost the respect of his patients and community. How could that happen to an honest man?

Actually- it didn't. Dr. Svenson is fictional. But it easily could have happened and did happen to one of the nation's largest retail firms, TJ Maxx. Credit card information was stolen from them and now financial analysts estimate the cost of that security breach may exceed one billion dollars.

But how does that relate to you, the owner of a private healthcare practice? You don't have millions of credit card numbers on file. Until recently, credit card security was really a non-issue for small businesses like private healthcare practices. However, that safe haven for small merchants no longer exists.

*"Data security breaches involving payment card information occur at small businesses more frequently than at all other merchant levels combined,"*

Michael E. Smith, Senior Vice President,  
Enterprise Risk and Compliance, Visa  
USA.

Before 2004, each of the card companies had separate guidelines for securing credit card data. Those guidelines were targeted mainly at the card processing vendors, the companies you send your card transactions to. In 2004, all the major card networks consolidated their compliance requirements through the formation of the PCI Security Standards Council. By 2006, the Security Council had implemented new standardized guidelines that covered not only the card processing companies, but merchants like you who accept credit cards as well.

These guidelines cover not only large merchants that accept millions of transactions per year, but EVERY merchant, even smaller businesses such as healthcare practices, who accept only an occasional credit card payment. The Security Council felt the need to respond to the fact that 80% of card theft occurs in small business, NOT in the card processing companies or large merchants. So, as of July, 2006, the various levels of merchants were redefined and a new level (Level 4) was created to include all merchants processing less than 1 million card payments per year. These requirements are centered around the **storage** and **transmission** of credit card information and **access** to that secure information.

## **Data Storage and Access**

In a healthcare office, sometimes card data is stored in a computer program such as a practice management system on the computer in their office or on a remote web server. Other offices store the card data on paper for use in processing future transactions for the patient, such as in an automatic payment plan or via a traditional "tickler file". Regardless of whether credit card data is stored on electronic media or on paper, it is the responsibility of the healthcare provider to assure that this confidential data is stored in a manner that meets PCI requirements and that required scheduled security audits occur.

The strictest of these PCI requirements are aimed at making sure that small businesses are not storing prohibited cardholder data after the initial transaction has been processed. According to Michael E. Smith, Senior Vice President, Enterprise Risk and Compliance, Visa USA, "This is precisely the kind of data most sought by hackers because of its use in counterfeiting payment cards. Merchants who store this sensitive data are placing their businesses in the cross-hairs for today's data thieves."

Aaron Biddar, President of ControlScan, a leading provider of e-commerce security services points out that, "Usually, Level 4 merchants do not have the technical expertise, nor the IT Staff, to properly secure card holder data. For all data breaches, you have two main risks: The internal risk-an employee obtaining a file that they shouldn't have, and an external risk-a hacker."

"A hacker is going to look for the path of least resistance. Level 1 and 2 merchants can afford to button up their IT infrastructure, because they have the money to do so; they can afford to staff a huge IT department, and they don't want to be a headline in the news. So, if I am a hacker, I'm going to go to the merchant that I know cannot afford the proper security or staff to mitigate that type of breach," he finished.

Hackers are not the only threat that must be addressed. Far too often, offices do exactly what the fictional Dr. Svenson was doing. It is not at all unusual to see a list of patient credit card numbers stored for running monthly payments, written on a sheet of paper and filed in an unlocked desk drawer or filing cabinet. In that situation, a dishonest co-worker or a member of the nighttime cleaning crew can easily steal the list and go on a spending spree. And who is responsible for the losses incurred by the card holders and the card processing companies? In a growing number of states, that liability now falls squarely on the shoulders of the merchant, or in your case, your Practice!

***"Regardless of whether credit card data is stored on electronic media or on paper, it is the responsibility of the healthcare provider to assure that this confidential data is stored in a manner that meets PCI requirements and that required scheduled security audits occur."***

And the liability does not stop with covering the fraudulent charges. Any related court costs, the costs of the card processing company in contacting the card holder and replacing old cards that are no longer usable, fines and fees from the card processor and fines from your state government can all add up to an amount much greater than the card liability itself.

Healthcare practices, therefore, should not make the false assumption that thieves will only concern themselves with hacking into large merchants or bank card networks. The card data stored in a healthcare office can be just the kind of low hanging, easily accessible fruit that the data thief is looking to pick.

### **Data Transmission**

The card data must be transmitted to the card processor using a secure method. Most healthcare providers process transactions by sliding the card through a telephone based card terminal. The terminal transmits the payment to the card processor through a secure telephone connection. If you are processing only "card present" transactions and using a card terminal from one of the major terminal providers such as Verifone or Hypercom, you should feel confident in knowing that the data transmission has been secured.

If card payment data is being transmitted across the Internet, then it must be sent through a secure encrypted transmission (for example, SSL/TLS or IPSEC). If you are not sure what these are or whether your card processor vendor is using secure encryption for the transmission of your card payments, ask them. Remember that ultimately, it is your responsibility to protect the integrity of your patients' credit card information.

### **What is involved in being PCI compliant?**

This is not an easy question to answer. First, it depends on the size of the merchant.

Almost all private healthcare practices, though, fall into the least regulated category- Level 4. (Level 4 merchants process less than 20,000 e-commerce transactions and less than 1,000,000 card transactions per year). Once an office has had a data breach, it is automatically promoted to Level 1 compliance, which involves regular on-site audits by a Qualified Security Assessor, which can easily cost \$10,000 to \$25,000 per year. So it pays to make sure that card data, if it must be stored at the office, is held in a very secure manner.

#### **The 12 Requirements for PCI Compliance**

##### **Build and Maintain a Secure Network**

- \* Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- \* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- \* Requirement 3: Protect stored cardholder data
- \* Requirement 4: Encrypt transmission of cardholder data across open, public networks

##### **Maintain a vulnerability management program**

- \* Requirement 5: Use and regularly update anti-virus software or programs
- \* Requirement 6: Develop and maintain secure systems and applications

##### **Implement strong access control measures**

- \* Requirement 7: Restrict access to cardholder data by business need-to-know policies
- \* Requirement 8: Assign a unique ID to each person with computer access
- \* Requirement 9: Restrict physical access to cardholder data
- \* Requirement 10: Track and monitor all access to network resources and cardholder data
- \* Requirement 11: Regularly test security systems and processes

##### **Maintain an information security policy**

- \* Requirement 12: Maintain a policy that addresses information security for employees and contractors

This represents only an outline of the PCI DSS requirements. For more details, go to

[https://www.pcisecuritystandards.org/pdfs/pci\\_audit\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf)

Even for Level 4 compliance, the requirements are not easy to meet and maintain. For example, Requirement 9 states that offices that store card data should "Restrict physical access to cardholder data." On the surface that sounds like a simple enough requirement-lock the data away in a safe place. However, the detailed requirement specifies the level of physical security required which includes, among other things:

- Secure video surveillance cameras that are monitored at all times
- Storage of the surveillance videos for at least three months
- An employee and visitor badge system. All people entering the office must wear a badge at all times. The office has to make sure that every visitor entering the facility signs into a log, signs out upon exit and surrenders the visitor badge.
- Restrict access to any room where there is an available network jack. Visitors can never be left alone in a room where there is a network jack that could be plugged into.

Understand that these are just 4 of 24 specific requirements within "Requirement 9" and "Requirement 9" is one of the simplest of the 12 requirements.

The bottom line is this... Don't store customer card data unless you are willing to take on major data security responsibilities and liabilities.

### **Why Comply?**

What happens if a practice chooses to ignore the security requirements set forth by the PCI Security Council? There are several possible outcomes:

1. It's possible that nothing may happen. The PCI SSC is not a police force and has no one going from office to office to make sure that every policy is enforced. As long as an office does not have a breach of security, they do not need to fear that the PCI SSC will come knocking at their door.
2. If a breach does happen, several unpleasant things will likely occur.
  - A. You could permanently lose your ability to accept credit cards. For many practices, that alone would be a devastating consequence.
  - B. You could be faced with thousands of dollars in fines and penalties from your card processor.
  - C. If the breach causes a financial loss to your patients and/or the card processing company, then you could be held responsible for 100% of the loss. If someone steals a group of card numbers and then runs charges against them, the patient will typically only be held responsible for \$50. But your office can be sued for 100% of the damages.
  - D. You could face criminal and/or civil penalties from your state government. Minnesota has already passed legislation making the regulations established by the PCI SSC have force of law. Similar legislation is being actively pursued in Texas, Illinois and several other states.
  - E. You could lose the confidence of your patients and the respect of your community.
  - F. Credit card numbers are considered part of the private patient information that HIPAA expects to be kept confidential. So a breach in credit card security in a healthcare practice carries with it the added consequence of not maintaining the security of private patient information.

## Summary - What Should I Do About This?

Offices that are storing patient credit card numbers (even if the storage is just on paper or in your practice management software), should follow the guidelines outlined by the PCI SSC for securing this information. (A detailed security audit checklist can be found on the Web at [https://www.pcisecuritystandards.org/pdfs/pci\\_audit\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf).) The guidelines for a merchant that stores card data include regularly scheduled security audits and compliance reporting to the card processing company. These security requirements go far beyond what is considered practical and do-able in a healthcare office, so the easiest policy to implement is simply to not store any credit card data in the office. A thief cannot steal information that is not there, so data storage related requirements become irrelevant.

If the Practice is storing card information in practice management software, is using a software program that transmits the card transaction across the Internet or through a wireless connection, or storing the card information in any type of computer file, then the PCI requirements DO apply. If that is the case, then contact the vendor who supplied the program that stores the data and ask them to provide documentation supporting their compliance with PCI regulations. However, keep in mind that even if the software vendor can verify the security of the data within their data files, your office still has to comply with the physical security regulations such as video surveillance and a visitor badge system as well!

The bottom line is this...

Don't store customer card data unless you are willing to take on MAJOR data security responsibilities and liabilities.

If the office is using a card terminal that processes the payment through a phone line, make sure that the terminal does not print the patient's credit card account number on the receipt. If it does, then either destroy the merchant copy of the receipt or have the vendor assist in changing the terminal parameters so that the card number is hidden on the receipt.

The card processing vendor also plays a key role in making sure that the practice stays within PCI guidelines. Talk to your vendor representative about these issues. If you don't feel confident that they are taking the issue seriously, then consider the option of finding a vendor who does. Ultimately, security compliance is YOUR responsibility. MasterCard, VISA, Discover, American Express, and most importantly, your patients have placed their trust in you to protect this information. Don't let them down.

*Ron Barnett is the President of Complete Systems, Inc. (CSI). CSI's payment processing division, DOCPAY, is one of the leading companies in the U.S. in providing automatic monthly patient payment plans for healthcare offices. Additional information can be requested by calling DOCPAY at 800-936-2729, by email at [info@docpay.com](mailto:info@docpay.com) or on the web at [www.docpay.com](http://www.docpay.com).*