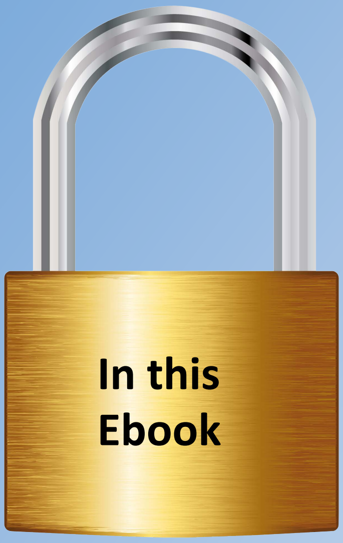
2nd Edition

A Pharmacy Owner's Guide to Point-of-Sale Security

Basics for protecting your pharmacy in today's technology landscape

Retail Management Solutions
The industry leader in pharmacy point-of-sale innovation



Introduction to POS Security

Chapter 1: What are you protecting?

Chapter 2: PCI Compliance

Chapter 3: EMV and more

Chapter 4: Passwords

Chapter 5: Virus protection

Chapter 6: The www. challenge

Chapter 7: Good common sense habits

An Introduction to Security

Technology allows us to do so many wonderful things, but for each measure of good, there is also a flip side. Someone out there who can and will use technological advancements to cause Irreversible damage to our businesses. We've all heard the stories of security breaches resulting in compromised personal information, credit card fraud and even stolen identities. If you've never been impacted by a breach, those stories probably seem far removed from daily life and the likelihood that your business will be targeted seems slim.

I could give you a hundred different statistics on why this isn't true, but I think that George Eliot says it best in his book 'Silas Marner'.

"The sense of security more frequently springs from habit than from conviction, and for this reason it often subsists after such a change in the conditions as might have been expected to suggest alarm. The lapse of time during which a given event has not happened, is, in this logic of habit, constantly alleged as a reason why the event should never happen, even when the lapse of time is precisely the added condition which makes the event imminent. A man will tell you that he has worked in a mine for forty years unhurt by an accident as a reason why he should apprehend no danger, though the roof is beginning to sink; and it is often observable, that the older a man gets, the more difficult it is for him to retain a believing conception of his own death."

These words may date back to 1861 but they strike a very relevant chord in today's technology landscape. Just because you've never fallen victim to a security breach or identity theft before, doesn't mean it won't ever happen to you. And complacency when it comes to your pharmacy's security will only increase your risk. In this E-Book, we'll explore some of the major security concerns plaguing point-of-sale technology today and talk about some of the steps that you can take to safeguard yourself and your business in an ever more threatening world.

Chapter One

In the pharmacy industry, you have a plethora of information that could seem like a veritable gold mine to someone with ill intentions. Basically, you have a lot to lose should your business be breached.

As a healthcare practitioner, you have access to some information about your patients and customers that can be pretty personal. This information is generally known as PHI (Personal Health Information) and PII (Personally Identifiable Information). Different systems in your pharmacy may contain this type of information, such as medical history, prescription information, social security numbers, driver's license information and more. Protecting this information is of paramount importance to help safeguard your customers against potential identity theft.

Enabling proper security measures, will not only help to protect customer information and credit card information, it will also protect your stores image and the integrity of your brand. In a 2013 poll, pharmacists were voted as the second most honest profession in America. Words like reliable and honest are often the most accurate descriptors for how people feel about their local independent pharmacy. But one misstep in how your security is managed could mean a potential breach and a significant loss of trust by your customer base.

Major retailer Target will be recovering for a long time to come after the December 2013 breach that resulted in theft of personal information for as many as 70 million customers and theft of credit and debit card information for more than 40 million customers. In this article from the New York Post, predictions spread far and wide as to how long it may take Target to recover from this blow to their credibility.

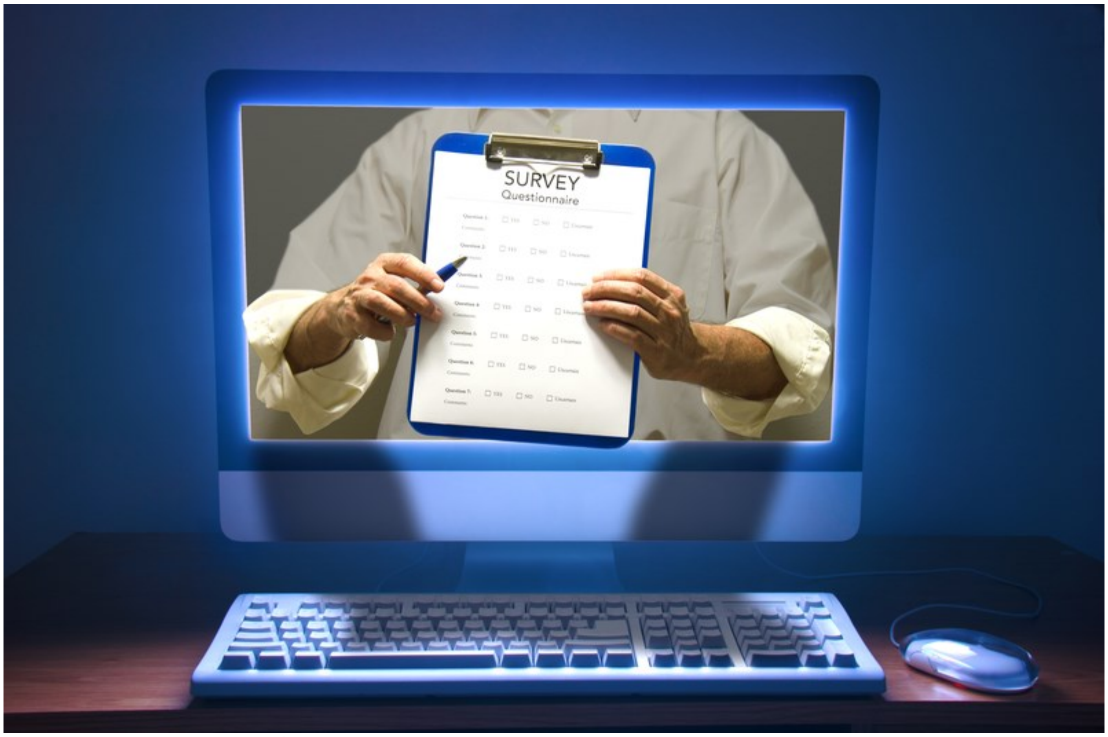
As a merchant that processes credit cards, you should also be familiar with PCI or Payment Card Industry Compliance. Each year countless and ever increasing numbers of merchants are breached, resulting in the theft of credit and debit card information. PCI Compliance is a requirement for merchants to certify that they follow recommended and required guidelines for protecting credit and debit card information. We'll talk about PCI Compliance more in the next chapter, specifically as it relates to pharmacy point-of-sale.

Chapter Two

PCI Compliance has become a necessity for merchants over the past few years. Protecting your customers credit card information is one of the most important things you can do to safeguard the integrity of your businesses reputation.

Before Target experienced its breach in 2013, T.J. Maxx made headlines in 2007 with a massive theft of credit and debit card information for more than 45 million consumers. At the time, it was believed to be the largest data breach of its kind in history. This breach, along with countless others, set the wheels in motion to reform security in the credit card industry.

Payment Card Industry Data Security Standards (PCI DSS) are a set of regulations, standards and requirements put in place for the secure processing of credit and debit cards. Simply put, the payment card industry as a whole believes that following these standards greatly lessens a merchant's risk of experiencing a breach.



Becoming Compliant:

In a general sense, the Payment Card Industry (made up of major industry players such as Visa, MasterCard, American Express, Discover) passes on responsibility for meeting PCI DSS to credit card processors and acquirers such as First Data, Heartland, Elavon etc. Generally those processors pass that responsibility on to the merchant. Every processor handles PCI for their merchants a little differently. Some will pro-actively contact you and assist you with the process to comply with these regulations and become what's known as PCI Compliant. Some will assume you're on the ball and say nothing, leaving you to begin and complete the process on your own. If you haven't heard from your processor about PCI Compliance you should reach out to your credit card representative and ask them what your PCI status is and what their process is to assist you with certification. The process generally consists of completing a Self-Assessment Questionnaire (SAQ) and scheduling quarterly scans that will test for vulnerabilities in your network and firewall.

Enlisting your technology providers to help:

Unfortunately the path to becoming PCI Compliant is not an easy one. Many of the questions asked in the SAQ will seem like they are written in a foreign language. Your Point-of-Sale Provider should be able to assist to a certain degree. Each service provider must certify to meet their own version of PCI DSS called PA DSS, or Payment Application Data Security Standards. If you utilize integrated credit cards through a certified POS system, your provider may be able to assist with a certain percentage of the questions on the SAQ. Beyond how your POS system handles credit card data, the SAQ also covers network security, store policy & procedure and a few other miscellaneous areas. It is always helpful to be in contact with whatever party manages your network and firewall to obtain advice on complicated security questions. No single provider can answer all of the PCI SAQ questions for you, but they may be able to help make the road to getting there a little less rocky.

If you choose not to certify:

While an anvil isn't likely to fall from the sky if you do not complete the steps necessary to become PCI Compliant, you'll probably eventually see some form of consequence. Today, many processing companies charge a non-compliance fee for merchants that have not yet completed a PCI Certification. On the more severe side of things, failing to be compliant can have some pretty bad repercussions if you are to experience a breach. It's impossible to say what exactly would happen as the reason and severity of the breach are always taken into account, but breaches could result in anything from fines from the PCI standards board all the way to a loss of card processing privileges. Needless to say, at RMS, we believe it's better to be safe than sorry.

Stay tuned to the remainder of this e-book as the tips and advice provided throughout the remaining chapters will help you on your road to PCI Compliance.

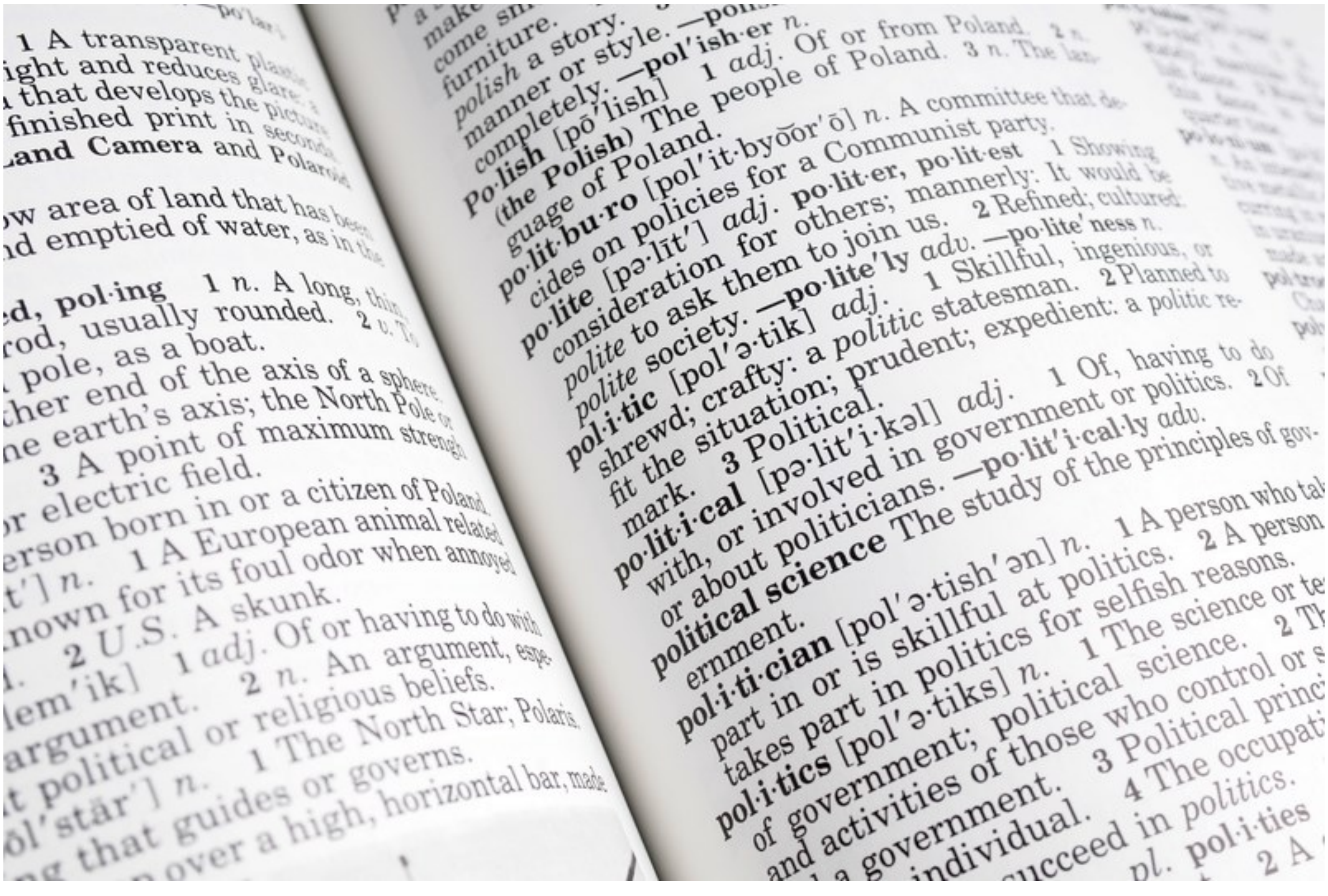
Chapter Three

Countless data breaches costing billions of dollars every year have prompted the credit card Industry to introduce new practices that they are hoping you'll adopt to minimize the risks both to their bottom line and yours. The information in this chapter is here to help you understand what these changes mean to your pharmacy.

Important Terms:

EMV: EMV stands for “Europay Mastercard Visa”. EMV technology was first implemented in Europe in 1995. EMV cards have an embedded microchip that creates a unique transaction code each time the card is used. This sharply contrasts to a standard card with a magnetic strip that contains constant and unchanging data. You may also hear EMV referred to as Chip and PIN, but EMV cards are more likely to be used in a signature based transaction during the early stages of EMV rollout in the United States. EMV prevents a card from being physically duplicated, which protects the card brands and acquirers, but it does not protect against data breaches. Additionally, EMV has no bearing on the scope of PCI Compliance.

P2PE: Otherwise known as Point to Point Encryption, P2PE virtually eliminates the chances of a data breach like the ones experienced by Target, Home Depot, and countless other retailers. With P2PE, when the card is swiped, it is encrypted by the hardware device and sent directly to the processor where it is decrypted for the first time. The only information returned to the POS system is an approval or decline, meaning there’s no credit card information in your POS system to be compromised. Additionally, P2PE dramatically reduces your scope for PCI Compliance.



Frequently Asked Questions:

Do I have to adopt EMV? EMV is not a requirement. While many news articles will tout October 2015 as a deadline for adoption of EMV, it's actually just the date when credit card brands agree to shift fraud liability from you to them on EMV transactions. This is a liability that you carry today and the liability shift only applies to EMV cards. Adopting EMV is a choice, and the decision is completely up to you. Think of the October 2015 date as an incentive offered by the credit card brands to get you to adopt this technology.

What is the best way to protect my pharmacy from a credit card data breach? Because EMV will not actually reduce your risk of a credit card data breach, we recommend Point to Point Encryption as the most secure option for processing credit cards in your pharmacy. Since no credit card data is stored in your POS system, the chance of a breach due to stored credit card information is virtually eliminated.

Where can I get more information? Check out the latest articles posted on our special website devoted to EMV and credit card security at www.rm-solutions/emv for the most up to date information on EMV, P2PE and implementation of these solutions. At RMS, we are working diligently with our processing partners to provide options for implementation of EMV and P2PE. RMS customers will also be receiving monthly updates via email and quarterly updates by mail beginning in February of 2015.

Chapter Four

Remembering passwords for all of the different applications that you have to log in to each day can feel like some bizarre game of Memory. "Match the right application with the right passwords and do it in 3 tries or less or you're locked out!" And while that may sound like some lesser form of torture, if you're in that situation, it probably means you're following at least some best practices for password security.

Password Management:

If secure passwords aren't really something you deal with on the daily basis, it's time to make some changes to your password management policies. Here are our best practices for password management.

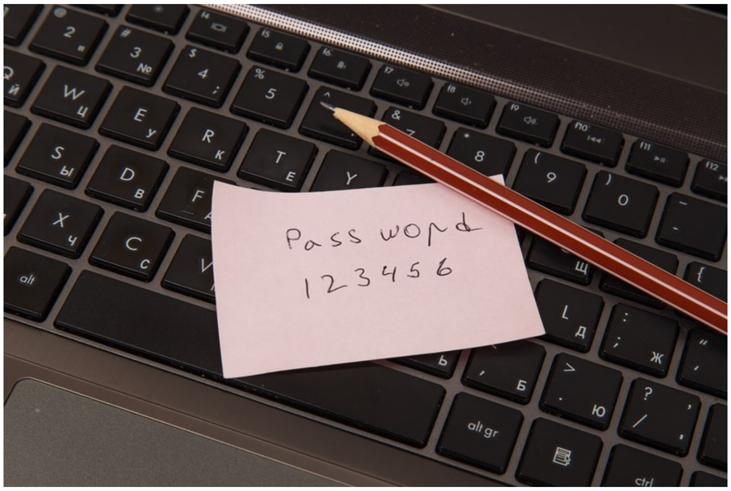
⇒ If you are using a generic, easily guessed password, such as "123456" or "password" you need to change it immediately. Check out this list of the 25 most popular passwords from 2013. If you have a password on this list, it's definitely not secure.

⇒ Don't compose your passwords with personal information, like your kid's birthdays, a pets name, your anniversary date or even a favorite TV show. With the prevalence of this kind of information via social media, it's not hard for a hacker to guess this type of password with limited effort.

⇒ Use strong, secure passwords. This means a minimum of 8 characters in length with a combination of upper/lower case letters and numbers/symbols. The longer and more random a password is, the more difficult it is to hack. You can use a website like www.passwordmeter.com to test the strength of your passwords.

⇒ Don't use the same password twice. One password being compromised by a hacker is bad enough, but if you utilize the same password for multiple applications, you become much more vulnerable. Instead of just accessing your email, a hacker could suddenly have access to your bank accounts, social media accounts and more.

⇒ Never write down your passwords. With so many different applications, this may be the hardest rule to follow. Don't despair; there is help for remembering your passwords. You can use an application such as www.keepersecurity.com to manage and store your passwords. With desktop and mobile application access you can safely store your passwords. This is much safer than a sticky note hidden on the back of your monitor or under your desk.



⇒ Don't share passwords. Once a password is shared among multiple people, it is immediately compromised, no matter how strong it may be. There is then no way to control the use of that password or hold any particular user accountable for their actions while logged in under that password.

Password Alternatives:

There's another way to safely, securely access a system without having to fuss with strong password requirements. Biometric fingerprint readers are now a viable alternative for accessing any number of systems. RMS customers have access to our unique fingerprint log-in program which virtually wipes out the need for a complex login and password. Not only is this the easiest, most secure way to access a system, it also helps with employee accountability and prevents sharing of passwords Since you have to be physically present to access the system, it also means that a hackers attempt to access that system becomes exponentially more difficult.

Chapter Five

Anti-Virus software is one of the most fundamental components of a secure system. Not only is anti-virus required to obtain PCI Compliant status, without it, no matter what other security measures you take, you are leaving a big hole in the overall security of your pharmacy.

There are more ways to obtain a virus on your computer than one can easily enumerate. Something as innocent as browsing the internet or clicking on a link in your email to downloading an application that looks like innocuous enough but is really hiding something sinister.

A virus on your system can be detrimental, and you might not even know it's there right away. If you're lucky, you might suddenly experience a lag in your systems processing and response. If whatever virus your computer contracts isn't quite so tame, it could cause a complete system failure and irrevocable loss of data. Perhaps even more detrimental to your business, viruses can also be a gateway to theft of personal and proprietary information. Needless to say, anti-virus software is paramount to the security of your pharmacy.

Not all anti-virus software is created equal:

When picking anti-virus software, you should carefully review the available features to make sure you have protection that will meet your needs and effectively protect your systems. Anti-Virus should be installed on every single system within your store network, not just those where transactions are run. Here are some things to consider when choosing your AV solution

⇒ **Beware of free anti-virus programs:** Every penny counts when running a business, but anti-virus software isn't generally an area where you want to focus on cost alone. A lot of these programs are simply too basic to suit the comprehensive needs of a business. Additionally, if you read the fine print in many free anti-virus applications, you'll find that they are not licensed for business use and are only for personal home application.

> "...anti-virus software is paramount to the security of your pharmacy."

⇒ **What once was there is now gone:** That PC you bought may have come with anti-virus software installed, and it may have been free for a month or two. But generally somewhere along the way that subscription expired. Your PC probably popped up a reminder to renew (at a cost) but often times those pop ups are ignored. Make sure that your subscription is current and that anti-virus is actually running on your PC.

Features to Look For:

- ⇒ **Active Protection:** This feature checks applications as you start them and monitors applications as they're run. Without it, if you are in-between virus scans, a new application could harbor a virus and have a detrimental impact on your PC before your anti-virus software can catch up.
- ⇒ **Automatic Updates:** The landscape of computer viruses changes faster than you'd imagine. Automatic up dates will make sure your computer has the latest virus definitions so that you are protected from the most current threats. Otherwise something new and dangerous could slip right on by and your anti-virus software would be none the wiser.
- ⇒ **Ability to schedule regular scans:** It's important to scan for viruses on a regular basis even with features like active protection and automatic updates. But the last thing you need is to have to remember to run those scans all the time. Make sure your software can be set to run scans at prearranged times. At RMS, our managed anti-virus solution is set to run quick scans every night and then a full scan after hours once a week.

Before you click purchase on any anti-virus solution, it's important to check with your technology partners for their recommendations. Some anti-virus programs may blatantly interfere with their software applications. Or, like RMS, they may have a solution that they can put in place, monitor and manage for you. One less thing to worry about in the name of security.

Chapter Six

The Internet is essential, but caution is necessary in order to utilize the world wide web without causing detriment to your business.

March 12th,2014 marked the 25th anniversary of the invention of the World Wide Web. In any modern business we use it every day without a second thought. It's not a novelty or a luxury anymore. Half the world's population takes the internet for granted. Much like other things we're used to these days, such as TV's, cell phones, and tablets, the internet is almost a must have today.

But as much as the internet has become a necessity, it also can pose an inherent danger to your business if good habits aren't practiced when it comes to use on your pharmacy network and business PC's.

Beware of what you click on:

One of the easiest ways to open yourself and your business up to a security risk is by clicking on a link that isn't what it appears to be. You'll find these hiding in plain site during internet searches and see them in emails. You may think you're going to one site, but actually be directed to a site that could be harmful to your computer. If you aren't exactly sure what website you are going to you need to exercise caution before clicking any unknown link. For example, there's a big difference between typing in www.rm-solutions.com to access the RMS website directly and searching for "Pharmacy POS" and clicking on a link to a website that promises "Low cost Pharmacy Point-of-Sale Systems!" You could click that link and it might take you to a website that does exactly as it promises, or it might take you to a malicious site which could do damage to your system.

Luckily, protecting yourself from this kind of fraudulence is actually pretty easy. Just hover over the link with your mouse (don't click!) and you'll typically see the URL that the link actually goes to in the left hand corner of your task bar. If the URL is anything different than what the link states itself to be, that's a good indicator that the link is fraudulent

Have an internet usage policy

The internet is a great business tool. But in your pharmacy, it should probably stay relegated to business use. Employees surfing the web, spending time on social media sites, checking emails, etc. only open you up to more risk. (Not to mention the hit your overall efficiency probably takes when employees are distracted.)

At the very least, it's prudent to put in an internet usage policy for your staff. Clearly define what they are and aren't allowed to do online. If you're going to allow them internet usage in the store on breaks or at lunch, make sure you provide a computer just for that purpose in the break room so that you're isolating the risk as much as possible from those systems vital to your business. Have every employee review the policy and sign that they accept and understand the terms and conditions that you've set forth.

If you're having trouble controlling internet usage, even with a policy in place, you might want to consider adding a domain blocking service which would allow you to block certain categories of online content from being accessed. Many of these programs allow you to be as strict or as lenient as you'd like while maintaining overall control of internet usage.

Chapter Seven

Technology continues to advance at an incredible rate. Computers get smarter and faster so quickly that it’s impossible to keep up with the latest and greatest. While you can practically run your home from a PC, smartphone or tablet (manage your thermostat, turn lights off and on, unlock and lock your door), a little bit of TLC is still required to make sure that your computers are doing their best to protect your software applications and sensitive information.

Turn on the time sync feature: It's important that your systems reflect the date and time correctly. If your store were to experience a breach, or you needed to track down something that occurred within the system, an incorrect date and time could throw a major wrench into resolution of the issue. This is an easy setting to turn on within Windows. In the Control Panel, there's a selection for "Date and Time". There's a tab for Internet Time where you can set the PC to automatically sync with time.windows.com. Setting this across all of your systems should ensure that they will all display the same date and time settings.

Set Window updates to Automatic: Microsoft supplies pretty frequent updates, fixes, security patches etc. to those platforms that are still in the Microsoft support cycle. Again, in the Control Panel you can access the section for "Windows Update". We recommend that you set these updates to automatically download. Once updates for your system are downloaded, your system may prompt you to restart to apply the updates. It is vital that you comply with this request as soon as you are able to safely restart the PC. Otherwise you'll have a bunch of downloaded patches and updates not actually doing anything to protect your PC. And, the next time you need to restart that PC in a hurry you might get caught in a torrent of applying outdated patches before your system will come back online.

It is important to note that in order for Windows Updates to function on your PC, the OS that PC is running is still supported. Standard versions of Windows XP will no longer be supported by Microsoft beginning on April 8th, 2014 which means that important security updates and patches will no longer be downloaded to your system. This leaves you vulnerable to attack so if you are running XP, it's time to think about replacing those systems.

Turn on Windows Firewall: While an actual physical firewall protecting your network is required for PCI Compliance, you can never be too safe. Windows has a built in software firewall that can be an added layer of security. Windows Firewall is accessible through the control Panel and can easily be turned on from there.

Back up important applications: Should unexpected catastrophe strike your pharmacy, whether due to a security breach, natural disaster, or technology failure, you have a lot to lose when it comes to the data you need to successfully run your business. We find that many independent pharmacies have little to no redundancy in their technology, meaning that the failure of even one key system can set off a chain reaction of lost information that can basically set your pharmacy back to square one when it comes to data and records. Having a current backup of data from the applications you depend on to run your business can help you to get back on track quickly if the need ever arises.

Luckily, keeping a current backup of all of your data is easy. While there are many cloud based backup services that charge for storage of date, perhaps one of the most cost effective ways is to simply use a rotating physical storage option. Simply obtain a couple of USB flash drives to start and then contact your pharmacy technology and system partners to set the appropriate system up to run a backup each night to a specified drive location. In this case, that backup will run to one of the USB flash drives. At the end of each day, plug one flash drive in and take the previous day's drive out. Then either take that drive with you off site, or store it in a secure fireproof, waterproof safe. You'll want to periodically check the drive to make sure that the backup was successful and updates are on the drive as expected, but this way you'll always have a recent copy of the databases and information that you need to keep your pharmacy running smoothly.

One step at a time:

The information in this E-Book is meant to be a starting point to help you understand some of the basic security concerns surrounding the pharmacy point-of-sale industry today. It's based on some of the most frequently asked questions posed to the staff here at RMS.

The best thing you can do as you start down the road to secure your pharmacy is ally with partners for your pharmacy technology that are both knowledgeable about the security needs of your pharmacy, and willing to help you in whatever ways they are able. No one system provider can address all of your security needs, but having people in your corner who understand your business is a good start.

Learn more at www.rm-solutions.com
Contact us to discuss the best fit for your needs.
1.877.767.1060 • sales@rm-solutions.com • www.rm-solutions.com

A Smarter Pharmacy Publication from

RMS Retail Management Solutions