

INSIGHT

THE QSI MAGAZINE

January 2002

*Is Your Business
Secure?*



www.qsi.com



Bill Cobb
President, QS/1

Security

In these changing times, security is on everyone's mind. We all want security for our homes, our families, our country. But how do we ensure that we're doing enough to protect the businesses that provide our livelihoods? Often it's a matter of deciding how much risk we're comfortable taking.

This issue of *Insight* offers some ideas on security that are specific to QS/1's core industries of pharmacy and HME. Physical security of store products is one issue we address. Cindy Wendland, for example, presents some suggestions on training your pharmacy staff to watch for theft within the store. Pete Peeler provides information on how to prevent employee theft in a small business.

The security of information is also an issue any business owner must consider. Here, again, the choices one makes on data security are based on risk tolerance. Providing data security for one's business is often learned the hard way. We've had customers lose systems and realize they haven't done a system backup in six months; that's a hard lesson in the importance of computer data to a business.

Technology makes almost any business more competitive and efficient, but I don't know anyone who has not lost a file or crashed a system, or somehow, at some point, been inconvenienced when technology temporarily fails. The key is to take reasonable precautions--virus protection and system backups, for example--to minimize the damage to business data and operations. The center spread article discusses some of these precautions.

Business--and life--will always have an element of risk, but finding a level of security you are comfortable with can provide increased peace of mind. And that's what security is all about.

January 2002

CONTENTS

The QS/1 Magazine

4 Security of People and Products

By Cindy Wendland

5 Employee Theft

By Pete Peeler

7 Security and HIPAA

By Jane Bunch

8 Cutting Costs:

A Closer Look At Pre- and Post- Edits

By T. Tyler Thompson

9 Data to Dollars:

Data Collection Programs In The Pharmacy

By Jennifer Langham

10 Securing Your System

By Jennifer Langham

13 Customer Spotlight: Evers Pharmacy/ Harold Smith Pharmacy/Allen's Drug

By Jennifer Langham

In this Issue:

Canadian Perspective

From the Support Center

QS/1 In Your Area

Special Credits:

Lock image courtesy of www.freeimages.co.uk.

Contact *Insight* at:

E-mail Address: Insight@qs1.com or

Write us at:

QS/1 Data Systems, Attn: Insight Magazine,

PO Box 6052

Spartanburg, SC 29304

UV INKS  NO VOC'S®



This publication is printed on recyclable paper and with environmentally friendly ink.

©2001, J M Smith Corporation. QS/1 and FamilyCare are registered trademarks of the J M Smith Corporation. RxCare Plus, PrimeCare, SystemOne, CRx, Q/Review and PowerLine are registered trademarks of the J M Smith Corporation. Product names, company names and logos are trademarks or registered trademarks of their respective holders.

Security: Focus on People & Products

The concept of security has become more significant since the events of September 11 and the armed forces action that followed. While security initially conjures up images of police, metal detectors, weapons and more, security in your pharmacy should focus on people and products.

#1 Focus on People

People are the most important asset and the biggest liability in your business. Customers and employees can steal, but more importantly, employees can be trained to curtail theft and increase sales while they're doing it. In fact, in a study by Retail Spy, 50% of the respondents felt that education of employees was the greatest deterrent to theft.

The same study suggests that customers are deterred from stealing from your store if they are greeted and approached by an employee. Depending on the size of your store and your staff, try to have each customer greeted at the door. If your check-out area is close to the entrance, the person at the register can make eye contact and say a greeting. If not, another employee should fulfill this greeting task while performing other duties in the front of the store.

Another way to keep an eye on customers and increase sales is to schedule a floater. This person "floats" through the various departments to help customers find items. Consider how many customers leave your store without finding what they were looking for. Your employees' familiarity with product location and assortment can be used to your advantage. While it is always helpful to ask at the checkout, "Did you find everything you were looking for?" few stores are equipped to then retrieve the items the customer wants if the answer is no. The floater can help this question to always be answered Yes!

Use the time of this floater to lightly face the shelves (pull products to the front of shelves) and keep the store clean. But, more importantly, consider that person the "knowledge employee" and make it a reward to have that opportunity for the day. Also, have the float employee make the customers aware of exciting products that have just come in and

inform them of health screenings, holiday store hours, or anything of benefit as long as it is brief and not pushy.

#2 Focus on Product

The technological devices available today to help order product, maintain it, change the price, and dispense it are numerous. Make sure you are using all the features on the systems you have. Make sure you are following up on prescriptions not picked up. Make sure you are double checking your fulfilled orders and running price updates. Keeping a tight control here ensures that products are watched and not pilfered.

Build in small checks. Rather than just doing inventory twice a year, put your fastest moving or most expensive prescription items on a rotating weekly schedule. If these items are inaccurate or were being pilfered before the checks, you can have a much more significant impact on your profitability with a small amount of work.

"Security in a pharmacy means using the technological tools available to you and training your people to interact with customers in a positive manner."

Have employees keep an eye on expensive items such as smoking cessation and diabetic products. At the beginning of each shift, one person should check the quantity of key expensive items, then monitor them during their shift and again at the end. After a few weeks, this becomes habit and not a big chore. Rather, it shows customers that someone is knowledgeable about what's in stock and what's not. By looking at the items often enough, that employee will be confident and able to answer questions and help sell those products.

Security in a pharmacy means using the technological tools available to you and training your people to interact with customers in a positive manner. Making security a forefront issue will help it to become second nature without making your customers feel like they're under the microscope.

*By: Cindy Wendland
Cindy Wendland is a freelance writer and web designer specializing in pharmacy applications. She is located in Milwaukee, WI. She can be reached at cindy@websitesbywendland.com.*

Employee Theft

Security experts estimate that as many as 30% of all employees steal and that another 60% will steal if given sufficient motive and opportunity. According to experts, the cost of employee theft and embezzlement adds up to billions of dollars annually and is a much more serious concern than burglars and shoplifters. To illustrate, retail businesses recover an average of \$1,350 from each employee apprehended for stealing, compared to \$196 recovered from shoplifters (US Small Business Administration).

Many employees may break an occasional company rule, but most employees don't steal or commit other criminal acts. Many employees come to work knowing theft is wrong and they govern themselves accordingly. However, when a motivated offender comes into contact with a desirable asset, they must make the decision to actually commit an offense. Our decision making theory explains that three required conditions must generally be present before a theft occurs. These general factors make up the following three sides of the "Theft Triangle."

MOTIVE / JUSTIFICATION

What motivates an individual to steal is still not well understood because every individual and business is different. The theft event is usually motivated by a perceived need or reason. The individual also justifies their actions by neutralizing their guilt. The following factors seem to play an important role in the actual decision to steal.

Motive to Possess - Knowledge of the existence and exact location of an attractive asset or target. Employees may want a company's assets, including money and merchandise, for many reasons, including survival, routine use, conforming with peers, or conversion to cash.

Motive to Steal - Dishonest employees normally form some motive that, at the time, is credible to them. Some motives to steal include impatience, impulse, embarrassment, retribution, financial pressure, excitement or thrill, peer pressure, and impairment or disease.



Contributing Factors - Other variables adding to an individual's decision to steal can best be labeled contributing factors. Examples include:

1. The company is viewed as an inanimate object with unlimited funds.
2. There is no commitment to the organization.
3. The greater degree of job dissatisfaction, the greater the frequency of dishonest events.

Justification of the Act - A fourth critical element involves neutralizing the guilt an individual feels before and after stealing. These justifications can include:

1. Denial of Injury - "The amount I take is so small that nobody will miss it."
2. Condemnation of Condemner - "Based on what this company has done to me in the past, they shouldn't be surprised when I take things."

3. Appeal to Higher Loyalties - "I am taking this because I need extra money to pay for my child's surgery."

4. The Metaphor of the Ledger - This justification is based on the idea that conforming to rules accrues credits that can be "cashed in" later and used to excuse breaking rules.

Other rationalizations include describing rule breaking as cheating, "interpreting" the rules, bending the rules, exploiting gray areas, reading between the lines, or just being creative.

Reducing Motive

The work environment plays a large role in the amount of theft employers suffer. Employees who feel they aren't treated properly or who witness the manager and others breaking rules are much more likely to steal than others are. Our charge is to "shape" and maintain a workforce culture of integrity. We do that by enacting fair but explicit rules of behavior. This code of conduct should be issued to and signed off on by all employees.

Loss control teams or committees should be formed and encouraged. Peers (especially "natural leaders") should be appointed and, within limits, empowered. Two-way communications should become a way of life. Employees who don't hate the company or who aren't frustrated by their lack of impact on company operations do not tend to steal as much. We can also monitor employee perceptions about workplace fairness and problems with periodic anonymous surveys and objectively conducted focus groups. Suspected problems require confirmation and sincere follow up. Many employers have also found that employee assistance programs for substance abuse and financial problems can help reduce theft motives.

ACCESS / ABILITY

The second part of the theft triangle is access/ability. An employee who is going to steal should have relatively easy access to the asset and the actual ability to commit the contemplated offense. Our dishonest subject knows about our asset, they feel they have a compelling reason for illegally taking it, and now they must be able to actually take it.

Access - Employees may have authorized access to our assets. They also normally have physical access to the asset. The level of security or ease of access (e.g., use of safes, procedural controls, physical barriers) and the mobility and concealability of an article dictate the probability of a theft attempt. These variables directly affect a potential thief's chances of a successful theft.

Ability/Skill Set - The prospective thief should also have prior knowledge of theft techniques or be creative enough to learn them. Emotional and intellectual skills, such as keeping cool under pressure and sensing the right time to steal, are also needed to steal from an employer. Finally, depending on the type of theft, special tools or special knowledge, such as a safe's combination, the store alarm code, or information about a manager's or security person's schedule, may be required. Potential thieves assess vulnerable times, locations, and assets. Managers, executives, and merchandise buyers, for example, have tremendous access to company assets and intimate knowledge of procedural and technological control compliance. Opportunity for the crime also means having adequate time to plan and steal an asset.

Reducing Opportunities

Employers can reduce theft by making the act tougher. Access to cash, merchandise, supplies, information, and other assets can be restricted. Passwords, procedures, codes, locks, safes, barriers, point-of-sale terminals, and

card access all limit potential offenders' ability to steal because they have a difficult time getting to assets. In addition, some high-loss items can be tied down. Opportunity reduction means both access and mobility control. Managers and loss prevention staff should change their schedules, practices, codes and keys periodically to avoid predictable patterns and unauthorized duplication or usage. Locked doors and other barriers should also safeguard access to restricted areas.

Careful screening of job applicants may reduce access to your assets by keeping out individuals likely to steal. Preemployment initiatives can predict a potential employee's future work behavior, including a tendency towards rule-breaking; knowing these tendencies can reduce company exposure.

LOW PERCEPTION of RISK

A critical factor influencing employees' decisions to steal (the third part of the theft triangle) is whether they believe they will get caught or not. The dishonest employee usually believes the probability of being caught stealing and then being quickly and severely punished is relatively low. Deterrence is critical for employers; we must clearly communicate our ability to detect theft attempts and quickly and severely punish those we catch stealing. This warning must be obvious, recognizable, and credible. The risk of employees getting caught and punished (formal sanctions) and/or humiliated in front of family and peers must be far greater than any potential gain from theft.

Increasing Risk

Employers can reduce staff theft by emphasizing to employees that breaking rules will be quickly detected and severely punished. Like our other prevention activities, promoting legitimate personal risk of detection and punishment to would-be thieves can come from people, procedures,

and technologies. Employers should market risk by convincing potential offenders their peers may report them at any time. Procedures, such as requiring supervisor verification and authorization, may also dissuade thieves. Clear trash bags and lockers expose forbidden items. Camera systems monitor and record sales transactions, exit/entry, and other behavior. Access control and alarm reports track individual and group variances on point-of-sale terminals. Electronic tag systems also reduce theft of proprietary documents and other assets, in addition to merchandise. Door alarms loudly indicate entry or exit to specific areas.

Touting the use of background and drug screening to applicants with visible signage may deter potential offenders from applying in the first place. Accurate annual and cycle inventories should be conducted and high loss items indicated to staff in common areas such as break rooms or time clocks. If employees think they will be caught and sanctioned, they'll probably think twice before stealing. Consistent, strict follow-up on all criminal acts is important in maintaining credible deterrence. Formal sanctions can include disciplinary action, termination of employment, criminal prosecution, and civil action.

The "theft triangle" helps security experts describe the factors that can lead to employee theft. But more important, it helps employers understand how to deter such theft.

By: Pete Peeler, Industry Analyst POS, QS/1

Special thanks to Read Hayes, CPP, Special Consultant, Loss Prevention Specialists, 5415 LK Howell Road, Suite 236, Winter Park, Florida 32792, for the generous use of his paper "Employee Theft Control," 1993, quoted extensively in this article.



Security and HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) will have far-reaching effects on many facets of healthcare, including transaction standards, privacy, unique healthcare identifiers, and security. Healthcare organizations should understand that HIPAA is essentially a set of rules that requires covered organizations to assess their risk and determine acceptable levels of risk, and security is a key area that all organizations will have to examine.

Security Standards

Security is an area of concern in HIPAA that rates its own Proposed and Final Rules. According to HIPAA, security standards must “establish and maintain reasonable and appropriate administrative, technical and physical safeguards to:

- Ensure the integrity, availability and confidentiality of the information,
- Protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information, and
- Ensure compliance by officers and employees of applicable entities.”

The security standards will apply to health plans, healthcare clearinghouses and providers that send electronic transactions. A provider is deemed to have sent an electronic transaction when either the provider or his representative (clearinghouse) performs that function.

An interesting sidebar for healthcare providers is that if they do not send electronic transactions, they are not subject to the HIPAA regulations. However, to counterbalance that perceived exception to the regulations, the Department of Health and Human Services further stated that in such a case, the paper claim must contain exactly the same information that would be contained in the matching electronic transaction, or the health plan has the right to reject the claim. Revisions of the HCFA 1500 and the UB92 are currently in progress.

While the security and electronic signature standards Notice of Proposed Rule Makings (NPRM) have been published, it is anticipated by DHHS insiders and industry experts that the Final Security Regulation will not contain rules regarding electronic signatures.

Of note, security under HIPAA involves physical security, systems and transmission security and, of most importance, security within an organization to ensure that only people who have a need to see and use Protected Health Informa-

tion (PHI) in the performance of their duties actually have access to the information. That means that every employee must be trained and retrained to understand their responsibilities. It is anticipated that, like the HIPAA Privacy Regulation, the Security Regulation will include all forms of stored information (electronic, paper, voice, fax, e-mail).

Penalties

The HIPAA regulations have penalties for non-compliance that can range from \$100/standard for minor, unintentional violations to \$250,000/standard (a felony) for knowingly/willfully violating the regulations. In addition, there are criminal penalties that range from 1 to 10 years in prison for profiting from the illegal sale of PHI. It has been estimated that the fine for a covered entity that decided to ignore HIPAA would be at least \$2.5 million.

Conclusion

It has been estimated that only about 25% of HIPAA solutions will be accomplished through electronic system changes. The balance will be accomplished by conducting risk analysis, developing comprehensive compliance plans with individuals identified to be “in charge” of privacy and security, and by training all staff members on their responsibilities. Internal penalties (personnel policies) for not complying are required and must be enforced.

As we learn more about the final form HIPAA regulations will take, the key for affected businesses is to get started. There will be many security precautions to take, and it's imperative not to procrastinate.

By: Jane Bunch

Jane is the founder and CEO of Jane's Billing & Consultation Services, Inc. (JB&C, Inc.) of Marietta, GA. A national consultant and reimbursement specialist, she specializes in setting up new HME companies and pharmacies as well as providing turn-key billing services.

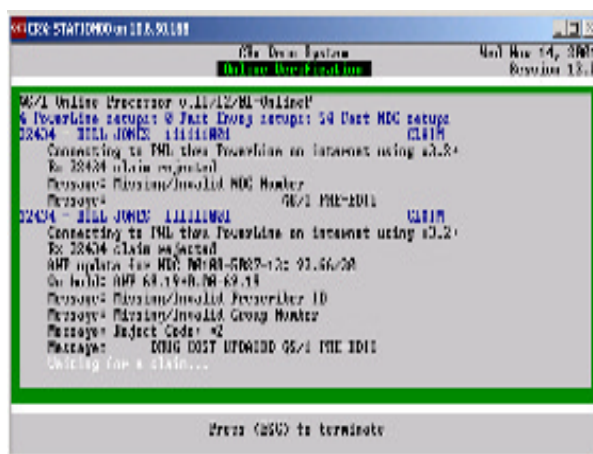
Cutting Costs: A Closer Look at Pre/ Post-Edits

Many pharmacy owner/operators are looking for additional areas to find incremental profits. A popular industry tool for improving margins is the use of pre- and post- edits for claims submissions. Pre- and post-edits (pre/post edits) can be especially effective for supermarket groups, chains, or higher volume pharmacies, who can find savings in five key areas.

The primary use of pre/post edits is to predict when a claim may be rejected or the when a claim may curtail a pharmacy's margin; pre/ edits give the opportunity to correct the claim before it is submitted to the provider. Using pre/ edits before online adjudication takes place can eliminate or significantly reduce claims rejections. In turn, this reduces the fees for the initial third party claim as well as any fees associated with multiple claims submissions. There are instances when the prescription may have multiple errors which are not corrected in one single try. The higher the prescription volume in a store or chain, the more frequently this type of situation occurs and goes unrecognized. Prescriptions may end up costing 20-30 cents in this situation just for adjudication.

The pre/post edit process can also automatically update your Average Wholesale Prices (AWP). This is probably the biggest financial advantage of pre/post edits and can be implemented in several ways depending on the service provider. Some providers will only check the AWP before submitting it. Switch providers, like QS/1, not only check AWP before submittal but also update your AWP drug record for future submissions potentially saving even more expense and fees.

Pre/post edits for AWP can really add up to profits for a pharmacy. Here's how. Before submitting a claim, the switch provider compares the claim to an AWP file for the third party provider and based on the increase will return the claim to be updated with the AWP. With a switch provider such as QS/1 that automatically updates the store AWP, the pharmacy gets additional profit because the U&C as well as cash sales have the new AWP. Depending on the volume of that drug dispensed between the pharmacy's normal AWP updates and the number of drugs that have a similar corrective action, the cost of the service becomes small compared to the amount of improved margins.

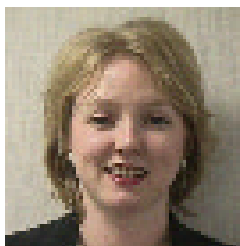


A third area in which pre/post edits can provide savings is the DAW field. Not specifying a DAW or not specifying the proper DAW can result in a significant reduction in reimbursements. Some pre/post edit systems can automatically check for the proper DAW before submission and return it to the pharmacy for correction before formal submission. Surprisingly, this is an area where many pharmacies have realized large savings, especially in combination with other pre/post edit uses.

Two final uses for pre/post edits are in the areas of ingredient cost and competitive pricing. Some pharmacies analyze the frequency of when the ingredient cost is too low compared to what is on file with the switch. When ingredient cost is too low, the claim can be stopped, allowing you to change the price and resubmit. With post edits, pharmacies can use the switch to compare their pricing with other competitors in the area. This information can then be used to put pricing in line with the competition and maximize business profits.

Shrinking margins in the pharmacy industry require all pharmacies to look for areas to cut expenses, and pre/ post edits can generate real savings. QS/1's pre/post edit service, which is available with the CRx pharmacy system, is an exceptionally effective tool for a pharmacy's cost-cutting efforts and for improving margins. In the search for profits, pre/post edits can make a significant difference to your business.

By: T. Tyler Thompson
National Sales Manager, QS/1 Chain Product



Jennifer Langham

Data Collection

Why is data collected? This article explores the benefits of Data Collection for both the manufacturer and the pharmacist.

Data to Dollars: Data Collection Programs in the Pharmacy

By: Jennifer Langham, Communications Specialist, QS/1

When pharmacies look for additional income streams, one service they often take advantage of is data collection. This service, which QS/1 and other software vendors provide, can be a revenue generator with very little effort on the part of the pharmacist.

Why is data collected? Drug manufacturers, certainly, can benefit from the demographic information the data provides. And the pharmacy industry as a whole can uncover demographic information about drug prescribing patterns of physicians and refill compliance patterns of patients. Data may indicate that, for example, a certain age and gender group has a higher degree of noncompliance on refills than other population segments and, thus, may need more aggressive counseling from physicians and pharmacists on the importance of such compliance.

Pharmacies may also collect data as part of their participation in rebate programs. In these cases, the payments received from business partners will be dependent on compliance with the individual rebate program's guidelines.

Russ Weber, QS/1 Vice President for Operations, says, "Data collection requires so little effort by pharmacies that it is really an attractive option for them. We've increased the number of business partners we work with, so that QS/1 customers have a selection of programs they can participate in."

Data collection sometimes suffers from a misconception that identifying information about patients is sent on to other parties. This is not the case. For those pharmacies who participate in data collection, QS/1 software creates a code, separate from the system's patient code, which accompanies zip code, gender, age, and drug information to the data collection company.

Patient names and addresses, in other words, are never transmitted for data collection purposes. Individual

patients, in fact, are not important in data collection. The data is only useful in the aggregate.

Recently, QS/1 changed its data collection methods for RxCare Plus and PrimeCare customers; PowerLine transmissions are now used to collect the data from customers with these products. PowerLine collections will eliminate the need for these pharmacies to set-up for dial-in collection, and, with the addition of programs to collect cash prescriptions, pharmacies will be providing more accurate data. QS/1 then sends this data to business partners once a week.

QS/1 is also changing how payments for IMS data are delivered to pharmacies. In the past, IMS sent payments to QS/1, and QS/1 dispersed these payments to the pharmacies. Now, IMS will send payments for the data directly to the pharmacies.

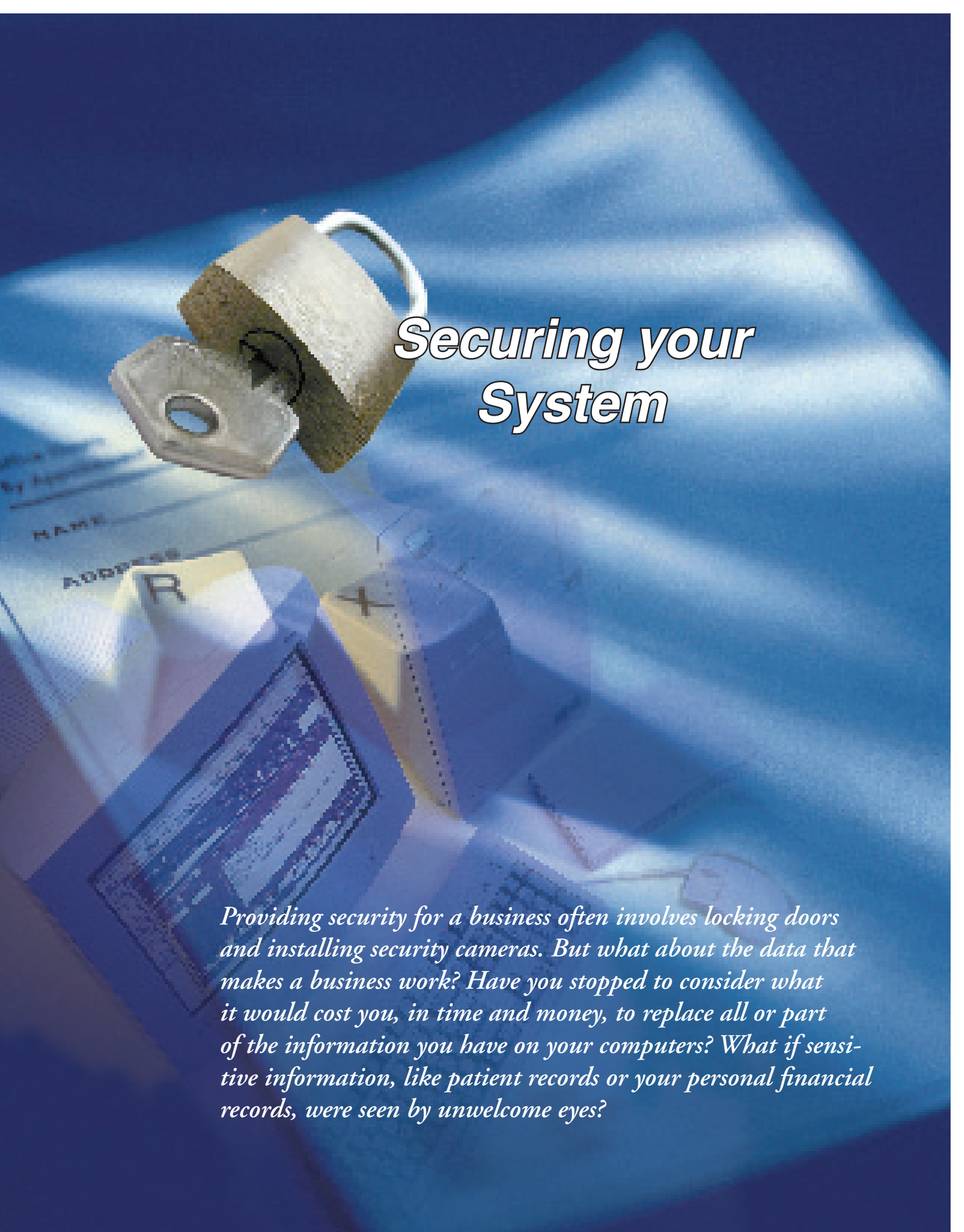
Unchanged is QS/1's long-standing policy of releasing data only from pharmacies who have given prior authorization. QS/1, unlike many other vendors, simply does not give out data unless the pharmacy approves the release of that data.

QS/1's Russ Weber notes, "QS/1's primary role has always been to deliver the data for pharmacies, and these changes simply clarify that role. Data collection programs continue to be a good opportunity for a pharmacy to add to its bottom line, and QS/1 has some great business partners for pharmacies to work with."

QS/1 Data Collection Business Partners

AC Nielson
Dendrite
Epic
IMS
IRI
NDC

NPSC
Pharmacy First
ScriptLine
SHA
TrueCare



Securing your System

Providing security for a business often involves locking doors and installing security cameras. But what about the data that makes a business work? Have you stopped to consider what it would cost you, in time and money, to replace all or part of the information you have on your computers? What if sensitive information, like patient records or your personal financial records, were seen by unwelcome eyes?

Computer security needs will vary from business to business. And much of a business's computer security implementation will depend on the level of risk the business is willing to assume. There are, however, some computer security issues that almost all businesses need to consider; these include protecting against Internet security breaches and against viruses, monitoring internal computer security, and maintaining current backup data.



Internet Security: Firewalls

Hacking into computers has become the stuff of movies and urban legends. But hacking really does happen, and it can be devastating for any business. Any computer connected to the Internet—or on a network connected to the Internet—can be attacked by hackers. For businesses like pharmacies, with private and confidential customer information on their computers, it's necessary to pursue reasonable protection against these attacks.

A firewall is the most common means of preventing hacking by outsiders. The kind of firewall solution a business uses will depend on the type of Internet connection the business has.

Many QS/1 customers connect to the Internet through a dial-up connection using a telephone line. This type of connection is not as easy as others for hackers to breach because a user's IP address changes each time the store logs on. For dial-up customers, QS/1 sells a LAN modem which acts as a basic firewall.

Using a cable modem or a DSL modem to connect to the Internet significantly increases the efforts businesses should make towards securing their network. With cable and DSL connections, a computer is up on the Internet all the time and, without a firewall, other people can see your computer on the network.

The firewall solution for businesses using DSL or cable connections is a DSL or cable router. These firewall products, which range in cost from \$100 to \$1000, become the only exposed device on the network, meaning that outside network users can't see the computers themselves. Businesses using T1 lines or similar for full-time Internet connection, because of the complexity of this connection, require even more sophisticated firewall products to protect their data. Installing and maintaining a secure system through a firewall is something that requires a certain level of technical expertise. Why doesn't a major software vendor like QS/1 provide this expertise to customers? Simple, says QS/1's Director of Product Development Sonny Anderson, "DSL and cable modem services are different throughout

the country. There's no way for us to preconfigure hardware here to work with all different services, and it's not a process we can work on over the telephone with customers. It's a hands-on service that has to be done on-site by a networking expert."

QS/1 recommends that customers hire a local consultant with networking expertise for firewall installations and network configurations. For customers in the Carolinas and in Georgia, QS/1 has a separate division specializing in wide area networks and firewalls, QS/1 Network Solutions.



Viruses

Some published studies estimate that \$200 billion is lost each year due to computer security breaches, and virus attacks are a significant part of this loss. Viruses, designed to make copies of themselves and then spread from location to location, can seriously damage workstations and networks. Viruses spread quickly because they usually have an extremely efficient means of transmission: e-mail.

The primary protection against viruses is anti-virus software. QS/1 preloads Norton Anti-Virus onto almost all new systems unless a customer opts to purchase a system without it. If the computer is connected to the Internet, the customer can easily download updates to the software off the Norton web site.

"The key thing to virus protection programs is that you have to be disciplined about downloading the updates," says Sonny Anderson. "If you're not going to get the updates, the program is not going to do any good. New viruses come out all the time, so you have to be sure that your protection program is as up-to-date as possible."

Another precaution against virus damage is to make a machine other than the server the e-mail client. In other words, don't access e-mail from the same machine you use as a server. This can limit the extent of computer damage should the business receive a virus attached to an e-mail message.



Internal Security

Often businesses are concerned with keeping out intruders but complacent about protecting computers against internal security threats. And yet experts estimate that anywhere from 30-80% of computer crime is committed by employees on their own networks. There are complex and expensive solutions to this problem--smart ID card scanners, thumb print scans, and even eye scans, for example but most businesses opt for less expensive solutions. The easiest, most common solution is to set up passwords for different levels of security.

Passwords are only as effective as their use, however. Passwords should not be an easy-to-guess word, like a spouse's name, and should have a combination of letters and special characters. Users should change passwords on a regular basis and should not write down passwords where they can be easily seen by others.

Another step businesses can take to protect sensitive information from internal misuse is to keep these files on a machine that few employees have physical access to. For easily transferable files, like Microsoft Word and Excel documents, this precaution is even more important. Few business owners want their financial and personal information seen, and possibly copied, by everyone within the company.



Backups

Security doesn't just mean protecting computers against ill-intentioned people. Computers and the important business data on them can be compromised by power surges, system errors, and even natural disasters. Backups are a business's primary defense.

"The key to doing data backups," advises QS/1 Director of Product Support Chris Cox, "is doing them on a regular basis, using quality hardware and recording media, and storing backups in a safe location." QS/1 provides several methods for customers to back up data and recommends that the backups are stored off-site when possible.

Because catastrophic events like system failures happen rarely, backups are easy to forget or ignore. But Chris Cox says that he has seen devastating results from pharmacies not doing system backups. "We've had pharmacies have system failures and they hadn't done backups in months. It's a huge loss for these pharmacies; they have to invest weeks and maybe even months re-keying all the data they lost."

Any business's security plan must consider the importance of computer systems and data to the business and protect

it accordingly. Firewalls, virus-protection programs, passwords, and backups will not make a business's data 100% secure. No device can assure that. But these precautions can go a long way towards keeping data safe and keeping a business going.

*By: Jennifer Langham
Communications Specialist, QS/1*

Protecting Against Viruses

*By: David Pienkowski
Developer, QS/1 Richmond Development Center*

Since "Melissa" made the word virus a household word, many more computer viruses (Code Red, Nimda, and SirCam, for example) have caused havoc and made the news. Not all viruses are designed to damage infected systems, but even benign invaders can cause problems because the virus consumes some of the machine's resources that could be doing other work (like processing prescriptions).

Staying on top of virus protection requires several precautions:

1. **Do not open or unzip files included in e-mail messages when you aren't sure of the source.** Some viruses replicate themselves through e-mail users' address books, so you might also receive virus attachments from people you know. Be wary of any usual looking .exe or .zip attachments.
2. **Get your software from reputable sources.** When you receive and load software from a source other than the manufacturer, there's a greater chance that you are also receiving and loading virus-laden software.
3. **Install and update anti-virus software.** You can set an option in your anti-virus software to remind you to update the virus protection files on a specified timetable.
4. **Scan files downloaded from suspect Internet sites with the anti-virus program.** Set the anti-virus program to do this automatically or manually scan files whenever you download.
5. **Do system backups on a regular schedule.** If your system is infected with a virus and if the damage is serious enough, you will want to go back to the data and software from before the virus attack. Doing frequent backups will make this possible.

When Todd Evers, RPh, graduated from St. Louis College of Pharmacy in 1987, he went right to work at Evers Pharmacy with his father. "It has been a real family operation," Evers says. And he has continued to expand his operations in the metro-St. Louis area.

Customer Spotlight

*By: Jennifer Langham
Communications Specialist, QS/1*

Over the past 15 years, Evers has bought 10 pharmacies, including Evers Pharmacy upon his father's retirement. He has consolidated these into four locations, consistent with the trend in Illinois. "In Belleville [the location of Harold Smith Pharmacy], the population is about the same as it was 15 years ago and yet there are half the number of pharmacies." Evers notes that the influx of large chain pharmacies, the reduction in third party reimbursements, and inconsistent payments from Illinois Medicaid have probably been behind this change.



*Allens Drugs
Troy, IL.*



*Evers Pharmacy
Collinsville, IL.*

But Evers' technology source has not changed. "We've had only one pharmacy system since 1987--QS/1," Evers says. He remembers how high-tech his initial system seemed. "We had an IBM PC AT and a workstation--a network! This was really cutting edge at the time."

With the recent purchase of a pharmacy using another system, Evers became even more enthusiastic about QS/1's capabilities. "RxCare Plus is so far ahead of these other systems it's unbelievable. People who use other systems just don't realize how much more you can do with QS/1."

But Evers sees the new store as a learning experience for both parties. "This new pharmacy is a Hallmark Gold Crown store and has a really robust front-end operation. They're teaching us how to do that part better in our other stores, and we're showing them how much more effective QS/1 can make their pharmacy operations."

One QS/1 service that Evers' stores use extensively is PowerLine. They use QS/1's switch to send third-party claims, and they also transport information through PowerLine to the data collection programs they participate in, including Pharmacy First and TrueCare Pharmacy (formerly Pharmacy Business Associates which has merged with Legend Pharmacy Southwest).

Evers is very excited about how his new broadband connection is improving the speed of his pharmacy transactions. "We've gone from a customer waiting at the register about 45 seconds while we send a credit card through to it taking about 5 seconds," he says. Evers points to how well QS/1 functions, like typing Q and enter to get clinical updates over the Internet, work with the broadband connection. "This improves the whole pharmacy workflow. Now, we're actually waiting for the label to print!"

Evers concludes that he will always try to keep up with technology for his pharmacies. And he adds that working with QS/1 makes this easy. "With a good computer system, you can just do your job," he says. "You're not fighting the system, because it works like an extension of a pharmacist's brain. It's logical. QS/1 has always done a great job at that."



The Canadian Perspective



Standing, from left to right: Jane Abbott (Customer Support Technician), Debbie Wentzell (Customer Support Technician), Rob Richmond (Customer Support Team Leader), Randy Romkey (Hardware Technician), Tim Robichaud (National Sales Manager), Gary Robinson (Customer Support Technician). Sitting from left to right: Lillian Johnson (Pharmacy Software Specialist), Nancy Allin (General Manager), Heather MacLeod (Administrative Assistant), Shona Bazilsk (Accountant), Susan Redmond (Implementation Co-Ordinator).



Brad Turner (Ontario/West Marketing Representative)



Shaunna Wolfe (Trainer)

It is not only the product that makes a company successful, but the people.

On a daily basis the QS/1 support team is ready to take your calls. The support team consists of 4 members: Jane Abbott, Rob Richmond, Debbie Wentzell and our newest member, Garry Robinson. Together the team brings a combined knowledge of 63 years in Pharmacy and Technical Support.

Support Hours

8 a.m. to 5 p.m. Monday through Friday,
(*local time)

Emergency after hours support:
Monday through Friday, 5 p.m. to 9 p.m.
(*local time), Saturday 8:30 a.m. to 9 p.m.
(*local time)

Sunday, 8:30 a.m. to 6 p.m. (*local time)

**Times are based on the local time in your particular region.*

Did you know that QS/1 Canada was incorporated as a company 17 years ago in Halifax, Nova Scotia, Canada? QS/1 now holds 80% of the market in Atlantic Canada and is growing in Alberta and Ontario.

QS/1 Canada offers customers a wide range of products. We strive to give you the tools that will help maximize your business success. Along with RxCare Plus, our pharmacy software package, you can add modules such as Nursing Home, Accounts Receivable, QReview (Consultant Pharmacist Package), IVR (Interactive Voice Response), WinFax, and on-line support using PC Anywhere. We also have a Point-of-Sale system that can be integrated with other QS/1 software or operate as a stand alone product. SystemOne, QS/1's home healthcare software, allows you to print customer invoices, track sales and rentals, bill third parties, control inventory, produce management reports and much more.

Training is another area that we are currently improving to ensure that you and your staff are utilizing the system to its full potential. We offer in-house, on-site and telephone training with qualified QS/1 trainers, as well as a wide selection of training videos.

Offering a high quality product and service is only part of the total solution. As a value added service QS/1 Canada also has supplies such as medication administration records, tapes, toners, etc., available for delivery to your door by courier at competitive prices.

By: Jane Abbott, Customer Support Technician & Susan Redmond, Marketing Representative

Congratulations To The 2001 "Bowl Of Hygeia" Award Winner

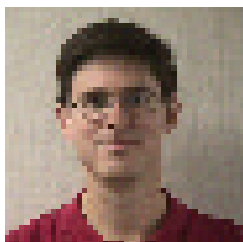
Neila I. Auld

South Shore Pharmacy
Prince Edward Island

QS/1 also Congratulates

John Ryan

Pharmacy Practice 2001 Commitment To Care Award
Mr. Ryan was instrumental in bringing QS/1 to Canada, and provided strong leadership to the Canadian company for a number of years.



Rich Muller

Central Reconciliation

How can Central Reconciliation benefit you? This article explores the benefits of Central Reconciliation for you the chain stores.

Central Reconciliation: Saves Time & Money

By: Rich Muller, Industry Analyst Manager, QS/1

The expression goes, “What you see is what you get.” This is not always true in the world of third-party transactions. An unsuspecting pharmacy can look at its pharmacy system and see that they are going to get paid twenty dollars from the third party, but when the check comes, that amount may be reduced, or not paid at all.

Reconciling transactions with the remittance advice is vital to the bottom line, particularly as margins continue to decrease. However, trying to filter through dozens of third parties and thousands of transactions each month is very tedious. While typically an accounting function, many pharmacists and technicians do this work within a pharmacy. If you have multiple locations, this work is compounded by having to work on multiple pharmacy systems on a regular basis or by having even more people doing reconciliation.

QS/1 offers a central reconciliation solution for its customers through the CMS product. “We have been using central reconciliation for several months and have found it much easier to manage and more reliable than reconciling at the store level,” says Dick Erwin, Director of Pharmacy for the Gibson Merchandise Group, which operates ten Drug Emporium stores in Texas and Arkansas. “The various reporting features on the CMS Host system provide the information needed to identify and track down missing payments. More importantly, utilizing central reconciliation allows our pharmacy staff to concentrate their efforts where they are most needed, in taking care of our customers.”

Initially designed as a central management product for CRx, CMS now can handle reconciliation with PrimeCare and RxCare Plus systems as well. The reconciliation process in CMS is very simple and easy to use. CMS collects data, including transactions with third parties, from each store location nightly. When

Transaction ID	Description	Amount	Status
1001	Pharmacy Transaction	20.00	Paid
1002	Pharmacy Transaction	15.00	Paid
1003	Pharmacy Transaction	10.00	Paid
1004	Pharmacy Transaction	5.00	Paid
1005	Pharmacy Transaction	3.00	Paid
1006	Pharmacy Transaction	2.00	Paid
1007	Pharmacy Transaction	1.00	Paid
1008	Pharmacy Transaction	0.50	Paid
1009	Pharmacy Transaction	0.25	Paid
1010	Pharmacy Transaction	0.10	Paid

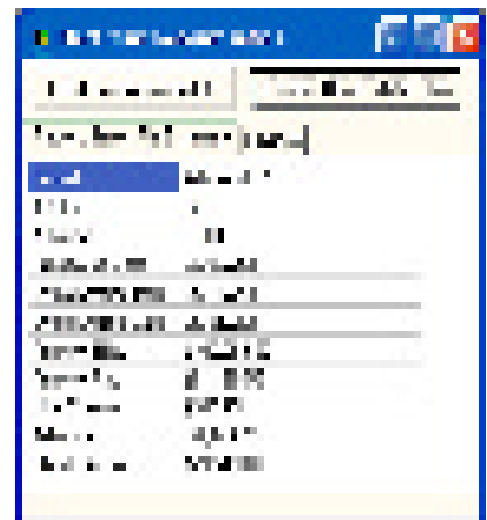
you reconcile claims in CMS, those transactions will already be there and are ready to be reconciled. You select the date range, the check, the third party, and the sites you wish to reconcile. CMS finds those transactions and returns them in a spreadsheet-like view where you choose the claims you wish to reconcile. To make an adjustment, click on the Paying field and enter the different amount. Or you can click on the check box at the left side of the screen and the transaction is marked as paid in full. CMS also makes it possible to mark an entire group of transactions as paid. For example, if the amount you were expecting to be paid matched exactly what the remittance advice said, you could click on each site, which marks every claim under it as reconciled.

CMS also contains aging reports both at a site view and a corporate view. You can print off a trial purge report before making your changes permanent as well. Best of all, CMS is a data warehouse, so all of your transactions are kept until you decide to purge them years later.

Another feature that CMS offers is electronic reconciliation. Most third parties offer chains (this varies anywhere from 5 to 10 stores owned by the same person or organization) the option of getting their claims on tape. If a chain authorizes QS/1 to receive tapes from a third party, we can translate this data into a format that CMS can read to reconcile your claims for you. This is a huge time savings. The sample file shown to the right takes about ten minutes to process in CMS; it may well take a full day to process manually.

PCS was QS/1's pilot test for electronic reconciliation. Other third parties are added based on prescription volume and customer interest. Electronic reconciliation costs \$50 per third party per month, regardless of the number of sites you have or the number of transactions handled.

If you're a multiple store owner or part of a large organization or chain, CMS is the tool to keep track of third party payments. Whether you process them all manually or have some done electronically, reconciliation is an important part of your business.



QS/1 is pleased to announce Rich Muller as QS/1's Industry Analyst Manager. Rich has a Bachelor of Science degree in Computer Science from the College of Staten Island, City University of New York. In 1992 he moved to Richmond, VA, and began his career with Compute-Rx (CRx) as a programmer. In 1995, Rich was selected to lead the pharmacy development group for the CRx product. In August 1998 he was named General Manager of the Richmond Development Center (RDC).

Rich's technical and pharmacy background, his experience with the CRx product, and his enthusiasm for QS/1's continuing success will make him an excellent leader for the industry analyst team.



Annual Conference

August 21- 25, 2002



Hyatt Regency Hotel ♦ Greenville, South Carolina

Come help us celebrate **25** years in the healthcare industry!



Meeting Speakers

Thomas M. Antone, IV:

Tom Antone is a Washington, D.C., health law attorney concentrating on fraud and abuse counseling, representing defendants, health policy and legislation, joint ventures, coverage and reimbursement issues, and the sale and acquisition of health providers and suppliers. He has a particular interest in the legal issues affecting DME suppliers and other home care providers. Tom previously served as President of NAMES (now AAHomecare), U.S. Assistant Secretary for Health Legislation, and U.S. Executive Secretary for Health.

Bruce Brothis:

Bruce Brothis has over 22 years experience in the HME business. He founded Centralized Billing & Intake, Ltd. (CBI) in 1994, to provide billing, consulting, and educational services to the HME industry. CBI currently services clients from coast to coast in virtually all aspects of HME operations. CBI boasts of being, to the best of their knowledge, the only HME billing and consulting company comprised solely of experienced billers and consultants from within the HME industry.

Jane W. Bunch:

Jane W. Bunch has been in the HME and pharmacy industry for over 20 years. Jane is the founder and CEO of Jane's Billing & Consultation Services, Inc. (JB&C, Inc.) of Marietta, GA. A national consultant and reimbursement specialist, she specializes in setting up new HME companies and pharmacies as well as providing turn-key billing services. She also provides assistance in Medicare audits and corporate compliance plans, and she provides educational seminars and publications. Jane is a published author for numerous pharmacy and HME publications and is active in state associations as well as the Medicare Region C Advisory Council.

Maureen Hanna:

Prior to consulting, Maureen Hanna was the Director of Legislative Affairs and Director of Reimbursement for Abbey Home Healthcare (now Apria Healthcare), one of the nation's largest HME companies. Ms. Hanna has been in the healthcare industry for over 20 years. She is now the President of Healthcare Reimbursement Consultants, Inc. located in Fountain Hills, Arizona. Her reimbursement experience encompasses physicians' offices, hospital services, pharmaceutical benefit management, and home care requiring her to work successfully with government and non-government payers of health care services.

Mickey Letson:

Mickey Letson is the President of Letco Medical, Inc. and Meridian Pharmaceuticals, Inc. Letco Medical, Inc. is a specialized wholesale drug company focused on unit dose respiratory and administrative devices. Meridian Pharmaceuticals, Inc. offers pharmacists education and supplies necessary to compound prescriptions. Meridian is the compounding market's leader from process to the codes that govern compounding. Meridian offers the compounding pharmacy the marketing skills necessary to promote their pharmacy's services directly to the physician.

Orlando, Florida

February 7-10

1-800-231-7776
www.qs1.com

Agenda

Thursday, February 7, 2002

5:00 pm – 6:30 pm Registration
6:30 pm – 9:00 pm Welcome Reception (Join us for Heavy Appetizers & Drinks)
Visit Exhibitors

Friday, February 8, 2002

7:00 am – 8:00 am Registration – Continental Breakfast
8:00 am – 8:15 am Welcome and Introductions
8:15 am – 9:15 am HME Basics – Bruce Brothis
9:15 am – 10:15 am Order Intake – Bruce Brothis
10:15 am – 10:45 am Break & Visit Exhibitors
10:45 am – 11:45 am Audits: Internal Audits & How to Test
Employees – Jane Bunch
Luncheon Provided
11:45 am – 1:00 pm How to Successfully Work Denials – Jane Bunch
1:00 pm – 2:00 pm Review of New Features In 17.1
2:00 pm – 3:00 pm Break & Visit Exhibitors
3:00 pm – 3:30 pm Marketing and Medicare Rules – Thomas Antone
3:30 pm – 4:30 pm HIPAA: Getting Ready for It – Thomas Antone
4:30 pm – 5:30 pm Trainers Available at Systems/ Visit Exhibitors
5:30 pm – 7:00 pm

Saturday, February 9, 2002

7:00 am – 8:00 am Registration – Continental Breakfast
8:00 am – 8:30 am Review of Features Scheduled for 17.2
8:30 am – 9:30 am Customer Discussion of Enhancements
Requests for Product Improvements
Break & Visit Exhibitors
9:30 am – 10:00 am 17.1 Detailed Training & Implementation
10:00 am – 12:00 pm Luncheon Provided
12:00 pm – 1:00 pm Opening Up a Nebulizer Pharmacy in
1:00 pm – 2:00 pm an HME Business – Mickey Letson
2:00 pm – 3:00 pm CMN's: The Secrets to Do Them Right – Maureen Hanna
3:00 pm – 3:30 pm Break & Visit Exhibitors
3:30 pm – 4:30 pm Reimbursement: 10 Management Strategies to
Increase Cash Flow – Maureen Hanna
4:30 pm – 5:30 pm QS/1 Staff Round Table Discussion
5:30 pm – 6:30 pm General Questions/ Trainers Available at Systems

Sheraton World

10100 International Drive

Orlando, FL 32821

For Reservations 800-327-0363

Special QS/1 rates are available to attendees:

\$139.00 for Single/Double Occupancy

(Rates good 3 days prior and 3 days after
Convention date)

Conference Registration Fee

\$249.00

Early Registration (Before 12/31/01)

\$199.00

Fee Includes:

Welcome Reception (Thursday), Continental Breakfast, Breaks and Lunch both days.

**For more information,
call Camille Corn (QS/1 Marketing)
at 1-800-231-7776.**

PrimeCare Customer Conference

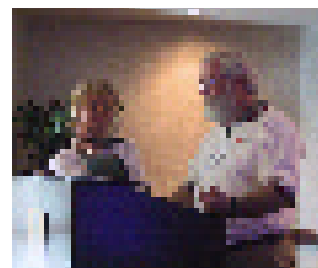
Highlights from the Embassy Suites
in Charlotte, NC, on October 18-19, 2001

QS/1's first PrimeCare Customer Conference was held in Charlotte, North Carolina, on October 18th and 19th, 2001. Over 80 customers and a dozen QS/1 staff members participated. The Thursday sessions covered the new 17.1 release and QS/1 Workflow. The Friday sessions covered Facility Setup and Maintenance, The Fill List, and other topics.

Based on the success and continuing interest of this first conference, we are planning another QS/1 PrimeCare Customer Conference for October 2002.

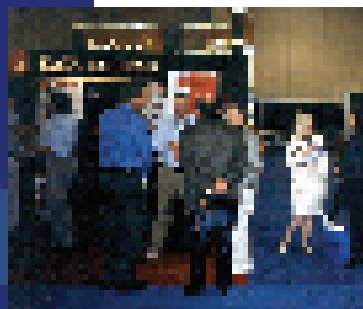
A special thanks to all the customers that took time out of their busy schedules to attend the conference.

Jim Hancock
QS/1 Sales Manager, PrimeCare





NCPA
October 2001
Philadelphia, PA



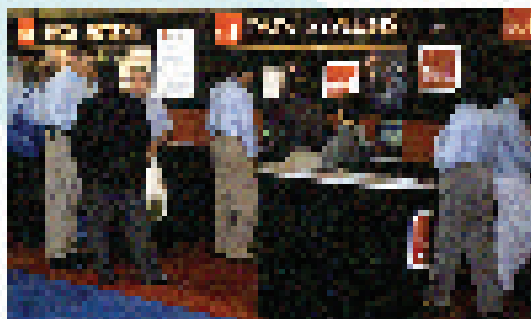
TRADE SHOWS



QS/1's Dave Floyd, Gary Throckmorton, and Tyler Thompson at the Western Food Industry Show, Las Vegas, NV. September 2001



NCPA
October 2001
Philadelphia, PA



NCPA
October 2001
Philadelphia, PA



MedTrade
October 2001
New Orleans, LA



ASCP
November 2001
Chicago, IL

From the Support Center



All QS/1 Products:

QS/1 provides many solutions to backups as well as virus protection.

One backup solution is a tape drive. QS/1 offers a 24 gigabyte unit which uses a 4 millimeter tape. Customers are always asking how many tapes they should use. We recommend at least 4 tapes so that when the full rotation has been used there are always at least 3 good backs to follow up with. This means that if you back up on Mondays, Tuesdays, Wednesdays and Thursdays, when you back up on Fridays, you still have good tapes for Tuesdays, Wednesdays and Thursdays. You can't have too many backups. No matter how you back up, there are logs that should be looked up daily.

QS/1's second backup solution is an external hard drive that can be swapped daily. These drives are used with our QSTORE software. This software can compress the data into smaller chunks; a 20 gigabit hard drive, for example, can compress the data 2 or 3 to 1.

QS/1's third and newest backup option is a DVD backup system that can support up to 4.7 gigabytes of data. The DVD has the same compression ratio as the external hard drive. These drives mainly back up the QS/1 data files and not the whole hard drive.

Anti-Virus Protection has been loaded on most QS/1 systems. The user must run weekly or monthly virus updates. The updates can be automatically received over the Internet or by mail. For example, Symantec (Norton) has a subscription that can be sent to you by mail.

Security on your Windows System

To better secure your patient information, you can set up your Windows screen saver to automatically enable after a

certain period of time. To set up your screen saver, right click on your desktop and choose Properties, click on the Screen Saver Tab, and choose the screen saver you would like to use.

PrimeCare:

One important file to any PrimeCare user is the Accounts Receivable file, and it is important to protect the information in this file. Beside doing normal tape backups, the PrimeCare technicians advise you to always take the time to back up the Accounts Receivable file to diskette before printing statements. A rotating set of diskettes would help recover data that you might not realize was in error or missing until the middle of the next month.

SystemOne:

SystemOne has several options for security access; these may be accessed at F8 from the Main Menu. You may designate what technicians are allowed to do. You may want some technicians only to look at information and not be able to change it. For these technicians, access their security codes, and place an N next to the records you do not wish them to change. For example, if you do not want a technician to change/update doctor records, place an N next to the Doctor Update option. If that technician tries to change a doctor record, he or she will see a message at the bottom of the screen reading "Access Denied for Doctor Update." You should also restrict access to the Security Access Codes area for all technicians by keeping the code you use to access that area a secret. Another tip is to make sure that ALL technicians have unique access codes. For true security, there should be no sharing of codes.

POS:

The QS/1 POS system gives you stronger control over the front end of your store. The ability to limit employees to certain functions and areas of your system provides tremendous accountability for your cashiers. In the event of any suspicious activity or trends, the security report is available as a tool to help track any unusual transactions.

CRx:

The CRx System provides the ability to set up user-specific security access. Each user is assigned a user name and password, and you can restrict access on a menu-by-menu basis. If security is set up on your system, each person will log in with their distinct user name and password. To log out, you simply type Alt-F9 at any screen; this will prompt for a user name and password.

QS/1 Support 1.800.845.7558 • CRx Support 1.800.441.1995

IN YOUR AREA

Training Seminars

San Leandro, CA: (866) 848-1942

01/08/2002 SystemOne: 17.1 Enhancements
02/12/2002 RxCare Plus: Workflow & Tickler File
03/19/2002 RxCare Plus: Nursing Home Processing
04/09/2002 RxCare Plus: Disease Management

Dallas, TX: (800) 233-0096

01/08/2002 RxCare Plus: Reconciliation & Reports
01/24/2002 SystemOne: HME A/R
02/12/2002 POS: Inventory Ordering & Receiving
03/12/2002 RxCare Plus: Inventory Ordering & Receiving

Brandon, MS: (800) 233-6204

01/08/2002 SystemOne: HME A/R

Indianapolis, IN: (800) 637-5251

01/17/2002 SystemOne: 17.1 Enhancements
03/14/2002 17.1 Enhancements

*Classroom Training

02/19-20/2002 RxCare Plus: Introductory Setup & Training
04/16-17/2002 RxCare Plus: Introductory Setup & Training

*Classroom Training (These are 2 day courses with detailed information that will start you out on the RxCare Plus product. The \$500.00 fee per attendee includes two nights' lodging and lunch each day.)

Lexington, KY: (866) 441-7011

01/22/2002 CRx: 6.1 Enhancements

*Classroom Training

03/13-14/2002 RxCare Plus: Introductory Setup & Training

*Classroom Training (These are 2 day courses with detailed information that will start you out on the RxCare Plus product. The \$500.00 fee per attendee includes two nights' lodging and lunch each day.)

Richmond, VA: (877) 392-5851

01/10/2002 SystemOne: 17.1 Enhancements
02/21/2002 CRx: 6.1 Enhancements
03/14/2002 POS: Enhancements
04/23/2002 RxCare Plus: 17.1 Enhancements

Miami, FL: (305) 494-2830

01/08/2002 RxCare Plus: Basic Nursing Home Functions
03/07/2002 PrimeCare: 17.1 Enhancements
(Ft. Lauderdale area registration required by 02/25/2002)
04/18/2002 RxCare Plus: 17.1 Enhancements

Orlando, FL: (407) 682-3246

01/21/2002 RxCare Plus: 17.1 Enhancements
03/19/2002 SystemOne: 17.1 Enhancements (Must register by 03/01)

Spartanburg, SC: (800) 889-9183

01/08/2002 RxCare Plus: Managing Workflow
01/15/2002 SystemOne: 17.1 Enhancements
02/05/2002 PrimeCare: 17.1 Enhancements
02/12/2002 SystemOne: 17.1 Enhancements
02/07/2002 POS: 17.1 Enhancements & Inventory Functions
02/19/2002 RxCare Plus: 17.1 Enhancements
03/19/2002 RxCare Plus: Custom & General Reports
04/09/2002 SystemOne: 17.1 Enhancements
04/16/2002 RxCare Plus: Basic Operation

Atlanta, GA: (Location to be announced)

01/30/2002 SystemOne 17.1 Enhancements

Sturbridge, MA: (800) 648-7428

02/20/2002 RxCare Plus: Basic Processing

Mechanicsburg, PA: (717) 795-2700

01/16/2002 RxCare Plus: Basic Processing
03/20/2002 PrimeCare: Basic Processing

Trade Shows

01/09 – 01/11 San Diego, CA

NCPA
National Community Pharmacist Association
Independent Pharmacy Conference

01/26 – 01/29 Key Biscayne, FL

NACDS
National Association Chain Drug Stores (Small Chain)

02/03 – 02/05 San Diego, CA

FMI
Food Market Institute Marketechins

02/06 – 02/09 Las Vegas, NV

NCPA/CDMA
National Community Pharmacy Association/
Chain Drug Marketing Association

02/11 – 02/14 Las Vegas, NV

NGA
National Grocers Association

03/15 – 03/19 Philadelphia, PA

APhA
American Pharmacy Association (Annual Meeting)

04/14 – 04/16 Orlando, FL

FMI
Food Market Institute (Pharmacy)

04/23 – 04/25 Las Vegas, NV

MedTrade West
Home Medical Equipment

04/27 – 05/01 Palm Beach, FL

NACDS
National Association Chain Drug Stores (Annual Meeting)

05/14 – 05/16 Las Vegas, NV

ASCP
American Society Consultant Pharmacists (Geriatrics)





QS/1[®] HME Software Helps You Put The Pieces Together.



PO Box 6052
Spartanburg, SC 29304

ADDRESS SERVICE REQUESTED

The HME business is like a complex puzzle. Your success depends on your ability to assemble the puzzle pieces of timely, accurate billing and inventory management. Neither of which can be left to chance.

To control and manage your HME business for maximum profit, you need the total solution of QS/1's SystemOne[®] software. This comprehensive package provides direct billing to all four DMERCs and 40 state Medicaid programs, tracking of repetitive rentals and sales, management of receivables so you know who's paid and who hasn't, and unparalleled reporting that gives you control of your reports.

And if you manage an independent, chain or institutional pharmacy, QS/1's industry-leading pharmacy system can integrate your entire operation, including point-of-sale. QS/1 is the only true total solution in the industry. To learn how a QS/1 system can help your operation call 1-800-231-7776 today. In Canada, call 1-800-565-1560.

Presorted
Standard
U.S. Postage
PAID
Greenville, SC
Permit No.
1284