HOME CARE
AUTOMATION REPORT

Vol. 10 No. 4 ★ April 2005

from Stony Hill Publishing

VNA Believed It Could Happen To Them

Texas provider was prepared for exactly the disaster that hit

They say it was the worst fire in Dallas in 24 years. 120 firefighters could not save the downtown building that housed, and was owned by, the VNA of Texas from the 6-alarm blaze of unknown origin. Though the 7-story structure at 1440 Mockingbird Lane was condemned following the February 19 disaster, no one was injured. Equally providential, VNA operations experienced virtually no interruption in patient care, payroll or billing.

Once it was determined that the Saturday incident occurred in an unoccupied building, except for a few construction workers who escaped without injury, concern quickly shifted to business continuity. As it turned out, both patient care and business processes survived the fire virtually without interruption, testaments to a disaster recovery plan other agencies would do well to investigate.

Continued on page 2

Stolen Laptop Raises Security and Liability Questions

Developing story serves as a harbinger to take security seriously

It was a quiet, low-crime neighborhood. It still is, to tell the truth; relatively affluent too. Residents know each other and the streets feel safe at night. Perhaps that in itself is what attracts gangs from larger cities. They have been showing up quite regularly lately and they seem skilled enough to be able to get into locked, occupied structures, take what they want and leave without detection.

First, they broke into cars in business office parking lots during the day while the offices were filled with people. Finally, it was an unlocked car *inside a locked garage* at the quiet, suburban residence of a home care nurse, while she was there. She thought her new laptop and a stack of paper visit documents would be perfectly safe, tucked away in the trunk, while she attended to children and dinner. Instead, her employer is now in danger of civil and criminal penalties for possibly exposing patient information.

Why This Incident is Important
What makes this particular security

Continued on page 4

Inside This Issue

VNA Believed It Could Happen continued from page 1

According to CIO Wyatt Davis, no patient visits were missed, fewer than two days of paper visit documents were lost and the VNA produced a complete payroll on Monday, two days after the fire. There were a couple of serendipitous events on the weekend of the fire that helped, Davis admitted. For the most part, however, the near-miracle recovery was the result of management's refusal to assume "it couldn't happen to us." The agency's disaster recovery plan reads like a primer for organizations concerned with guaranteeing business continuity, or for healthcare providers concerned with complying with HIPAA Security Rule contingency planning provisions (see sidebar next page).

VNA fire photographer: JEFF COVINGTON/Special Contributor

ENSURING BUSINESS CONTINUITY

How Texas VNA beat the blaze

Shortly after succeeding the retiring Mary Suther in 2003, CEO Robert Carpenter presented the VNA IT department with his ideas to upgrade computer data systems to address the possibility of a disaster that could disrupt operations. The cornerstone of his plan was to move the network core, consisting of 45 servers, out of company headquarters to a safe, off-site location. A vendor was selected and the conversion completed in the fall of 2004, with former Baby Bell SBC hosting the VNAs servers in its secure data center.

Four VNA branch offices continued to connect to routers at Mockingbird headquarters after the servers were relocated. A one-GB fiber pipe was provisioned to carry network traffic from there to SBC's site. With this configuration in place, the need for a tape backup system was eliminated, but Carpenter and Davis decided to ratchet up safety one more notch. An automated routine copied the "My Documents" folder from every desktop PC to a designated backup server in the data center each night. In the event of a catastrophe, not only patient and billing information would be preserved but also supporting documents, patient letters, spreadsheets and the like.

Carpenter's next step was to implement a document imaging system, which went online months before the fire. On a daily basis, physician orders, paper forms, faxed documents and hand-written notes were scanned into electronic storage, filed and catalogued as soon as they arrived at headquarters or a branch office. When the fire hit, not only data entered into software applications but paper documents were also safe at the SBC data center. Policy called for scanning of all such documents on the same day they arrived. Documents that could not be scanned before the end of the business day were stored in fireproof filing cabinets overnight.

Planning, aided by good fortune

You've seen the bumper stickers. Well, sometimes unpredictable good things happen too. While the fire was still raging out of control, Carpenter called a friend in commercial real estate and found him in his office that Saturday. After describing his predicament, his friend thanked him for explaining where all the smoke was coming from, and said he happened to have a building in his inventory whose occupants were in the process of moving out that same day. And they were leaving behind rented office furniture.

Then, practically out of the blue, Carpenter heard from Texas Health Resources, a large area hospital with which the VNA has a strong referral relationship. They offered to lend the VNA 100 spare desktop computers and some printers that they keep in storage as part of their own disaster recovery program. Together with the approximately 40 salvageable computers from the fire, that brought the VNA to its full complement of 142 workstations.

All Davis and his IT team had to do was put in a couple of "all-nighters" – not an unfamiliar job requirement for seasoned IT professionals – to configure the borrowed machines for the LAN and send the smoky ones out to be professionally cleaned. SBC managed to quickly configure a temporary Internet connection at the new location and the VNA was printing paychecks by the close of business Monday.

Continued on page 3

VNA Believed It Could Happen
continued from page 2

Insurance issues settled quickly enough to allow Davis to order replacement desktop computers, which arrived by Friday. During another sleepless weekend, the IT team returned 100 computers to Texas Health Resources and configured an equal number of new PCs to the LAN in time to resume operations Monday morning.

Yes, there were glitches

"Having our servers offsite was the smartest thing we ever did," Davis declared. "If we would have had to purchase new servers, reinstall all our software applications and restore data from tapes, we would never have been operational so quickly." So convinced is CIO Davis of the security offered by offsite data centers, he says he will look into putting his phone switch there once the VNA moves to new permanent quarters.

"The phone system took longest to come back online," he said. "We did everything we could but we had to resort to a contingency plan for a couple weeks." The VNA convinced SBC to send its technicians into the smoldering building as soon as the fire department would allow. Wearing miners hats with front-mounted lights, the technicians combed through the rubble until they found the central phone switch. It had suffered only smoke damage and was salvageable but required extensive cleaning. It did not come back online until March 8, three weeks after the fire.

To keep the VNA's telephone-dependent business running in the interim, Davis contacted the company's answering service and instructed them to answer all calls around the clock. 40 cell phones were pressed into service and a call tree was devised routing calls from the answering service to the appropriate department.

The HIPAA Security Rule (164.308 (a) (7)) requires that healthcare providers take steps to ensure business continuity in the event of a debilitating disaster. Though the rule does not officially take effect until later this month, the Texas VNA understood that physical disasters and computer hackers know nothing of federal mandates. Preparing for the worst-case scenario, eschewing the notion "it isn't going to happen to us," and investing in recovery measures have paid off a hundredfold for this insightful provider.

HIPAA Security Rule – Ensuring Business Continuity

The HIPAA Security Rule, which goes into effect later this month, requires that an agency establish, and implement as needed, policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (ePHI).

The rule includes five implementation specifications, three of which are *required* and must be implemented and two which are *addressable* and may be implemented.

- Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of ePHI.
- Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
- Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
- Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.
- Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

The contingency plan requirements of the Security Rule are intended to protect the confidentiality, integrity and availability of ePHI during an emergency. Agencies are expected to develop a plan that ensures software applications and data required to support critical agency operations are protected in an emergency and that procedures are in place to restore any lost data and resume normal operations as quickly as possible.

Most agencies already have some type of emergency response or emergency operations plan in place, and this is certainly the case for agencies accredited by JCAHO or CHAP. Such plans typically focus on emergency preparedness within the context of protecting the safety of patients and staff. To comply with the Security Rule, agencies *must* expand the scope of such plans to include emergency response measures addressing critical software applications and data retained in agency information systems.

Taken together, these requirements are quite significant. For the first time, business continuity planning is mandated for virtually all healthcare providers in the U.S. Providers must have disaster recovery capability and plans must be in place to restore critical business operations. They must also have emergency response measures in place to secure and restore essential information systems during the period immediately following a disaster.

Stolen Laptop continued from page 1

incident of interest? It is certainly not the first time that a home care clinician's laptop has been lost or stolen. This incident occurred and is unfolding in California, the only state with a law requiring organizations to disclose security breaches to all affected parties.

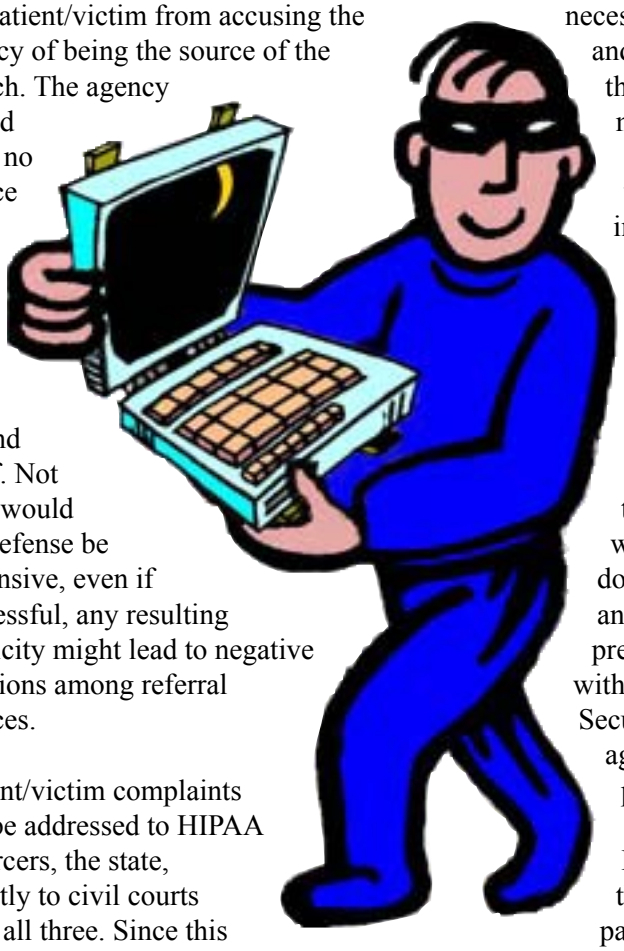
Under SB 1386, a California law enacted in September 2003, any business having personal information on state residents must promptly disclose security breaches that could lead to identity theft. It is this law that triggered ChoicePoint's disclosure of the massive security breach it uncovered last fall, and dozens of other incidents impacting millions of individuals that have come to light since the law was enacted just 18 months ago. This is the law that is being emulated in legislation being considered by more than 20 states as a result of the recent rash of security incidents. It is the law that Senator Diane Feinstein (D-CA) is trying to replicate on a national level.

HCAR will follow this story as it unfolds. It will be an object lesson for other agencies regarding the dangers of suffering a security breach. The affected home care agency has agreed to provide us with ongoing detail on the condition that it not be named, hoping that the very act of making its situation public will spur others to take preventive measures. This incident truly is a harbinger of what is to come should similar laws be enacted at a state or national level (see HCAR, March 2005, page 1).

Truth and Consequences

For now, the agency can do little more than wait to see if the thieves are smart enough to figure out the laptop's home care software application and harvest patient information. Even though that is not likely – login to the operating system is password-protected and encoded patient data can only be accessed through the Patient Care Technologies application, which is protected by another login routine – there is still the matter of the paper records which were stolen along with the computer. Possible repercussions may include incidents of ID theft and subsequent victim complaints.

The agency may be at risk even if the data is secure within the laptop. ID theft randomly affects approximately 10% of the population. If a patient of this agency falls victim to ID theft from an unrelated, unknown incident, and if the laptop theft becomes widely known, there is nothing to prevent the patient/victim from accusing the agency of being the source of the breach. The agency would have no choice but to defend itself. Not only would the defense be expensive, even if successful, any resulting publicity might lead to negative reactions among referral sources.



Patient/victim complaints can be addressed to HIPAA enforcers, the state, directly to civil courts or to all three. Since this incident occurred before the HIPAA Security deadline, federal complaints would go to the Office of Civil Rights (OCR) under the HIPAA Privacy rule, not to CMS. (See sidebar, "CMS Announces Complaint-Driven Security Enforcement," p. 11.) Needless to say, any combination of the above would be expensive, possibly beyond what the agency can bear.

Whether a victim of an unrelated ID theft incident, or his or her attorney, would be aware of the laptop theft depends on state disclosure laws and the agency's own policies. In this case, the agency immediately attempted to alert its affiliated hospital's Privacy Officer, apparently an extremely busy individual, for guidance. The earliest available meeting time was four days later, only that soon because the home care administrator was willing to schedule a ten minute meeting at 7:30 AM. Upon hearing the details, the officer determined it would be necessary to notify OCR and accept the risk that the enforcement agency might use the report as a reason to initiate a wide-ranging privacy inquiry with the hospital.

Assessing its Security Controls

In the midst of waiting for the other shoe to drop, the agency wonders what else it could have done to prevent such an occurrence. While preparing to comply with HIPAA Privacy and Security regulations, the agency had already put a number of safeguards in place. It established a policy that laptops and all paper with identifying patient information must be kept in car trunks rather than on car seats. It made sure consequences to policy violations were established and made known to all staff.

Continued on page 5

Stolen Laptop continued from page 4

Since the incident, the agency has upped the ante. "Now we tell the story of the theft at all point-of-care software classes and instruct clinicians to treat the computer like a baby," the acting administrator explained. "If it's 10 degrees or 100 degrees outside and you wouldn't leave a baby in the car for 10 minutes, don't leave the computer in the car. If you're going into a store or the post office or a laundromat in the middle of your shift, take the computer with you. We bought the smallest notebook computers Fujitsu makes, and they're a lot lighter than a baby." Clearly, she added, trunk locks are no deterrence in a town where car theft is much higher than the national average.

Prior to establishing this policy, the agency acknowledges that its staff was a bit casual regarding privacy and security controls. Management often witnessed visit paperwork lying, face up, on car seats. On one occasion, a nurse was rushed out to the parking lot to close her car's trunk. She had put the paper where it belonged all right, but forgot the final detail.

The nurse who lost a laptop and some paperwork from her trunk inside her garage had done everything possible, short of locking her car while it was in her garage, which may not have slowed the thieves down anyway. Such extreme incidents of thieves with extraordinary skills are nevertheless considered by the HIPAA Security Rule. Recognizing that laptop computers will be lost or stolen from time to time, the regulation specifies that administrative, physical and technical safeguards be put in place to minimize the risks associated with such incidents.

New Technologies Making Passwords Obsolete

"Something you have," "something you are," replacing "something you know"

Password hassles are nothing new. Nearly 20 years ago, in the "green screen" days of computing, Ferris Bueller figured out that Marge, the school secretary, wrote down the daily password and always hid it in the same desk drawer. That's how he was able to get good grades without studying and skipping school nine times.

To the horror of security officers everywhere, Post-It notes have made it even easier for today's Ferris's to steal passwords; they just glance at the monitor. "Let's see, grocery list, husband's birthday, ah, here it is, login ID and password." To quote Principal Ed Rooney, "Wake up and smell the coffee Mrs. Bueller…"

Today, there are companies trying to make passwords a thing of the past by producing low-cost versions of technologies that formerly fit the budgets of none but Fortune 500 companies. Two such technologies were demonstrated at last month's Healthcare Information Technology Summit West in San Francisco. One has strictly business uses but the other seems also to be targeting the consumer market.

Flipping off passwords

No matter how exotic or James Bond-like fingerprint authentication may have seemed a few years ago, today the technology is being marketed to home users as well as businesses. The rationale is that in today's connected, security-conscious world, everyone who uses a computer has so many login names and passwords for so many applications and web sites it has become impossible to remember them all. $80 fingerprint readers may soon sit beside – or be embedded within – not only office but also home computer keyboards.

Take, for example, the innovations coming from Silicon Valley company Digital Persona. The software developer has created a secure enterprise identity management system, *DigitalPersona Pro*, that integrates with Microsoft Active Directory and uses a proprietary fingerprint reader technology the company has dubbed "U.are.U." The *DigitalPersona Pro Software Development Kit* (SDK) is also available for web programmers. It is an ANSI C-based toolkit, including Java wrappers, that enables developers to create fingerprint recognition enabled applications.

Microsoft resells *DigitalPersona Password Manager* with its line of consumer fingerprint readers, including those built into keyboards and standalone readers that connect through a USB port. The software giant said, with the introduction of its new line of low-cost fingerprint authentication tools, that it foresees the day when U.are.U-based readers will be commonplace in homes. Family members will be able to share a single computer but easily log into

Continued on page 6

Passwords Obsolete continued from page 5

separate user sessions by touching a U.are.U reader.

In the healthcare provider office, ever-growing lists of passwords for network access, application login and web sites easily exceed the capacity of office workers without a photographic memory. In addition, HIPAA regulations make password management far more complex and challenging than at home. No longer will a security-aware IT department allow pets' names or wedding anniversary dates to be used. Modern password policies typically require at least 8-character passwords made up of random letters mixed with numbers and a few character symbols. Then, just when a month or two has passed, perhaps enough time to memorize a password, policy requires changing it again.

Before fingerprint reading technology became affordable, network administrators and security officers had to settle for trade-offs between high security and more convenience. Separate login IDs and passwords for desktop, network and application authentication, plus unique logins for each commonly used web site provide good security but at the same time force the need to create and frequently update a paper or electronic password log for each user, which weakens security. The complexity exacerbates as the number of secure web sites a typical home care agency must regularly access continues to grow.

A commonly selected trade-off is single sign-on technology (SSO). One password to the desktop authenticates a user to the network as well as that user's list of authorized applications. Most SSO systems also produce an audit trail of network and application logins and logouts. While more convenient for the user, SSO requires additional management by network administrators and opens up a wide range of potentially valuable patient and business data to a hacker who manages to acquire only one ID and password combination.

Fingerprint technology seems to combine security with convenience. Users do not have to remember any passwords. Once they create a password for network login and each application and web site they use, they simply associate the new password to their fingerprint for each one and no longer have to remember it or use it. Even if company policy calls for periodic password changes, it is easy to reassign new passwords to fingerprints and login applications.

DigitalPersona customer Sutter/ California Pacific Medical Center believes that fingerprint authentication has enhanced its level of security. Authorized users access protected patient records by touching a U.are. U reader and the system automatically builds a time and date stamped log of all accesses, a key Security Rule requirement. Some organizations report that fingerprint technology has resulted in reduced password-related help desk calls of up to 90%.

While such systems are virtually impossible to fool, veteran users recommend establishing some contingencies such as ensuring that network administrators maintain oversight control over every user or group of users. From time to time, employees do leave companies with no warning, for a variety of legitimate and illegitimate reasons. The company or department must always be able to cancel an account without having access to a particular finger.

Something you have

Fingerprints, like retinal scanning, are considered as authentication based on "something you are." Passwords, of course, rely on "something you know." A third means of authenticating users based on "something you have" is also receiving attention from technology companies. Radio transmitters worn on neck chains, carried in pants pockets or embedded in ID tags can now communicate with computers within approximately 50 feet.

Ensure Technologies, a security systems company in Ann Arbor, Michigan, has introduced a product called *XyLoc*. It consists of a radio transceiver "lock" that plugs into a computer port and a wireless radio transmitter "key' worn or carried by the user. When the user approaches a computer with the lock, the user's key transmits a unique, 32-bit encrypted ID code. The lock verifies the user's identity and unlocks the computer's keyboard and screen. Unauthorized users see nothing but a locked system.

Two options allow *XyLoc* to adapt to environments where more or less security is needed. In low security organizations or departments, the system can be configured to automatically log the user in when the user wearing the key nears the computer. If additional security is called for, perhaps in high traffic areas, users can be forced to select their login name from a list of authorized *XyLoc* users detected in the area. In high security environments, the user can also be required to enter a

Continued on page 7

Passwords Obsolete continued from page 6

password, which will only work, even if correct, when the key is nearby. In all three configurations, when the user walks away from the computer, the account is automatically logged out.

The system uses a technology that Ensure originally developed for public kiosk terminals, XSS, which is capable of handling thousands of users and computers. It can store up to 32 username and password combinations for each user on a given computer. Administrator tools enable workarounds for legitimate users who forget their keys or passwords. It can also be set to encrypt files as they are saved so that data is protected even if login systems should be breached. XSS is based on 300, 800 or 900 MHz radio signals, depending on the country of installation.

If a user forgets or loses his keycard, administrators can suspend that Key and provide a temporary override password. Like fingerprint systems, XSS also creates audit logs. When a user logs on to the network, XSS records how they logged on (with their Key or with an emergency override password) and the time and date of the logon. It also notes every time the user's key card leaves the 50-foot perimeter and returns and it logs each application the user launches.

XyLoc requires a server but its minimum configuration is not sophisticated and it does not have to be a separate box. It will run on Pentium III-class servers with 256 MB memory and 2 GB available disk space, running Windows NT 4.0 (Option Pack 5), 2000 or XP. It also requires Microsoft Internet Information Services (IIS) 4.0 or higher. XyLoc also supports Citrix MetaFrame, Microsoft Active Directory or Terminal Services and Novell eDirectory/NMAS.

Phishers Become More Aggressive

Experts offer tips to educate naïve, trusting computer users

Every day, an estimated 2 billion spam email messages are circulated worldwide. During the past 12 months, $2 billion has been lost due to illegal access to checking accounts. Coincidence? Not according to security experts Mark Rasch, William Malik and Paul Pak, featured speakers last month at a Ziff-Davis seminar. The one dollar per email profit ratio is on the rise and can be directly attributed to computer users, both home and corporate, who have not gotten the word that the Internet is not populated exclusively by saints and legitimate businesses.

In fact, according to Rasch, Chief Security Council for Solutionary, Inc., naïve new-hires are favorite targets of today's phishers. Phishing, as most everyone knows by now, is a sophisticated attempt to steal valuable information such as credit card or social security numbers, user IDs and passwords by delivering spam designed to look like official email from banks, credit card companies, retail stores, etc. (See sample, p.10.) Hackers have learned to build web sites that look identical to official company sites, with the exception of a login box that routes passwords to Russia or Nigeria.

Rasch related the story of a recent attack against a large media company. "On their first day of work, all new hires get employee badges and SecurID cards for internal corporate network access," he began. "They also attend a new-hire orientation where an example of the official corporate format for emails is shown. A warning is also given to protect sensitive information, such as logins and passwords.

"Within one week of a recent orientation, two new mid-level employees received an email in the official corporate format that appeared to come from the IT security department. It said their SecurID cards were expiring and provided a link to follow to re-authenticate the cards. Both did as instructed and entered SecurID serial numbers, corporate usernames, PINs, and tokens as instructed.

"One of the new hires became suspicious after the fact," Rasch continued. "She contacted the Security Operations group a day later to learn that a number of employees received the email, that the email was fraudulent, and that the entire corporate network had been compromised. The IT security department had to spend the time to close security holes, reissue SecurID cards, check all computers for malicious software and trace all account activity."

The implication of such attacks, which are reported to be on the rise, is far-reaching. Once entry is gained to the network through a user account, firewalls and other perimeter security measures become useless because the hacker is now inside the perimeter, posing as a legitimate user. With access to internal systems, hackers are free to engage in billing and invoice fraud, customer or patient account theft or employee ID theft.

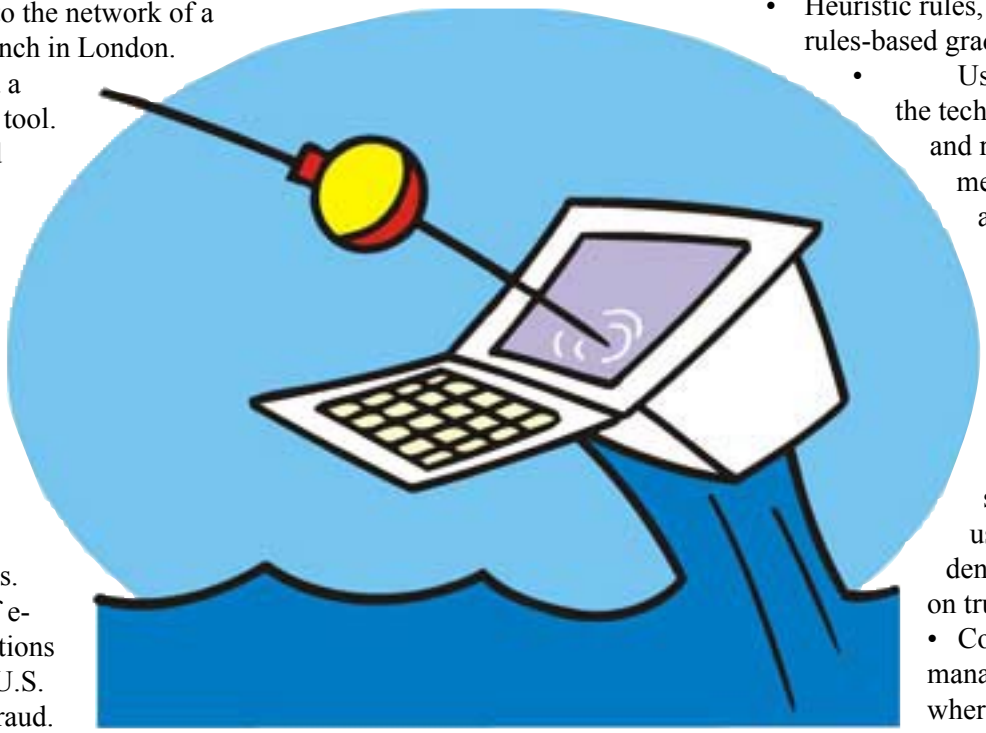
Additional forged messages, sent directly from trusted co-workers' accounts, can phish for access to additional areas within the

Continued on page 8

Phishers Become More Aggressive continued from page 7

organization. Malicious software can be installed and turned loose. Files can be deleted and entire systems brought down.

In another anecdote, Rasch described how this type of attack against new hires may be the way a hacker injected malicious code into the network of a Japanese bank branch in London. The code installed a keystroke logging tool. The hacker gained complete control of the bank until discovered just weeks ago.



Malik, president of his own security consulting company, added a frightening list of additional statistics. Last year, 6.2% of e-commerce transactions carried out in the U.S. were attempts at fraud. More than half of these attempts were carried out by non-U.S. hackers. "Following the United States in the fraud stakes," Malik explained, "was the U.K. (5.25%), while in third place was Nigeria (4.81%), where the 419, or advance-fee, fraud epidemic rages unchecked. Attackers who gain control of web servers use them for both security attacks and fraudulent, e-commerce transactions."

It gets worse. Malik warned that the number of reported security incidents doubled between May and August of 2004 and quoted other findings from a number of research and virus-tracking organizations:

- Ferris Research says the annual cost of spam to U.S. corporations *increased* from $8.9 billion in 2002 to $20 billion in 2003.
- Nucleus Research estimates that the average annual cost in lost productivity to spam is now $874 per employee.
- The cost to spammers, phishers and hackers to create this havoc? $500 per million spam email messages, as opposed to over $240,000 to send out 1 million letters via U.S. Mail.

Time for a new email standard

Paul Pak, CEO of Athena Archiver, attributes the problem to the fact that email has not changed much in its 10 years of existence and popular use. He wants to see email mature to keep up with increasingly capable hackers. Calling for an entirely new email standard, Pak proposes 2-way ID verification. "People believe that certificate-based email, such as what VeriSign offers," Pak said, "is too cumbersome to install and you have to give up too much personal information to get a certificate. We need an easier one but new proposed standards will probably take a couple years."

There are currently four basic email vulnerabilities, in Pak's view, malicious code, unwanted e-mail, identity verification and privacy. We manage malicious code attacks with antivirus software's signature-based code detection method, with active-content removal, which filters potentially malicious content arriving in JavaScript, ActiveX, HTML and .exe files.

Spam management comes in four flavors:

- Heuristic rules, an intelligent, rules-based grading technique
- User-defined spam, the technique of identifying and reporting spam messages one by one and then blocking them. This method is employed by users, companies and ISPs.
- Blacklist/Whitelist, which compiles lists of specific servers or users, permitting or denying delivery based on trust.
- Confirmed user management, a technique whereby recipients perform a manual confirmation step before mail can be delivered.

Identify verification is currently managed with signed and encrypted certificate-based email. Because it is perceived as cumbersome, an email version of Caller ID has been proposed. It might include both a sender ID and a system of domain keys.

Lastly, Pak observes that email privacy is currently ensured by encrypted mail systems, email client protection, "remailers" and SSL protocol encryption. Encryption makes email messages less like postcards, stopping eavesdroppers from reading

Continued on page 9

Phishers Become More Aggressive continued from page 8

messages. Client protection, available with certain email readers and ISPs, blocks web bugs, turns off return receipts and blocks external pictures and links before they arrive at the user's desktop. Remailers are servers that strip out headers, effectively "anonymizing" email messages. SSL protocol encryption uses Secure Socket Layer to encrypt messages between clients and servers.

Pak envisions a future for email when most or all of these measures will be unnecessary but email will be more secure. The problem will be attacked from six directions, reliability, authenticity, encryption, secure clients, anonymous clients and a communications convergence.

"Reliability will be built up by fault-tolerance and reliable systems, which will one day enable a more robust and scalable communications infrastructure," he predicted. He offered his specific vision for how the other five points will soon be addressed.

- Authenticity: Email messages need authentication on a user *and* server level. A proper cryptographic solution involving signing is necessary for validation of e-mail credentials and for trusting the sender of an e-mail message. This prevents spoofing, phishing attacks, and anonymous e-mail. By having credentials for servers and users, enforcement of standards like spam control become possible for law enforcement.
- Encryption: Network eavesdroppers are a great threat to individual and corporate privacy worldwide. Encryption and secure authentication protocols will effectively stop anyone from intercepting private communications
- Secure Clients: Future clients will have much more intelligence in managing high-risk active content. By default, anonymous messages will need to be put in a "sandbox" with no ability to run scripts, HTML or JavaScript, minimizing risk.
- Anonymous clients: In an age where spam will be effectively eliminated, legitimate commercial mail will need a proper channel to reach customers who opt-in for such services. It should be separate and anonymous to prevent abuse by commercial companies
- Communications convergence: Email is only one of a number of communications methods in common use. Users will soon come to expect one central tool to manage all their interactions, including RSS, blogs, email and faxes, all of which will eventually arrive and be sent through a single communication protocol.

In the meantime, Pak offers steps most users can take without significantly lessening their email experience. "Most people never use scripting tools but they leave them turned on anyway," Pak noted. "Turn off JavaScript, ActiveX and HTML and you will be far more secure but, as far as convenience goes, you will hardly notice the difference." He also believes the only reason Whitelists are necessary is because Blacklists are so often inaccurate. Maintain Blacklist accuracy and you won't have to bother with creating Whitelists.

Until new standards appear, he also recommends the use of at least an email encryption tool. "Clear-text email needs to become an unacceptable email protocol," he warns. "It is time to stop sending 'postcards' for the whole world to read."

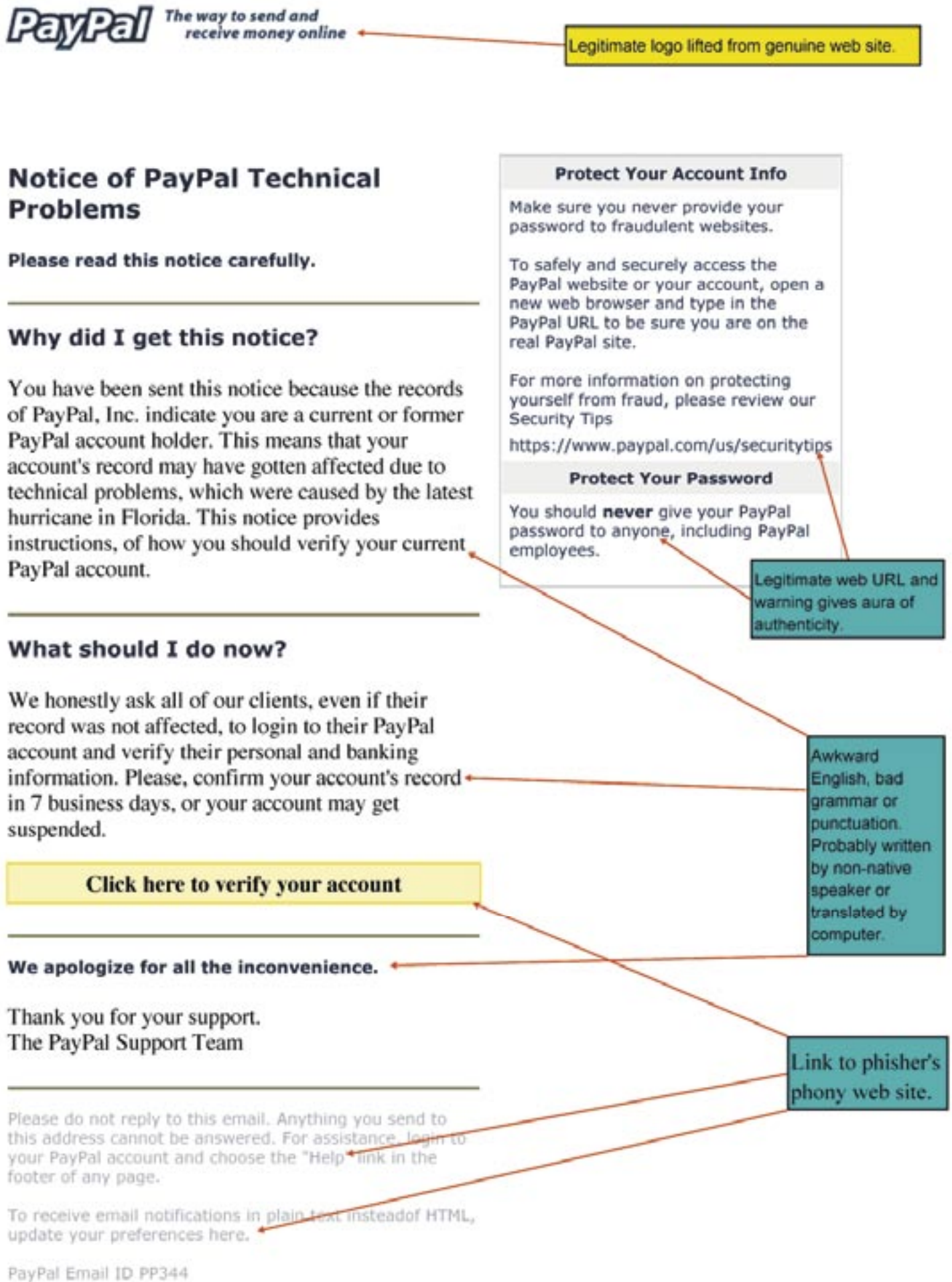
HIPAA Security Tool Available

Stony Hill Management, publishers of HCAR, has reported that its GetHIP software is already in use at nearly 1,000 locations throughout the U.S., making it home care's most widely used HIPAA compliance tool. *GetHIP-Security* is designed to help home healthcare providers comply with the HIPAA Security Rule, which goes into effect this month. The software is highly scalable, with users ranging in size from more than 200 sites to single-site providers with as few as three computers. A version of *GetHIP-Security* is also available for long-term care and assisted living facilities.

GetHIP-Security is the third in a series of HIPAA compliance tools developed by Stony Hill Management. In 2003, more than 500 organizations utilized *GetHIP-Privacy* to achieve compliance with federal privacy requirements, and thousands of staff were trained using the company's HIPAA educational videos.

GetHIP-Security users give the product consistently high marks for comprehensiveness and ease-of-use. The software employs a TurboTax™-like interface, with users responding to a series of questions about their organization's operations and security measures. They are guided through a thorough assessment by the software's unique "HIP Advisor" feature, an in-house consultant that provides implementation advice and step-by-step explanations of regulatory requirements and key security concepts. As users respond to questions, the software automatically builds a work plan, presents sample documents and provides a variety of tools to document and manage compliance efforts.

GetHIP-Security can be installed on a single PC or deployed over a network, and an enterprise version is available for larger providers. A single-site, perpetual software license is $950, with significant discounts available for multi-site organizations. Six months of support and maintenance are included in the initial purchase price. Ordering information is available at www.hipaahomecare.com or by calling 866-436-7047. An evaluation copy of the software can be downloaded from www.gethipsoftware.com/evaldownload.


PayPal
The way to send and receive money online
Legitimate logo lifted from genuine web site.
Notice of PayPal Technical Problems
Please read this notice carefully.
Why did I get this notice?
You have been sent this notice because the records of PayPal, Inc. indicate you are a current or former PayPal account holder. This means that your account's record may have gotten affected due to technical problems, which were caused by the latest hurricane in Florida. This notice provides instructions, of how you should verify your current PayPal account.
What should I do now?
We honestly ask all of our clients, even if their record was not affected, to login to their PayPal account and verify their personal and banking information. Please, confirm your account's record in 7 business days, or your account may get suspended.
Click here to verify your account
We apologize for all the inconvenience.
Thank you for your support.
The PayPal Support Team
Please do not reply to this email. Anything you send to this address cannot be answered. For assistance, login to your PayPal account and choose the "Help" link in the footer of any page.
To receive email notifications in plain text insteadof HTML, update your preferences here.
PayPal Email ID PP344
Protect Your Account Info
Make sure you never provide your password to fraudulent websites.
To safely and securely access the PayPal website or your account, open a new web browser and type in the PayPal URL to be sure you are on the real PayPal site.
For more information on protecting yourself from fraud, please review our Security Tips
https://www.paypal.com/us/securitytips
Protect Your Password
You should never give your PayPal password to anyone, including PayPal employees.
Legitimate web URL and warning gives aura of authenticity.
Awkward English, bad grammar or punctuation. Probably written by non-native speaker or translated by computer.
Link to phisher's phony web site.

CMS Publishes Notice Regarding Security Rule Enforcement

Analysis by Tom Williams, publisher

On March 25, the Feds finally published their proposal for enforcing non-privacy related provisions of HIPAA. As expected, they dropped the ball, calling for a complaint-driven process rather than taking seriously the challenge of adequately securing patient information. One wonders if anyone at CMS is reading the papers and has noticed in just the last two months we have had disclosures of security breaches potentially affecting nearly two million Americans. And those are just the security incidents we know about. Only one state requires security breach disclosures at this time.

Announcement of this complaint-driven enforcement posture is ironic in light of other efforts underway on both state and national levels to beef up regulations protecting personal information. More than 20 states are presently considering legislation requiring public disclosure of security breaches, in response to ChoicePoint, Bank of America and other recent harmful security incidents. Congress is also finally tackling this issue, no doubt because Senators who found themselves among the victims of B of A's latest faux pas (the loss of backup tapes including credit card records of a majority of the Senate) have suddenly developed a new-found interest in identity theft.

CMS's announcement is particularly ironic when contrasted with a recent report from the National Committee on Vital and Health Statistics, one of the key organizations helping shape the President's electronic medical records initiative. NCVHS has called for research into the need for better-defined security standards for healthcare providers. Jeff Blair, co-chairman of the NCVHS Subcommittee on Standards and Security, has characterized the HIPAA Security Rule as a set of general guidelines that do not necessarily define a minimum security threshold that healthcare organizations should provide.

In spite of all this, we are going to rely on complaints to trigger enforcement, in other words, waiting until the damage is done before taking any action to determine if security controls are adequate. Does this sound like a plan? Hardly. It sounds more like closing the barn door after the horses have escaped. It is an approach not likely to stand the test of time.

Full text of CMS's enforcement proposal can be found at: Federal Register / Vol. 70, No. 57 / Friday, March 25, 2005 / Notices; page 15329.

Vendor Watch

Bob Dean returns to home care. Veteran home care IT sales executive Robert Dean chose home and family over career last year when **Misys Homecare** wanted him to move from New Jersey to its new headquarters in Raleigh, North Carolina. In spite of his successful track record and career prospects at Misys, he left the sales organization he had built there for a sales VP position with **MedAptus**, a Boston company that offers PDA-based point-of-care software for physicians. While there, he designed and executed another successful sales and marketing strategy.

Apparently, however, he missed home care as much as it missed him. Late last month, **Viterion TeleHealthcare LLC, a Bayer-Panasonic Company**, introduced Dean as its new Director of Sales and Service. Based in Tarrytown, New York, Viterion provides web-based home telehealth systems to home care providers. Dean brings more than 20 years of sales and management experience to his new company. During his tenure at Misys, its homecare division's sales grew by 800%. Dean also served as Vice President of Script Systems, the physician software business of **InfoMed Holdings, Inc.**, now known as **CareCentric**.

"Robert Dean is a high-energy sales executive whose unwavering determination for winning new business, combined with a passion for marketing strategy, makes him a definitive asset to any organization," commented Dr. Pramod Gaur, President and CEO of Viterion Telehealthcare. "We are delighted that he has joined our growing sales and service organization and we look forward to his many great successes during his tenure at Viterion."

http://www.viterion.com

Third HITC magazine released. HCAR parent **Stony Hill Publishing**, of Fredonia, Wisconsin, lent its editing

Continued on page 12

Vendor Watch
continued from page 11

and production expertise to the **Home Care Information Technology Council** (HITC) and produced a printed guide to 24 leading home care software vendors, service organizations and consultants. The 80-page, full color magazine, **Home Care Technology 2005**, includes information about each HITC member company as well as six major articles by some of the most listened-to voices in the industry. The issue's theme, "Best Practices of the Data-Driven Organization," touches every important stage of the home care workflow process.

HCAR publisher **Tom Williams** opens the discussion with an overview of the critical role technology plays in each agency's survival and growth. **Mike Ferris**, president of consulting firm **Home Care Marketing Solutions**, follows with "Data Determines Sales & Marketing Success," a technology guide for home care sales teams. Jeff Lewis, president of **Lewis, Inc.**, reprises in paragraph and diagram form the presentation that drew SRO crowds at last year's NAHC Annual Meeting, "A Pre-emptive Assessment Model for OASIS."

HCAR editor **Tim Rowan** summarizes the experiences and advice shared in a recent panel discussion among eleven veteran point-of-care automation users and executives from across the country in "How to Benefit from Data Gathered at the Point of Care." **Frank Giannantonio** and **John Morris**, principles of **FGA, Inc.**, share the insights into PPS and insurance billing that they teach to their customers in "Best Billing Practices of the Data Driven Organization." Wrapping up the issue is **Dr. Robert Fazzi**, aided by researchers **Gina Mazza, RN** and **Jo Gladine-DiLorenzo**. "From Data to Benchmarking to Best Practices: How Successful Agencies Get Better Financial and Quality Results" is an exploration into **Fazzi Associates'** years of research into the importance of data-guided benchmarking.

Home Care Technology 2005 will be distributed at no charge by more than 30 state and national associations at meetings and other events held this spring and summer. Members unable to attend their state's meeting can call their association to obtain a copy.
http://www.homecaretechnology.com

Customer relationship management software released.
Home Care Marketing Solutions, of Raleigh, North Carolina, has announced the release of a new, re-written version of *Homecare CRM*, its customer relationship management application for tracking and supporting referrals, prospects and patients. The new version has been redesigned and re-coded on top of **SalesLogix**. The previous version was a customization of **ACT!**. Both base products are now owned by **Best Software**, which provides migration services for ACT! users wishing to upgrade. Though at first glance the two are visually similar, SalesLogix is a far more powerful, SQL-based platform. Like ACT!, it is available in single-user and enterprise versions.

HCMS principle Mike Ferris said that the new product will better serve the needs of agencies with multiple locations and larger sales and marketing staffs. A SQL server is necessary. Licenses are available for up to 20 users and for unlimited users. Options include a standard synchronization server for facilitating communications with remote offices and a PDA synchronization server for organizations that equip sales staff with handheld devices.

http://www.hcmarketingsolutions.com

Sweden, HP collaborate on wireless monitoring device.
Nordic telecommunications operator **TeliaSonera AB** announced last month it is moving into the healthcare market with a new product that lets caregivers monitor patients through a wireless device. A company release said it is launching the product, and associated services, jointly with **Hewlett Packard Company** and Swedish technology company **Kiwok**. To be known as *BodyKom*, the system connects wirelessly to sensors on a patient. When undesirable changes are detected, the appropriate hospital or other health care provider is automatically alerted over a secure mobile network connection. The unit receiving the alarm will also be informed of the geographic position of the patient through the use of GPS technology.

Free Security Rule Seminar Available

Stony Hill Management, publishers of HCAR, has made its popular HIPAA Security Rule seminar available on the Web at no cost to home care, hospice, home infusion and HME providers. This seminar series is accessible from Stony Hill's website and includes four separate modules ranging in length from 30 to 40 minutes. A handout including slides accompanies each module.

Content, which includes audio, video and slides, is streamed over the Web. No special software is required to access and view the sessions but a high speed internet connection is recommended.

Over the last year, more than 4,000 executives have participated in Stony Hill's live Security Rule seminars and workshops. These sessions have been very well received across the country and attendees have consistently given them high marks. This four-part series is based on material used in these seminars and workshops. Topics covered include:

Part 1: Understanding Security Principles and HIPAA
Part 2: Risk Assessment and Initial Compliance Project Phases
Part 3: Administrative Safeguard Requirements
Part 4: Physical and Technical Safeguard Requirements

According to Stony Hill CEO Tom Williams, he is pleased with initial response to his seminar offer and is seeing traffic continue to build daily. "We began widely publicizing the seminar series in late March," Williams said, "and in a little more than a week more than 400 organizations registered. More than 50 different trade associations and vendors are working with us to let their members and customers know about our offer, so I expect this will continue for some time."

Williams plans to make the seminar series available at least through the end of May and noted that industry foot dragging on compliance will likely have him extending that time frame. "This feels much like the industry's reaction to OASIS several years ago," he said, explaining that many agencies took their time complying with that CMS initiative. "Home care providers will eventually get around to complying with this regulation. The increasing visibility of security incidents will ultimately bring them to the realization that this is a serious issue."

The free seminar series can be accessed by registering at Stony Hill's website, www.hipaahomecare.com.

WANT YOUR OWN SUBSCRIPTION?

If you got this copy of HCAR from someone else, you could have next month's issue delivered right to your email box as soon as it is published. Subscribing is easy. Just send us an email message with your name, organization and phone number. Make certain to put the words "new subscription" in the subject line. Or call us at **262-692-2270**. We'll send you the first issue absolutely free. If you like it, and we know you will, you can become a regular subscriber at our low introductory rate of $147 for 12 monthly issues ($110 off our regular price). *Special offer for association members!* If you belong to either a national or state association your first year e-subscription will be only $127. If you belong to both, there's an additional $20 savings, reducing your 12-month e-subscription price to $107. **That's more than 60% off our regular price.**

Publisher Tom Williams
Editor Tim Rowan
Page design Loran Mundy

Home Care Automation Report
is published monthly.
©2005 Stony Hill Publishing
ISSN 1083-5059

Our mission is to provide independent and timely information about how home health care executives use automation to boost productivity, cut costs and improve patient care.

Questions or comments?
Call Publisher, Tom Williams at 262-692-2270
Home Care Automation Report
Stony Hill Publishing
N5837 Kohler Rd., Fredonia WI 53021
e-mail info@stony-hill.com