HOME CARE
AUTOMATION REPORT

Vol. 10 No. 5 ★ May 2005

from Stony Hill Publishing

Home Telehealth: State of the Technology

Issues and concerns have upgraded since last year

Last month's annual meeting of the American Telemedicine Association (ATA) in Denver was replete with reports of new studies showing the effectiveness of remote electronic patient monitoring. Evidence of provider and payer cost savings as well as improved patient outcomes served to settle some old questions once and for all, though new ones were quick to follow. The industry's leading concern going forward appears to be how, rather than whether, to deploy a home telehealth (HT) program.

Few of the meeting's scholarly or anecdotal discussions appeared to be aimed at convincing providers that electronic remote patient monitoring is effective. Rather, the unspoken strategy seemed to be to convince regulators, legislators and payers. Perhaps symbolic of the industry's readiness to look beyond evidence of efficacy to the next step was a question from the floor during a home telehealth-oriented workshop. The questioner put a presenter on the spot

Continued on page 2

Healthcare Hiding from HIPAA

"The regulations are only there because common sense is so uncommon," says former CMS CIO.

Representatives from across healthcare gathered in Baltimore last month to assess the industry's readiness to comply with the HIPAA Security Rule and hear from CMS officials about enforcement plans. Perhaps the most revealing announcement was from Denver-based consultant Steve Lazarus, who said he had received phone calls from five provider organizations in the three weeks before the April 21 deadline asking for help starting a Security Rule compliance program.

The general consensus one week before the April 21 deadline was that compliance probably hovered around the 15%-20% range nationwide. However, federal bureaucrats and private consultants – most of whom are former federal bureaucrats – urged participants to look beyond the deadline and prepare to meet an uncertain, troubling future where security will become increasingly difficult to assure.

Setting the stage for the three-day discussion, former CMS Director of Enterprise Standards John C. Parmigiani, now a VP with Connecticut-based QuickCompliance, Inc., reminded participants that the

Continued on page 6

Inside This Issue

New Home Telehealth Issues continued from page 1

with, "How long do you predict it will be before healthcare providers who do not offer telehealth can be cited for substandard care?"

NEW ISSUES

HT as service

Previous ATA meetings heard endless discussions of the absence of telehealth equipment purchase reimbursement from CMS and other payers, including opinions of whether and when that may change. This year, a more resigned attitude was in evidence. Many presenters proposed accepting the cost of telehealth equipment and starting to think of remote monitoring as a service that happens to require the acquisition of certain equipment rather than a capital expense that happens to be used to provide a service.

Cost report anomaly

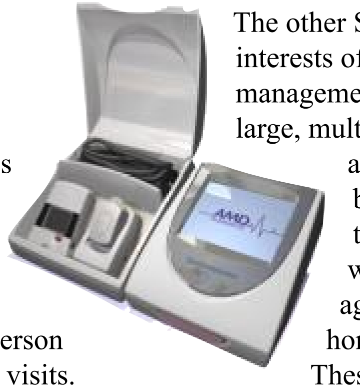
For home care, there is still the issue of Medicare categorizing the equipment for cost report purposes as an administrative expenditure, equivalent to office computers, rather than treating HT as a patient-oriented clinical tool along the lines of a stethoscope or portable pulse oximetry sensor. However, a number of home care presentations mentioned optimism that that policy may soon change.

HT is for everybody

Signs of the industry's maturing approach to telehealth were evident in frequent references to the technology as "one tool among many" in a nurse's or physician's arsenal. Another sign was a new answer to the perennial question about which diagnoses are appropriate for telehealth services. Replacing complex formulae about co-morbidities in specific combinations was new advice to simply monitor everybody, or at least every patient mentally and physically capable of operating the device. For those who are not capable, it was explained, there will soon be passive monitoring devices that will require little if any patient competence.

To be seen or not to be seen

Clearly, the industry is finally realizing that the term "telemedicine" does not convey the same image to everyone. Some vendors offer home telehealth devices that replace in-person visits with virtual, video visits. Others offer computer-like screens instead of cameras; with patients viewing displays with large-type words and images customized to their diagnosis and care plan. Some have neither video nor display screens but instead speak instructions to patients. The simplest do not communicate with patients at all; patients must be trained to hold a stethoscope and fix a blood pressure cuff at specified times and nurses use the telephone when two-way communication is necessary.



Perhaps the most cogent advice of the week came from McKesson's Karen Utterback, who participated in a panel discussion on disease management. Her recommendation is to incorporate home telehealth decisions into care planning for each patient. Instead of choosing a vendor based on whether it uses video-conference or not, choose more than one vendor or choose a vendor that offers options. Then decide, patient by patient, whether to use video or other monitoring systems.

Home care may have waited too long

One last issue that surfaced during the meeting involved a set of assumptions more implied than spoken. There are 12 special interest groups (SIGs) which ATA members can join. This year, the home care SIG emerged as the largest and fastest growing of the twelve. There were constant reminders, however, that it is still only one among twelve, still dwarfed by the combined membership of the other eleven SIGs and still deserving to be treated as a healthcare industry afterthought.

The other SIGs represent the interests of hospitals, disease management organizations and large, multi-physician clinics. An attitude that appeared to be shared among them is that there is no reason to wait for local home care agencies to jump on the home telehealth bandwagon. These other provider groups are moving forward and are purchasing telehealth equipment in substantial numbers. Some are establishing their own monitoring centers, staffed 24/7 with either trained telehealth nurses or low-cost, hourly employees who have access to on-call nurses if needed. The vast majority of presentations reporting findings of fewer re-hospitalizations, reduced office visit and emergent care use and improved patient outcomes, made no mention of home health care services.

Politics makes strange bedfellows, even in home care

NAHC president Val Halamandaris reported to the ATA home care SIG about his member's annual trek to Capitol Hill during last month's Policy Conference. In spite of the "left-handed compliment" nature of what he heard from various agency administrators who managed to schedule audiences with their Representatives and Senators, he did offer one new reason for hope. Apparently, several elected officials who have been steadfastly against home care budget expansion in the past listened with interest when home telehealth technology was explained to them. When they heard that it records and digitally certifies every patient encounter, virtually eliminating any new fraud opportunity as well as

Continued on page 3

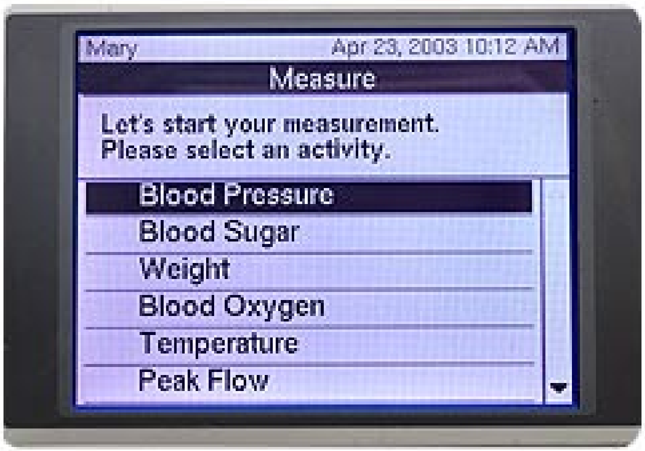
New Home Telehealth Issues
continued from page 2

hampering the use of legacy fraud methods, many of these traditional opponents reportedly said, “Sure, I can get behind paying for that!”

FOLLOWING LEADERS

While many ATA presenters apologized for the limited scope and duration of their studies – most reported on small, pilot projects that show good results but have been in place for less than a year – two stood out because of their sample size and study length.

One was a recent self-assessment by the healthcare arm of the federal Department of Veterans Affairs. The Veterans Health Administration (VHA) offers telehealth services at 21 Veterans Integrated Service Networks (VISN), a program that began in early 1999. Dr. Faith Hopp, Ph.D. presented results of a recent staff satisfaction survey at the Indiana VISN, which has served over 850 patients since implementing its remote monitoring program two years ago. Hopp believes administrator, clinician and referring provider feedback may offer useful insights to civilian providers.



Mary Apr 23, 2003 10:12 AM

Measure

Let's start your measurement.
Please select an activity.

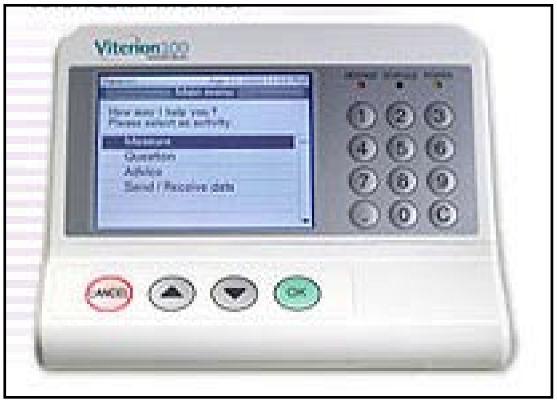
Blood Pressure
Blood Sugar
Weight
Blood Oxygen
Temperature
Peak Flow

A second report with significant participation and duration came from Strategic Healthcare Programs, LLC (SHP). The Santa Barbara, California benchmarking services company reported on an analysis it conducted comparing monitored patients with a control group served by agencies that do not use home telehealth monitors. The study was conducted over a 27-month period and included 478 home health agencies in 41 states. SHP reported that the study was based on analysis of “millions” of OASIS assessments already stored in its databases from its benchmarking customers.

Surprising user reactions

The VHA’s phone-based staff survey established a base line this year and will be repeated in one year for comparison. It included both open-ended and closed-ended questions designed to elicit staff opinions of telehealth across several domains, including:

- Technical issues
- Advantages to staff
- Advantages to patients
- Training/support
- Communication/rapport
- Clinical applicability, and
- Perceived outcomes



Acknowledging the assumption that “home telehealth has the potential to profoundly influence the way in which health care staff members deliver clinical services,” VHA’s Dr. Hopp warned that that potential may be challenged by staff acceptance or non-acceptance. “Initial results indicate that all three stakeholder groups (administrators, clinicians and referring providers) perceived potential for telehealth at the VA,” Dr. Hopp began. “However, there were also group differences in perceptions and priorities.”

She explained that administrators often focus on their budgetary responsibility to make sure telehealth resources are adequately prioritized vis á vis other facility needs. Referring providers were enthusiastic about time saved by reducing the number of patient clinic visits. On the other hand, they were frustrated with organizational problems leading to delays and challenges. Hopp found that nurses were the most enthusiastic about long-term impact on patient outcomes but noted that telehealth’s learning curve was underestimated and detrimental to implementation.

“Data from this study indicate the importance of recognizing the wide variability in perceptions among key internal stakeholders,” Hopp concluded. “Input and support from these groups are needed to address potential barriers to implementation and ensure successful program development.”

Some good comments

Administrators were cautious and budget-oriented, Hopp said. Their concerns revolved around program viability depending on adequate resource allocation and

Continued on page 4

New Home Telehealth Issues
continued from page 3

fiscal realities such as federal hiring freezes and budget deficits. Primary care providers, on the other hand, expressed more enthusiasm, speaking appreciatively of newfound ability to detect early evidence of patient condition changes and to take action before hospitalization became necessary. Physicians were also pleased to note that remote monitoring seemed to inspire patients to pay more attention to their own care.

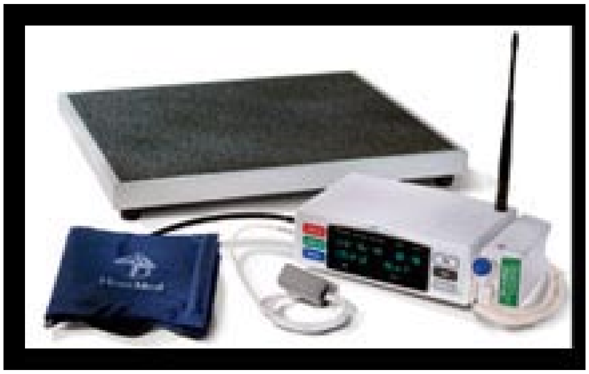
Home care nurses offered the most positive comments, particularly when expressing their hope that more patients will be monitored in the future, especially patients with multiple conditions. Some emphasized the educational role some monitoring devices can play, teaching patients about their condition and any appropriate lifestyle and dietary changes it may have made necessary.

Some bad

No researcher expects, or wants, 100% positive responses and Hopp was not disappointed in this regard. Physician dismay centered on being kept informed. They requested better information about which patients are given monitors and which are not, what happens to a patient after referral to the home telehealth program and about the devices themselves. Physicians want to know enough about telehealth equipment so they can explain it to patients themselves.

Nurse complaints were slightly different. Many said they were not adequately prepared for home telehealth equipment's learning curve. Some worried that productivity would be decreased rather than enhanced at first. Others thought success would never come if they were not properly trained from the beginning. The strongest assertions, however, had to do with inappropriate referrals. One typical commenter complained, "I don't think that the people who are doing referrals are familiar enough with the equipment and what it can and cannot do in order to make the appropriate referrals."

Hopp concluded her revealing presentation with comments from all three respondent categories about outcomes tracking. Administrators, referring providers and nurses want to know aggregate statistics about re-hospitalizations, ER and intensive care usage and condition improvement. They want to know how costs and patient improvement are affected in contrast with non-monitored patient groups.



Sizable study confirms smaller ones

As noted, one of the universal cries at the ATA meeting was from lobbyists who reported that CMS and other payers say they will not be convinced to pick up part or all of the tab for home telehealth equipment until long-term studies of sizable populations, showing cost- and outcome-effectiveness, are completed and verified. A study released at the meeting by SHP and Honeywell HomMed may soon find its way into the portfolios of those lobbyists.

SHP was hired by Honeywell HomMed to determine whether remote monitoring affects outcomes and costs over the long term. By analyzing its large database of OASIS assessments, submitted by its own benchmarking customers between January 1, 2002 and March 31, 2004, SHP was able to draw relatively immediate conclusions based on volumes of historical data instead of having to begin a study and wait 27 months before being able to analyze it.

The SHP study compared outcomes from 178 home health agencies that use Honeywell HomMed monitors against patients served by 300+ agencies that do not use home telehealth systems. Patients were selected for the study if they had one or more of the following diagnoses: Congestive Heart Failure (CHF), Coronary Artery Disease (CAD), Diabetes or Chronic Obstructive Pulmonary Disease (COPD). Some had more than one of these diagnoses; many had them in combination with other conditions. Patients with multiple co-morbidities were more likely to be chosen for monitoring by agencies offering home telehealth services, which weighted the monitored sample generally sicker than the control group.

Results confirmed previous anecdotal evidence – including most of the small, work-in-progress studies presented at the same meeting – that monitored patients use less emergent care, are admitted to the hospital less often, visit their doctor's office with less frequency and become more medication compliant. One factor, though minor, may prevent full comparison of this study's results with those reported by medical clinics, hospitals and disease management companies. Many of those providers had selected other home telehealth devices, with equipment that offers video conferencing, either exclusively or as an option alongside remote vital sign monitoring. Honeywell HomMed

Continued on page 5

New Home Telehealth Issues continued from page 4

does not offer a video option; its devices measure and transmit patient vital signs only.

THE SHP FINDINGS*

CHF average rates

- Hospitalization, not monitored: 10.1%; monitored: 6.2%
- 29 agencies showed zero hospitalization rates_
- ER visit, not monitored: 8.8%; monitored: 4.5%
- 39 agencies showed zero CHF ER visits
- ADL improvement/stabilization, not monitored: 71%; monitored: 75.9%
- IADL improvement/stabilization, not monitored: 58.2%; monitored: 69.1%

Diabetes average rates:

(50% of monitored patients also have CHF)

- Hospitalization, not monitored: 2.4%; monitored: 0.6%
- 109 agencies with 2,316 monitored patients showed zero hospitalizations
- ER visit, not monitored: 1.8%; monitored: 0.3%
- 109 agencies with 2,316 monitored patients showed zero ER visits
- ADL improvement/stabilization, not monitored: 70.4%; monitored: 77.2%
- IADL improvement/stabilization, not monitored: 59.4%; monitored: 70.7%

CAD average rates:

- Hospitalization, not monitored: 15.7%; monitored: 11.2%
- ER visit, not monitored: 12%; monitored: 7.9%
- ADL improvement/stabilization, not monitored: 70.4%; monitored: 77.2%
- IADL improvement/stabilization, not monitored: 59.4%; ADL, monitored: 70.7%

COPD average rates:

(42% of monitored patients, 24% of control group also have CHF)

(57.9% of monitored patients, 46% of control group have "any other co-morbidity")

- Hospitalization, not monitored: 16.8%; monitored, 8.3%
- ER visit, not monitored: 13.1%; monitored: 4.5%
- ADL Improvement/stabilization, not monitored: 71.8%; monitored: 80.3%
- IADL improvement/stabilization, not monitored: 60.8%; ADL, monitored: 77%

*SHP did not include some agencies in its reported averages, explaining, "Certain [monitoring] agencies are intentionally excluded from the population for a particular metric. Factors that contribute to a[n]… agency's exclusion are related to issues such as, a) insufficient data within a diagnosis category, b) insufficient experience with monitoring, and, c) factors that render the agency an 'outlier.' … the report documentation also indicates instances where, if the 'outlier' agencies are included, there is no adverse effect on the results."

Any study funded by the organization most likely to benefit from the exact findings that the study produces is always quoted with disclaimers but this one offered results in line with other reports presented at the ATA meeting. It appeared as one of thirteen briefings in a focused educational track titled, "Telemedicine Success Stories." Exhibitors and their customers were given 20 minutes to describe their standout programs. Though only two had a home care orientation, all 13 claimed drastically reduced hospitalizations, virtually eliminated ER use and less frequent physician office visits.

Sentara Home Care Services of Chesapeake, VA discussed its use of ViTel Net's "ViTelCare™ system and the VNA of Somerset Hills, NJ offered results of four years of virtual videoconference visits with CHF patients using units from American TeleCare, Inc.

Sentara's results were similar to those reported by SHP. The 100 year-old VNA's list of home telehealth benefits expanded to include improved patient satisfaction, shortened home care lengths of stay, improved compliance with medical regime and diet and reduced depression and feelings of isolation through active participation in their own care.

Brief summaries of home telehealth companies that exhibited their products at the meeting can be found in this month's Vendor Watch Special ATA Edition, page 11.

Healthcare Hiding from HIPAA continued from page 1

current Security Rule is nothing more than what the government thinks healthcare providers should be doing about security *today*. "The legislation says," he emphasized, "that any of these regulatory requirements only have to stay in place for one year, after which they can be enhanced." (see related story, page 10.

Parmigiani should know. During his days as a federal employee, he chaired the Government-wide HIPAA Administrative Simplification Security and Electronic Signature Standards Implementation Team, was a member of the federal committee that oversaw the development and implementation of the HIPAA Transactions and Code Sets as well as the Privacy Rule and helped develop national policy for electronic health care information security and privacy. He recommended the industry keep a close watch on what his former co-workers in Baltimore and Washington do next.

In addition to future federally enhanced security regulations, Parmigiani also urged providers to stay abreast of developments in three key areas:

- Coming technologies that will better enable healthcare security
- The impact of new IT developments such as Electronic Health Records (EHR), Regional Health Information Organizations (RHIO) and the National Health Information Infrastructure (NHII)
- The effect of recent large-scale security breach incidents on Congress and the public.

Paranoia over identity theft, he added, is increasing not only on Capitol Hill but among healthcare consumers at large. Providers should become accustomed to being repeatedly asked, "Why are you collecting this data? What are you doing with it? How are you protecting it?"

Addressing your adversaries

Characterizing the real-world security threat in military terms, Ronald Ross, Ph.D. of the National Institute of Standards and Technology (NIST) Information Technology Laboratory warned that "your adversaries will always attack your weakest link." Those adversaries, says Ross, threaten far more than electronic personal health information, they threaten an organization's ability to compete. Security, according to NIST, is not merely a defensive reaction to realities of a connected business environment; it is a confidence builder between business partners.

"Security creates visibility among mission partners," Ross believes. "Developing your own security safeguards is good from an internal due diligence perspective because you have to attain compliance and secure your own networks. But eventually that critical data that you process and store within your system may be transmitted over a network to be shared with a business partner."

Implementing commonly accepted security practices and adhering to published guidelines establishes a normalization among partners so they can reach a mutual understanding of due diligence and know what to expect of each other when they exchange critical health information. "Look at it as a chain of confidence," Ross explained. "Every link in the chain, representing components of your security program, contributes to the overall strength of the chain. A person with dishonorable intentions does not have to defeat your entire program, just compromise one link in the chain."

Examples of Ross's point can be found in recent headlines.

- ChoicePoint had excellent firewalls and security policies but criminals gained access to records by posing as legitimate customers.
- San Jose Medical Group had trained its employees thoroughly about inappropriate disclosures of patient information. Then thieves broke into their building, which had no alarm system or surveillance cameras, and beat down a locked computer room door, walking away with two computers that stored patient billing information.

Continued on page 7

Healthcare Hiding from HIPAA continued from page 6

- The IRS has arguably the world's strongest IT security systems after the CIA, but they become totally ineffective when employees fail to follow procedures. In a recent test, 35% of employees gave their login IDs and passwords to auditors posing as help desk personnel.

Weakest link may be in the next cubicle

Greeted by audience gasps, Parmigiani and Ross presented statistics demonstrating where an organization's greatest risk is typically found. Depending on which report you choose to believe, employees are responsible for 50-80% of security breaches. The higher number results when accidental disclosures are included along with intentional acts.

According to February 2005 NIST recommendations regarding security controls (http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf), organizations attempting to prevent internal breaches should put three policies in place. Ross strongly recommended pre-employment background checks, separation of duties so that two persons are required to perform certain critical tasks, and a "least necessary access" policy. Ross emphasized that technical and physical security safeguards, such as intrusion detection systems, firewalls, encryption and audit mechanisms, must be supported by corporate security policies, including an initial risk assessment, contingency planning, awareness training and ongoing security assessment and planning. "And vice versa," he added. "Neither administrative policies nor technology can create a secure environment on their own."

The key to any good security program, the entire panel concurred, is balance. No matter what the sales rep with the latest gadget says, there is no technological silver bullet that will "make you secure." Balance policies and procedures with gadgets and know where your weakest link is.

Most presenters were at a loss to explain why healthcare has been so slow to complete HIPAA Security compliance tasks. Uday Ali Pabrai, HIPAA Academy CEO, travels the country as a consultant and claims he has not encountered a single organization that was on schedule to achieve compliance by last month's deadline. "There is no such thing as a 100% secure organization," Ali Pabrai proclaimed, "but there are few healthcare provider organizations that are anywhere close."

The most serious deficiency appears to be in the area of contingency planning, a core HIPAA Security Rule requirement. The primary reason, according to Ali Pabrai, seems to be that provider organizations regard the Security Rule as an unfunded investment without a return. He hears frequent complaints that money spent on security safeguards and staff training is money lost. He does not hear those complaints, however, from customers who hire him *after* a breach has occurred.

Gary Christoph, Ph.D. agrees with Ali Pabrai. The former CMS CIO drafted many HIPAA sections, including the security regulation, and is now Senior VP for Government and Healthcare for Seclarity, Inc. (San Francisco, CA). He noted that security experts repeat the theme that security is about common sense, not about regulations. "The reason the regulations are there is because common sense is so uncommon," he half-joked. "Network security is difficult and it is expensive. If it weren't for HIPAA and other federal mandates such as Sarbanes-Oxley, many businesses would not do what they ought to do to protect customer and patient privacy."

Christoph continued to pelt the audience with metaphors. "The quickest way to drive across town is to pick the most direct route and then ignore red lights and stop signs," he said. "The safest way might take a little more time." The security balancing act, in Christoph's view, is to keep a network safe from intruders without keeping people from doing their jobs. If people are forced to look for ways around security to get their job done, your security is probably too tight.

"You need to learn the M&M model of security implementation," Christoph continued. "You want a hard shell on the outside but a soft center. A hacker wants to become an insider by getting through your perimeter with legitimate passwords or through holes opened up by email or instant messaging. Once inside, he has the same power as your staff." A new tool from the Trusted Computing Group, an industry association made up of chip makers, hardware manufacturers and software developers, is a firewall that encrypts internal as well as transmitted data. It will be useful, in Christoph's opinion, because "people are unreliable, yet we give them near-infinite power in the form of desktop computers."

There are three critical obstacles to achieving security, Christoph believes.

- People are involved. People are neither uniform nor logical and they make inappropriate assumptions.
- Technical solutions are too complex. Purchasing "point products," multiple solutions each aimed at one problem, is like tiling a floor with some triangular tiles, some hexagonal, others square. They don't completely cover the floor. In addition, every time technology advances, new

Continued on page 8

Healthcare Hiding from HIPAA
continued from page 7

vulnerabilities are introduced, wireless networking being the latest example.

- Administrative solutions that are not solutions. Tight processes interfere with work, leading to policies violated without management knowledge or without consequences, until there is no more security.

Internal firewalls and encryption may protect an employer from insider security breaches but it might also halt important work.

What the other 80% should do

Ultimately, conference presenters agreed, the value of achieving business security may have become more visible to healthcare administrators as a result of the Security Rule or perhaps through the almost daily news reports of security breaches. One thing, however, is certain. Security's lifespan as a major business concern stretches from April 21, 2005 through the day that administrator retires. The estimated 80% of providers that were not compliant by the deadline should continue to push forward. As our next story details, non-compliant providers making a good faith effort to achieve security will fare much better with CMS investigators – not to mention with a barrage of hackers – than non-compliant providers who appear to have taken a cavalier attitude.

The Eleventh National HIPAA Summit will be held in conjunction with The Second HIT Summit, September 7-9, 2005 in Baltimore.

Feds Put Some Meat on HIPAA Enforcement Bones

Just days after announcing they would implement a primarily complaint-driven enforcement approach for non-privacy HIPAA elements, the Fed's began to provide insights into how the process will work. We can now see the degree to which they will pursue enforcement action with regard to non-compliant providers. Those who would like to have seen CMS take a tough stance will view the process as deficient. Those looking for any sign that the Fed's take security seriously may find a glimmer of hope in these latest pronouncements.

In a presentation at last month's HIPAA Summit, two DHHS staffers reviewed enforcement efforts that have taken place to date and outlined the proposed complaint-driven process for the Security Rule. Just a week later, CMS sponsored a national conference call covering much of the same process-related ground. Finally, a week later on April 18th, DHHS published its proposed HIPAA enforcement rule for public review and comment. http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/pdf/05-7512.pdf

CMS Weighs In

Brad Peska, with the Office of HIPAA Standards (OHS), was CMS's official spokesperson at the recent Baltimore HIPAA Summit. He was also one of the primary presenters on the subsequent CMS conference call. Among Peska's insights:

- Anyone can initiate a complaint, not only the injured party.
- An online complaint form is available on the CMS web site.
- Decisions have yet to be made regarding monetary penalties.
- Covered Entities (CE) will be accountable for the actions of their Business Associates (BA). Whether a CE is permitted and/or required to monitor BA activities depends on their contractual relationship. There is no specific Security Rule requirement.
- If a complaint is filed against a provider, they may never hear about it. Public reports will include closed cases only.
- "Primarily" complaint driven means that CMS has the ability to look into violations where no complaint has been registered. Peska added that his office does not know yet whether or how it will use that power.

Peska's most significant announcement at both venues was that OHS will look for good faith efforts, even if they occur after a complaint investigation has begun. He stated, "If a CE fixes a problem as soon as a vulnerability is discovered, even if it is discovered only after a breach has occurred and a complaint has been registered, we will probably move toward closure." The worst case will be that of a CE that is the subject of a complaint and can show no previous HIPAA Security compliance activity.

What Can We Learn From Recent Events?

Complaints regarding Transaction and Code Set violations are filed with CMS, as will be Security Rule violations. Privacy Rule complaints are directed to the DHHS Office of Civil Rights (OCR). Examining what has transpired since these requirements became effective (October 2003 and April 2003 respectively) may shed some light on what to expect from CMS with regard to security-related complaints.

Peska reported that CMS has handled only 325 TCS complaints since October 2003. This is as expected, as there is little reason to believe a

Continued on page 9

CMS' HIPAA Enforcement Plans
continued from page 8

complaint would be filed against a payer that continued to process claims even though they were submitted in non-compliant formats or used non-standards codes. Provider fear of payer retaliation may also play a role in the small number of TCS complaints filed thus far.

Privacy complaints, however, have been another matter. OCR chief Richard Campanelli reported that 12,000 privacy complaints have been filed in the two years since that rule became effective. Two-thirds (65%) of these have been "resolved," which could mean adjudicated or dismissed. Nearly 200 were referred to the Justice Department for criminal investigation. Campanelli could not say how many of those would actually be prosecuted.

OCR has chosen not to impose fines in cases where the privacy violation resulted from ignorance (though he noted that excuse loses credibility with each passing month), where the violation could not have been prevented by the CE or where criminal penalties are likely. Campanelli added that OCR has 250 FTE investigators working out of 10 regional offices. They are enabled to operate with a great deal of discretion.

Campanelli explained that when a CE cooperates with investigators, they are quick to allow extra time to resolve a problem. However, the law does not permit investigators to take intent into consideration. They are empowered to note when a violation occurred "knowingly" but they do not look at "willfully." The law only mentions intent with regard to acquiring and selling personal health information. Peska and Campanelli agreed that there is considerable overlap between the Privacy and Security Rules and that CEs can expect CMS to imitate many of OCR's procedures.

The Ballgame May be Changing

While intent has not played a prominent role in enforcement to date, that may be changing. With publication of its proposed enforcement rule, DHHS spells out the process it will follow to investigate and adjudicate HIPAA-related complaints. The document details, in language only an attorney would appreciate, the steps both DHHS and CE's must follow when a complaint has been filed. It also explains the bases on which a CE can defend its actions and DHHS investigators can look the other way (what oftentimes appears their preferred means for handling complaints).

What is obvious in reviewing the proposal is the Fed's interest in implementing a consistent process for dealing with all complaints, regardless of the particular aspect of HIPAA involved. Citing the DHHS Secretary's interest in "One HHS," the CMS document says a uniform policy is being adopted to encourage voluntary compliance through education, cooperation and technical assistance. The proposal goes on to note however, that the department's complaint-driven enforcement activities may be expanded to include compliance reviews. Regardless, attempts will usually be made to resolve matters informally before pursuing legal action.

Good Faith Efforts vs. Willful Neglect

From our initial review of the Fed's proposal, it appears they intend to continue to give CE's the benefit of the doubt if they can demonstrate that a good faith effort has been made to comply with the various HIPAA requirements. We find it quite significant, however, that they take a marked departure from their "look the other way" posture when they introduce the concept of "willful neglect." This may alter the calculus of those providers that have chosen to ignore the regulations, expecting little meaningful enforcement.

The proposed rule spells out in great detail when and how a CE can avail itself of an affirmative defense should a complaint be filed against it. While a number of doors are left open providing ample opportunity for providers to explain away their non-compliance, one is firmly slammed shut. If it can be demonstrated that an accused CE has willfully neglected compliance with the regulations, an affirmative defense is not available when the allegation is adjudicated. The proposal defines willful neglect as "…conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."

Premium on Documentation

This enforcement approach is not unexpected. It places a premium on documenting steps one takes to address compliance. If a provider can demonstrate it has made a good faith effort to comply, the Fed's are quite clear how they will respond: they will try to work things out. On the other hand, if a provider has chosen to ignore the regulation for whatever reason and reasonable efforts to comply cannot be demonstrated, the Fed's are likely to take enhanced punitive action.

Noting the significant level of Security Rule non-compliance evidenced in recent surveys across all healthcare industry segments (the most recent polls put it at about 20%) the Fed's will give providers time beyond the recently passed deadline to comply. At some point in time, however, expect their patience to wear thin. Particularly if major security incidents such as those widely reported in recent months continue and if Congress responds by moving forward on proposals to require disclosure of security breaches. Providers who have failed to take any action to comply or to document their compliance efforts will then find themselves squarely in the enforcement crosshairs.

Some Providers Laugh at HIPAA's 'Simple' Requirements

TriCare participants and rehab facilities have a far steeper climb to compliance

The HIPAA Security deadline has just passed and chances are you are among the estimated 80% of providers who say they still have work to do to become compliant. The last thing you need to hear right now is that it could be worse, but it could. For participants in the military's TriCare system and drug rehabilitation facilities, it already is. Are their stringent privacy and security requirements coming to home care? Some say it is possible.

DITSCAP

TriWest Healthcare Alliance, a records company in the Department of Defense's TriCare system, instituted new contractor requirements after computers and files were stolen from its Phoenix offices several years ago. TriWest has decreed that all U.S. Family Health Plan (USFHP) healthcare providers must attain Defense Information Technology Security Certification and Accreditation Process (DITSCAP) certification.

DITSCAP has been called "HIPAA on Steroids." Like HIPAA, it addresses physical, administrative and technical infrastructure but has none of HIPAA's flexibility for providers of different sizes and resources. There are no addressable specifications; everything is required. Enforcement will be proactive rather than complaint-based. An onsite, JCAHO-like survey must be passed *before* a provider may participate.

Consultant Wayne Mackert, speaking of his work with a large Washington state practice, said a DoD inspection team paid the facility two visits, eight weeks apart. During the first, consisting of 10 24-hour days, the team uncovered 58,000 security vulnerabilities and described them in a 6,000-page report. During the second visit, expectation for a passing grade was to find zero unmitigated vulnerabilities and documentation explaining how all 58,000 were mitigated. Mackert said the clinic passed after eight weeks of concentrated effort, including additional staff, technology upgrades, including upgrading all servers from NT to Windows 2000, and considerable expense.

42 CFR Part 2

The Federal Confidentiality Law Specific to Alcohol/Drug Services makes HIPAA look like a stroll in the park, according to Janelle Wesloh, Director of Privacy Operations for the Hazelden Foundation in Center City, Minnesota. 42 CFR Part 2 (42) is the result of a 1992 consolidation of two laws enacted in the early 1970's, one for alcohol rehab facilities, the other for drug centers.

Under 42, all alcohol and drug abuse patient information must be protected and cannot be discussed with anyone. If a person obtains knowledge from some outside source – even if it is directly from the patient or from a newspaper – that an individual was admitted to a program, a staff member cannot acknowledge that such information is accurate.

42 requirements supersede law enforcement interests, even with a subpoena. Program staff *memories and impressions* are considered "records" protected by the regulations even if they are never recorded in any form. A payer or funding source that maintains records of a recipient of drug/alcohol treatment becomes subject to 42 to the same extent as the rehab facility.

Wesloh spends a significant portion of her time determining whether 42 or HIPAA applies in specific situations. "Generally, the more recently enacted 'wins,'" she said, "but not if the earlier law has a more narrow, precise or specific subject. And not if the later law addresses an issue on which the earlier law was silent."

Basically, 42 starts with an opposite point of view from HIPAA's Privacy and Security Regulations. "42 *prohibits* all disclosures except any specifically mentioned as allowable," Wesloh added. "And that short list is limited to medical emergencies, crimes committed on the premises, child abuse and written authorization. Even internal staff discussions must adhere to strict 'need to know' rules." Where HIPAA makes exceptions to its "minimum necessary" limitation for disclosures for treatment by other providers, to HHS for compliance and enforcement, pursuant to a consent or required by law, 42 limits *all* disclosures for any reason to that information which is necessary to carry out the purpose of the disclosure. Only disclosures to the patient are excepted.

42 requires patient consent for disclosures for payment. Only persons who have been legally appointed the patient's guardian can sign consent forms; HIPAA permits personal representatives with power of attorney. During medical emergencies, HIPAA allows providers to inform family members of the patient's location and condition; 42 strictly limits this information to medical personnel.

Since the very presence of a person in a facility dedicated to substance abuse rehabilitation indicates too much about their condition and diagnosis, 42's most stringent provisions affect those organizations. However, some provisions cover any healthcare provider offering substance abuse rehab services. Wesloh said Hazelden is covered by these two federal and six state privacy and security laws. Determining how to proceed without violating the one that applies in a given situation is nearly a full time job.

Will one or both of these super-privacy/security regulations influence future enhancements to HIPAA? Mackert and Wesloh seem fairly certain that some provisions will ease their way from military and rehab providers into a broader healthcare market. Stay tuned.

VENDOR WATCH - Home Telehealth Special Edition

(regular Vendor Watch topics begin on page ***14****)*

More telemedicine companies than ever demonstrated an interest in home telehealth at the traditionally hospital- and physician-oriented American Telemedicine Association annual meeting in Denver last month. Here is our rundown of who was present and what they were saying about themselves, along with our objective interpretation.

One insight that should jump off the page is that there is still no single, neat definition of "Home Telehealth." Technical device variations combined with wide-ranging pricing models make vendor evaluation and selection a complex process. Some may decide that a combination of vendors is a sensible choice. Others may look for one vendor with a variety of technical features or multiple business models. Many will be concerned first about price, hopefully also about cost-effectiveness. Here is a list of other variations to consider as you read through these summaries.

- Purchase or lease vs. rent. You will either own the equipment (and hire sufficient staff to deliver, pick up and disinfect it between uses) or order it to be sent via FedEx from the vendor directly to each new patient. Consider: obsolescence, repair and replacement; unused units gathering dust, the ability to quickly respond to multiple unexpected admissions.
- Video vs. vital sign monitoring: They are both called home telehealth but they are as different as planes, trains and automobiles. Do you need all of one or the other or a mix? Consider: video is most like an in-person visit, saving nurse travel time but requiring one-on-one attention; vital sign monitoring allows one nurse to evaluate a range of measurements with dozens, even hundreds of patients but only offers a view of digital data, not the patient.
- One-way vs. two-way communication: Attach a stethoscope, scale and BP cuff to a phone line and you receive information about a patient. Put a small computer screen at the patient's bedside and you can deliver customized instructions, teaching materials and warnings. Consider: what is your typical patient population, age, education, income-level, rural distance factor? What diseases and conditions do you plan to select for your monitored patient category? Budgetary restrictions are important here.
- Standalone vs. integrated/interfaced data: One home care software vendor has produced its own home telehealth system, another has incorporated an existing one into its family of products. Alliances are becoming more frequent between home telehealth companies and billing and clinical software developers. Most implementations still exist in silos, keeping telehealth data separate from core systems, sometimes keeping the monitoring station entirely off the network. Consider: how important is it to you to incorporate patient vital sign data into your primary clinical and billing system? Have you developed a clear list of pros and cons before talking to vendors?
- Owned vs. hosted data: Some systems establish direct connections from each patient's home to an application residing on an agency PC or server. Others have the home unit dial an 800 number and transmit to a central, secure web server or server farm. Agency clinicians and designated primary care physicians access patient data on a web site. Consider: isolated data can only be accessed from one computer in the agency; web-based data can be viewed anywhere, by anyone. Does your care model call for consultations between your field nurses and the patients' primary care physicians or nurse specialists? Are your referring physicians likely to check on their patients on a web site? Would that feature be a marketing advantage on which you could capitalize?

ADT Home Health Security Srvcs
Palm Harbor, FL

A division of **ADT Security Services, Inc.**, a **Tyco** company, **ADT** more often sells its emergency response service directly to the consumer, though it will work through hospices and home care providers. In addition to a 24/7 call center, ADT places small, wireless, motion sensors throughout the home. The central computer behind the sensors "learns" normal patterns of daily activity and reports abnormalities. Following a triage algorithm, call center staff notifies emergency response services, home care or hospice nurses or family caregivers by phone, secure web page, text message or pager.

http://www.adt.com

AMD Homecare
Lowell, MA

CareCompanion is an FDA-approved, two-way monitor that records vital signs via wireless peripherals and transmits patient information to a server through a standard phone line. It delivers customized assessment questionnaires and event reminders to the patient through a large-type, touch screen. AMD offers an optional video phone but most off-the-shelf video speaker phones are supported. On the

Continued on page 12

Vendor Watch Home Telehealth continued from page 11

agency side, *Nurse Station Software* analyzes and stratifies vital sign data on a standard Windows PC.

http://www.amdtelemedicine.com

American TeleCare, Inc.
Eden Prairie, MN

The home telehealth pioneer has been around since 1993. Today, in addition to its flagship video phone system, it offers options that cover nearly the entire decision matrix outlined above. Members of the FDA-approved **ATI** product family include simple, one-way, stethoscope over phone line units, two-way bedside units with large-print touch screens, wired and wireless peripherals, and both in-house server and hosted web server options. Two-way audio/video virtual visits can be combined with real-time medical peripheral operation. For wound-care, ATI's *Video Patient Station* can download high-resolution digital snapshots.

http://www.americantelecare.com

Caregmatix, Inc.
Chicago, IL

Founded in 2001 by three engineers, Carematix markets its system mostly to disease management companies, insurance companies and self-insured employers, though it does have a few home care and hospice provider clients. The *Carematix Wellness System* is a low-cost, one-way vital sign measurement and transmission system that features wireless peripherals and an open systems design that permits interfaces with multiple device brands. Patients already using a glucose monitor can often continue using the same one. A centrally located wireless hub can communicate with peripherals up to 100 feet away, allowing the patient to leave the bathroom scale in the bathroom. Data is forwarded to a web site for caregiver monitoring. Patient interaction can be done via Interactive Voice Response (IVR) or standard video phone.

http://www.carematix.com

Cybernet Medical
Ann Arbor, MI

Remember Tang? **Cybernet Systems Corporation** develops products for NASA and the U.S. military and then spins off commercial corporate divisions when one of its creations is deemed to have a wider market application. **Cybernet Medical** offers the *MedStar™ Remote Data Collection System*, originally built for astronauts. It collects and transmits blood pressure, weight, pulse oximetry, respiration values, blood glucose and EKG from the patient's home to the caregiver, either via a web-based clinical information system or directly to a standalone system. A companion product, *PALStar* (for Patient Activity Log), allows for two-way communication of customized questions and answers between caregiver and patient. Decision matrix logic selects subsequent questions based on patient answers.

http://www.cybernetmedical.com

Health Hero Network, Inc.
Mountain View, CA

The *Health Buddy* system is a two-way communication device that forwards patient vital signs to a central web server and provides the patient visual and sound reminders, customized questionnaires and disease or condition education through a large-print touch screen. The system includes content development tools so caregivers can customize content for each patient. Two monitoring devices are available, *Health Buddy* and *Health Buddy II*. The newer device, which received FDA approval last month (see page 15), is smaller but offers more peripheral connection ports, including four USB ports, so patients no longer have to swap cables in and out of one port to perform multiple measurements.

http://www.healthhero.com

Honeywell HomMed
Brookfield, WI

The *Honeywell/HomMed Health Monitoring System®* consists of two FDA Class II medical devices. *Sentry*, the full-featured model, and *Genesis*, the more economical version, are one-way communication monitors with voice prompts that guide patients through the use of attached peripherals up to four times per day. Both models can also be programmed to ask a series of subjective, disease-specific questions which patients answer by touching buttons. *Sentry* accepts multiple peripherals attached simultaneously, including glucose meter, peak flow meter/FEV 1, spirometer, PT/INR and ECG. A multiple-user card reader for multi-resident environments, a digital camera or videophone can also be attached. *Genesis* measures heart rate, blood pressure and weight. Units can be upgraded in the home through Smart Media Card technology.

http://www.hommed.com

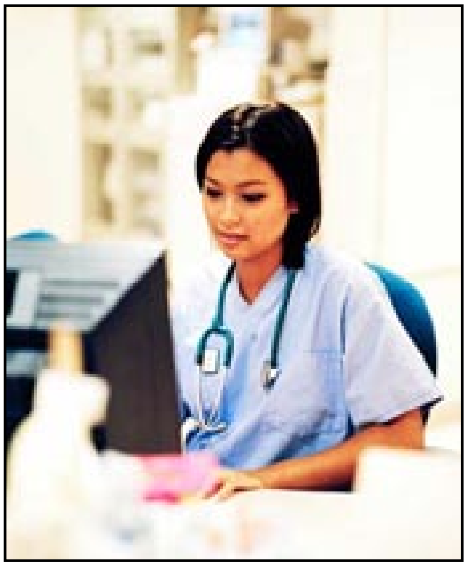
Continued on page 13

Vendor Watch Home Telehealth continued from page 12

LifeLink Monitoring
Lake Katrine, NY
A creative business model makes **LifeLink** a consideration for providers who want to start a home telehealth service but do not want to invest capital in home telehealth equipment. Once they determine a new patient is appropriate for monitoring, LifeLink customers submit a one-page enrollment form to the company. LifeLink delivers its monitoring kit to the patient by FedEx. If necessary, a nurse can set it up and train the patient in its use but many patients can follow the large-print, laminated instruction card and do it themselves. Setup involves little more than attaching the unit to a phone line. The battery-powered unit is about the size of a cigar box and the peripherals are wireless. Patients send their vital signs with a single button and then pick up the telephone handset to answer subjective questions via an IVR system, which has been customized to their disease or condition. At discharge, the patient or nurse re-boxes the equipment and calls FedEx for pickup. LifeLink sanitizes equipment between uses.
http://www.llmi.com

Patient Care Technologies
Atlanta, GA
The first home care software application vendor to develop its own home telehealth system, **PtCT** offers *well@home*®, an FDA-approved, two-way communication system. Patients interact with an 8" touch screen to answer subjective questions and receive education and instructions based on their physician's plan of care, as well as reminders tailored to his/her plan of care and daily routine. The *well@home* bedside device includes BP, Pulse Oximeter, Temperature and ECG measurement devices and contains a modem for communication with a web browser management system. Ports enable connection with other external physiologic measurement devices such as a digital scale or glucometer and battery backup for portable use or use during power failures.
http://www.ptct.com

SCOTTY Technology of the Americas, Inc.
Wilmington, NC
SCOTTY is an international videoconference technology company that has recently introduced a home telehealth system, *CareStation*. FDA 510, Class II Medical Device certified, the *CareStation* product line includes video phones with vital sign measurement connection ports. One model connects over standard telephone lines and another over public IP or H.323 PSTN video conference systems. A PC-based agency application receives and organizes patient records. Available peripheral measurement devices include Peak Flow, Stethoscope/Stethophone, BP, Weight Scale, Blood Glucose, Fetal Monitor and Pulse Oximeter.
http://www.scottygroup.com/telehealth



ViTel Net, Inc.
McLean, VA
ViTel Net established itself in hospital telemedicine before developing a home telehealth version of its ViTel*Care*™ system. ViTel*Care Turtle* is a one-way communication, touch screen device with peripherals for measuring SpO2, blood pressure, pulse, temperature, blood glucose, and weight. A video camera can also be attached. ViTel*Care Patient Care Management* is a desktop PC application that receives transmissions from patient homes and creates a database that can serve as an electronic health record. ViTel Net also offers transport monitoring, clinic/hospital telemedicine, tele-rehabilitation and assisted living health kiosks.
http://www.vitelnet.com

Viterion TeleHealthcare LLC
Tarrytown, NY
Viterion Telehealthcare, a Bayer-Panasonic Company, offers two in-home units, one with more features, the other lower-priced. Both are two-way communication, FDA-approved devices that transmit patient vital sign measurements to a secure web site. The *Viterion 100 Home Telehealth Monitor* is a bedside unit that measures BP, Blood Oxygen, Blood Sugar, Weight, Temperature and Peak Flow. Case managers can change measurement schedules and patient instruction materials through a web connection. The *Viterion 500 Home Telehealth Monitor* adds real-time video conferencing, digital photography, stethoscope and ECG. Both models offer personalized advice messages, schedule reminders and a large-print touch screen user interface. Physicians can be given access to their patients' information on a secure web site.
http://www.viterion.com

Continued on page 14

Vendor Watch Home Telehealth continued from page 13

WebVMC
Conyers, GA
WebVMC, LLC has put a Windows PC into the typical home telehealth bedside device form factor, enabling customizable, two-way communication and software enhancements without requiring equipment change. WebVMC's *RemoteNurse*™ system monitors **ECG, Blood Pressure, Weight, Pulse-Ox, Blood Glucose, Peak Flow and PT/INR**, up to four connections at a time. The *RemoteConsult*™ model adds two-way voice and video communication and can be set to provide threshold alerts when patient measurements go outside a set range. WebVMC is also the first home telehealth company to have announced the addition of the *Zoe*™ skin resistance monitor for CHF patients (see below).

http://www.webvmc.com

ZOE
OMNI Medical Supply
Walled Lake, MI
The *ZOE™ Personal Impedance Monitor* is a new peripheral device that will soon be available with many of the above monitors. It checks fluid levels to detect an impending CHF attack earlier than existing methods. By measuring thoracic base impedance or "ZO" – the time it takes a small frequency electric current to travel from the top to the bottom of the thorax – the ZOE™ monitor detects fluid congestion or dehydration two weeks before weight gain occurs or breath capacity decreases. An FDA-approved product, ZOE™ is being marketed by **OMNI Medical Supply, Inc.** of Walled Lake, Michigan, primarily to other home telemedicine vendors to be incorporated as a peripheral into their systems.

http://www.omnimedicalsupply.com

HIPAA Security Tool Available

Stony Hill Management, publishers of HCAR, has reported that its GetHIP software is already in use at more than 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.

Vendor Watch

Alacare switches software systems. Alabama's oldest and largest privately-owned home care and hospice provider has signed a deal to convert its point-of-care and billing systems to one of home care's newer market entrants, **Homecare Homebase**. Birmingham-based **Alacare** will help the Dallas-based software developer design a hospice application, Alacare president John Beard told HCAR. Homecare Homebase offers a web-enabled application and handheld, Pocket PC point-of-care system, which will replace Alacare's current laptop/notebook field computers.

Alacare's 20 offices are located throughout Alabama; the provider employs over 300 field staff and more than 200 office workers. Since 1970, Alacare has provided home care, hospice and palliative care, diabetes education, rehabilitation services, wound care, nutritional services and infusion therapy. Implementation is set to begin during the third quarter of 2005.

http://www.hchb.com
http://www.alacare.com

Cerner BeyondNow adds electronic signatures.
The home health care subsidiary of **Cerner Corporation** (Nasdaq: CERN) has inked an agreement with **SecureCARE Technologies, Inc.** (OTC-BB:SCUI) of Austin, Texas, to provide paperless document exchange for home care and hospice providers. Cerner BeyondNow will use SecureCARE's Internet-based document exchange and e-signature technology to provide its clients with the ability to capture electronic signatures from physicians, reducing paper use. According to Cerner home care director Lisa Cone, several

Continued on page 15

Vendor Watch
continued from page 14

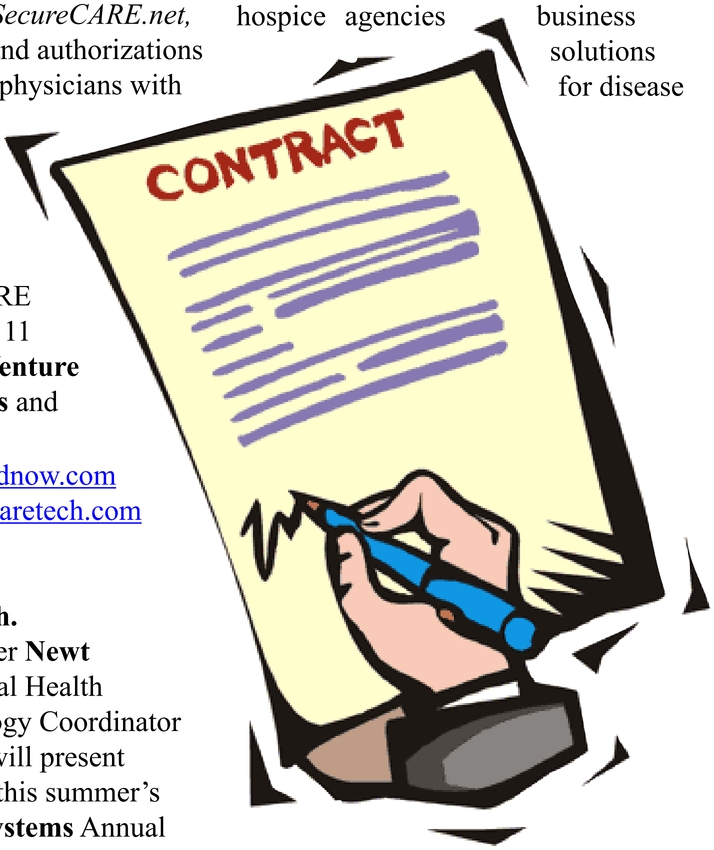
BeyondNow clients were using the SecureCARE system. "Now we are able to offer this functionality to all of our customers." SecureCARE Technologies offers a Microsoft ".NET" application, *SecureCARE.net,* for managing forms and authorizations online and providing physicians with a way to track and report patient oversight time spent. Longtime HCAR readers will remember SecureCARE under its pre-Chapter 11 names, **eClickMD**, **Venture Information Systems** and **Link-dot-com.**

http://www.beyondnow.com
http://www.securecaretech.com

Misys to host Brailer and Gingrich. Former House Speaker **Newt Gingrich** and National Health Information Technology Coordinator **David Brailer, MD** will present keynote addresses at this summer's **Misys Healthcare Systems** Annual Conference and Expo in Orlando, Florida. The annual event is open to hospital, physician and home care customers of the Raleigh, North Carolina software vendor. Brailer will speak on "The National Agenda for Health Information Technology Adoption" at a general session; Gingrich is scheduled to appear at an "invitation only" Executive Summit during the conference to discuss his vision for the future of U.S. healthcare. Misys indicated it expects more than 1,000 healthcare professionals at this year's meeting, set for July 21-24 at the Walt Disney World Dolphin Hotel.

http://www.mysishealthcare.com

Procura to offer Innovative pathways. Vancouver-based **Procura** and its U.S. subsidiary **Procura, LLC**, have completed an agreement with **Innovative Healthcare Solutions, Inc.** (IHS) of Naperville, Illinois to integrate 96 Care Pathways into its home care billing and clinical application. IHS is a subsidiary of **VNA First**, based in nearby Willowbrook, and offers homecare and hospice agencies business solutions for disease management, case management, OBQI/M and documentation. Their products and services include *VNA FIRST Home Care Steps® Protocols*, *Steps to Health*™ patient education, telecourses and consultation services.



Procura president Warren Brown said he believes this joint venture will provide *Procura* software users with the ability to increase the quality of care they provide, particularly organizations focusing on disease management services. Protocol integration work will begin immediately at several U.S. and Canadian customer sites. Procura's U.S. sales offices are located in Detroit, Baltimore, Chicago, Tampa, Los Angeles and New Orleans.

http://www.goprocura.com
http://www.innovativehcs.com

FDA approves new Buddy. Health Hero Network made two announcements last month. On April 11 the Mountain View, California company said it had received FDA clearance for its next-generation home telehealth appliance, *Health Buddy II*. A smaller version of the original *Health Buddy*, the new device offers multiple USB and serial ports to enable simultaneous peripheral connection, reducing the need for patients to handle cables. The appliance measures and transmits patient vital signs and returns customized reminders and instructions to patients through a high-resolution touch screen and large response buttons.

Health Hero Network also announced that a home telehealth study with CHF patients is being conducted by the Henry Ford Health System, using its *Health Buddy* system. Preliminary results, reported at last month's ATA annual meeting in Denver by Health Hero Network medical director Julie Cheitlin Cherry and Jonathan Ehrman, Ph.D. of the Henry Ford Health System, indicate 92% patient satisfaction, 88% patient compliance and early indications of decrease in ER visits and hospitalizations. Henry Ford will add a weight management study and is currently recruiting participants in the South Eastern Michigan area.

http://www.healthhero.com

Private duty software vendor hopes to raise its profile. Kaleida Systems, Inc. has over 300 clients, most of them **Comfort Keeper** franchises, but they have kept a low profile until recently. Based in Matthews, North Carolina, the vendor offers a web-enabled application for scheduling private duty nurses, aides and non-medical home care assistants. According to VP Barry Duppstadt, the Windows .NET system, *electronic Resource Scheduling Pro,* is commonly knows as *eRSP*.

www.kaleidasystems.com

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