Providing the highest quality information for 24 years

Hospital Home Health®

the monthly update for executives and health care professionals

AHC Media LLC

IN THIS ISSUE

Financial Disclosure:
Editor Sheryl Jackson, Managing Editor Mark Granger, Associate Publisher Coles McKagen, Board Member Elizabeth Hogue, and Consulting Editor Marcia Reissig report no consultant, stockholder, speaker's bureau, research, or other financial relationships with companies having ties to this field of study.

APRIL 2007
VOL. 24, NO. 4 • (pages 37-48)

As identity theft increases so does your responsibility

Laptops and handheld devices require extra attention

Imagine contacting over 350,000 patients to tell them that their private medical and financial data has been stolen. The staff and management of Providence Home Services, a division of Seattle, WA-based Providence Health Systems, doesn't have to imagine it.

After data backup tapes and disks were stolen from the car of an employee who took the information home as part of the agency's protocol for protecting data from fire or other disasters at the office, agency managers found themselves in the midst of investigations and policy reviews.

While there have been no reports of the stolen information being misused, this theft points out some of the weak spots in many agencies' data security plans, says **Robert W. Markette Jr.**, an attorney with Indianapolis, IN-based Gilliland, Markette & Milligan law firm. "I've seen two prevailing models of thefts," he says. In the first typical theft, the employee does something such as leave the laptop or handheld device in the car outside the home overnight. The second theft occurs when the employee carries the device home, then resigns without returning the device, he says.

In both cases, home health agencies may have policies governing the security of information but employees chose to ignore the policies, Markette points out. "It is not enough to develop policies, you have to educate employees and incorporate sanctions that emphasize the importance of the policies," he says. For example, if your policy does prohibit leaving the laptop in the car, make violation of the policy a reason for firing the employee, he suggests. Although you may not discover the policy violation until a laptop is stolen, other employees will think twice before leaving the laptop in their car," he says.

In the case of an employee who quits before returning the laptop or device, you might have two scenarios: the employee may simply not want to take the time to return the equipment or the employee may want to use the information to attract clients to his or her new employer, says Markette. In either case, it is important that the process for retrieving equipment is spelled out in your policies, he says. "The loss of a lap-

top represents a significant expense to replace the equipment alone, without the threat of exposing patient information," he points out.

Report thefts immediately

If theft by someone other than the employee is the reason for the equipment loss make sure that employees know to report the theft immediately so that steps can be taken to recover the item or warn patients whose information was on the laptop, says Markette.

A quick report from an employee prevented major problems for Nightingale Home Healthcare in Carmel, IN. A nurse who had been with the agency for a few weeks dropped her car at a repair shop then left in another car to make her visits, explains Melinda Jewell, director of human resources for the agency. As soon as she arrived at the first patient's home, she realized that she left her handheld device in her car at the repair shop. "She admitted that she was logged in on the device when she left the shop so we told her to immediately return to the repair shop and recover the device," she explains. Fortunately, the device was exactly where the nurse left it and did not appear to have been accessed.

"We contacted the patients whose charts were accessible by the device to let them know that although it did not appear that anyone accessed their information, they should be aware of the risk, then the nurse repeated our HIPAA training," says Jewell **(See story on p. 40 for more information about activities to take after a theft)**. Luckily, there have been no incidents involving Nightingale patient identities and the risk was minimized because the nurse's device only provided access to information about patients she was scheduled to see for the upcoming week. "Our nurses synchronize their device with our server every morning and every evening to upload the day's documentation and retrieve updated schedule and patient information," she explains. "We only provide access to information that is no more than 45 days old," she says.

The more information that is accessible on the laptop or handheld device, the greater your risk when a security breach occurs, points out Markette. An important aspect of HIPAA is the requirement that employees have access only to information that is necessary to perform their jobs, he says. "A HIPAA security officer needs to consider if it is necessary for a nurse to have access to everything about every patient," he adds. "When nurses were carrying paper files on their visits, they carried the five or six files they needed that day, not dozens or hundreds of files on patients they might not see for two months or might have seen two weeks before," he adds.

Use passwords

Password protection and encryption are excellent ways to protect data if the laptop or device is stolen, says Markette. While encryption software may not be practical for all agencies, he does point out that agencies that encrypt their data are exempt from the disclosure requirement in the states that require con-

Hospital Home Health® (ISSN# 0884-8998) is published monthly by AHC Media LLC, 3525 Piedmont Road N.E., Building Six, Suite 400, Atlanta, GA 30305. Telephone: (404) 262-7436. Periodicals postage paid at Atlanta, GA 30304. POSTMASTER: Send address changes to **Hospital Home Health**®, P. O. Box 740059, Atlanta, GA 30374.

Subscriber Information

Customer Service: (800) 688-2421 or fax (800) 284-3291. E-mail: customerservice@ahcmedia.com. World Wide Web: http://www.ahcmedia.com. Hours: 8:30-6 Monday-Thursday, 8:30-4:30 Friday.

Subscription rates: U.S.A., one year (12 issues), $499. Add $9.95 for shipping & handling. Outside U.S.A., add $30 per year, total prepaid in U.S. funds. Discounts are available for group subscriptions. For pricing information, call Tria Kreutzer at (404) 262-5482. Missing issues will be fulfilled by customer service free of charge when contacted within 1 month of the missing issue date. **Back issues**, when available, are $83 each. (GST registration number R128870672.)

AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity has been approved for 15 nursing contact hours using a 60-minute contact hour.

Provider approved by the California Board of Registered Nursing, Provider # 14749, for 15 Contact Hours.

This activity is intended for nurses, managers, directors, and management involved in hospital-owned home care agencies, including health care professionals involved with home care issues such as end-of-life care, pain management, multicultural issues, elder care, and similar issues. It is in effect for 24 months from the date of publication.

Opinions expressed are not necessarily those of this publication. Mention of products or services does not constitute endorsement. Clinical, legal, tax, and other comments are offered for general guidance only; professional counsel should be sought for specific situations.

Editor: **Sheryl Jackson**.
Senior Vice President/Group Publisher: **Brenda Mooney**, (404) 262-5403, (brenda.mooney@ahcmedia.com).
Associate Publisher: **Coles McKagen**, (404) 262-5420, (coles.mckagen@ahcmedia.com).
Managing Editor: **Mark Granger**, (404) 262-5461, (mark.granger@ahcmedia.com).
Production Editor: **Ami Sutaria**.

Editorial Questions
For questions or comments, call **Mark Granger** at (404) 262-5461.

tact with the patients after data is stolen.

When evaluating different encryption software, be sure to look at how the software affects the nurse's ability to do his or her job as well as evaluating cost, suggests Markette. Some software is easier to use and less intrusive than other software, he says.

Don't forget that even if a file is deleted from a laptop, the information is still retrievable until it is written over, warns Markette. "Because wiping a hard drive with a wipe utility is time consuming, it is worthwhile to evaluate encryption software that will encrypt information before it is deleted," he adds.

If you decide that encryption is not affordable or workable for your agency, make sure that information can only be accessed with a login name and unique password for each user, says Markette. "Your policy should also state that when the employee is not actively using the laptop or device to document a visit, to review information on upcoming visits, or to download or upload data, the user should log out of the system," he says. This eliminates the risk of quick and easy access to information, he adds.

The best way to protect data is to make sure your policies are clear about employees' responsibilities for protection of the laptops, handheld devices and the information they contain, says Markette. Even though no one would leave their own valuables, such as a laptop, in a car outside the house overnight, employees don't always treat their employer's property as their own, he admits. "Make sure that employees understand how they are supposed to care for the equipment, what the equipment is worth financially, and how important it is to protect the information on the equipment," he says. Holding an employee financially responsible for a lost laptop can be tricky, so Markette believes that firing anyone who loses the equipment emphasizes the importance of protecting the laptop.

"Our policy is that the nurse must have the handheld device in his or her possession at all times," says Jewell. In addition to always having the device with them, employees are warned to be aware of who else might have access to the device, she adds. "An employee who has the device in her home, might have a grandchild who thinks it's a game to play," she explains. Password protection will keep someone from accessing the information but a child that picks up the device and wanders through the house with it might place it where the employee can't find it when needed, she adds.

Employees also need to be aware of who can see the information when they are using the laptop or device, points out Markette. HIPAA requires that workstations be designed so that other people can't see information displayed on a screen, so laptop users who stop at a Starbucks to finish their documentation, or use a place other than home to upload information, need to look around and be sure that no one else can see their screen, he adds. Even when working in their homes, employees need to make sure that visiting neighbors, friends, or family members cannot access or see what is on the computer, he says.

The other big issue that home health agencies face is protection of backup data. In the Providence Home Services' incident, the health system's corporate policy was that employees did not take backup data home, but the home services division did not adhere to that policy, says Markette. "It is important to store backup data away from the main server in case of a disaster such as a fire in the agency office, but having an employee carry it home is not a way to protect it," he says. Markette knows of organizations that store their backup data in a safe in the office but the safe is designed to protect contents from extreme heat or water so the data is protected.

The other consideration for backup data is the need to delete old files, Markette adds. "When we had to pay for space to store paper files, we were diligent about throwing out files that no longer had to be kept," he says. "Now that electronic storage is cheap, agencies hold onto old files longer than necessary," he explains. Not only are these files not necessary, but also they increase an agency's exposure if the data is stolen because there are thousands of patients who information did not need to be in the database, he adds.

Once you make sure your policies address the special precautions that laptop users must take, be sure you educate your staff, says Jewell. "Our education includes examples of how and where information might be accessed so that employees recognize situations, such as the neighbor wandering in while the employee was completing her documentation, so that they realize how easy it is for others to access patient information if we don't logout."

"Unfortunately, the risk of losing data through stolen laptops and handheld devices will only increase," says Markette. He adds, "It is best if agencies review their policies now, and make sure that they are prepared for the future." ■

SOURCES

For more information about laptop security, contact:

- **Robert W. Markette Jr**., Attorney at Law, Gilliland Markette & Milligan, 3905 Vincennes Road, Suite 204, Indianapolis, IN 46268. Telephone: (800) 894-1243 or (317) 704-2410. Fax: (317) 704-2410. E-mail: rwm@gilliland.com.
- **Melinda Jewell**, Director of Human Resources, Nightingale Home Healthcare, 12766 Hamilton Crossing Boulevard, Carmel, IN 46032. Telephone: (866) 334-7776 or (317) 334-7777. Fax: (317) 569-1403. E-mail: mjewell@homecareforyou.com.

The laptop is gone What do you do now?

Investigate, communicate and educate to cut risk

It is very unlikely that many home health agencies will be faced with the theft of data on more than 350,000 patients at one time, but Seattle, WA-based Providence Home Services' experience in 2006 and the actions taken by the agency after the theft of data backup tapes from an employee's car may be a clue as to the standard for follow up in the future, says **Robert W. Markette Jr.**, an attorney with Indianapolis, IN-based Gilliland, Markette & Milligan law firm.

After investigating the theft, evaluating employee actions, and reviewing home care's policies, Providence notified patients of the data security breach. "Providence set up a toll free hotline number for families and offered free credit monitoring service to patients whose information was included in the data," says Markette. Most agencies will not have to handle a breach that involves this many patients but it is important to study the actions Providence took following the theft, he says.

The HIPAA security officer should be in charge of the theft investigation within the agency, says Markette. "Find out how it happened, what policies were followed or not followed, and identify what changes can be made to improve security," he says.

Contacting patients involved in a breach after your investigation into the cause of the breach is a good move, recommends Markette. "HIPAA requires mitigation but does not specify that patients must be contacted. However, 34 states require disclosure," he says.

"Even if you live in a state that does not require disclosure, it is good public relations to notify patients whose information might have been accessed, explain what happened, and provide directions on how to place a fraud alert on their credit reports or other steps to prevent identity theft," suggests Markette. Be sure to describe the level of threat as well, he says. "If your information is password protected or encrypted, you can explain that to patients and say that, while they should take steps to protect themselves, the risk is minimal," he adds.

Have an attorney review the letter, says Markette. "There is always the risk of lawsuits following a breach in data security so an attorney can reduce that risk by making sure the letter does not create any additional exposure." ■

Wanted: Focused, motivated person to sell

Hire sales person based on passion for selling

Hiring the right person for the job is the key to success for any business but in home health many managers are not sure how to identify the right person for a sales and marketing position.

Home health managers usually come from the clinical side of the agency and may have no sales experience in their background so it is harder for them to evaluate a candidate for a sales position, says **Lucy Andrews**, RN, MN, chief executive officer of At Your Service Home Care in Santa Rosa, CA. "We all love to take one person who is doing well in their job and move them to another position that is important to the agency because we trust them to do a good job," she says. "Unfortunately, the nurse who is passionate about the use of telemedicine in home care may not be the right person to sell the agency's telemedicine service to referral sources," she adds.

"There are many clinical staff members who are enthusiastic about the service they provide and they want to tell others about it, but you have to look for someone who can close the sale," says Andrews. "You need someone who

can talk about the service and then ask the referral source to give your agency a try," she explains. "This is the area with which many clinicians struggle," she says.

It is also important to have a person who is dedicated to sales and marketing, points out Andrews. "Sales and marketing is an ongoing effort, not something that can be done between seeing patients," she says. For this reason, you need to screen your candidates carefully to make sure that nurses who apply for the position understand that they won't be working with patients, she adds.

It is not necessary to hire sales and marketing staff members who have only clinical or only sales experience, points out Andrews. "You are looking for a person who is excited about selling the agency's services and getting results," she says.

Home health managers may think they need someone with a clinical background because the "product" the person is selling is clinical, admits Andrews. "You can teach enough about your business to a non-clinical person but you can't teach a person who doesn't love sales how to sell," she explains.

"A good sales and marketing person can talk about the benefits of using your agency's services from the perspective of the referral source," says Andrews. Talking in terms of reduced hospitalization, improved outcomes, and reduction of the cost of providing care, and how that helps the referral source's business is important, she points out. "The sales person also needs to be able to communicate how the agency can make the referral source's job easier," she adds.

Because sales and marketing people are motivated by results and by money, you need to be clear about your expectations upfront, recommends Andrews. Develop your sales and marketing program with specific goals related to new admissions, development of new referral sources, or increase in specific programs, she suggests. "Tie these expectations to monetary rewards because sales people are motivated by money," she adds.

The type of pay structure for your sales and marketing staff depends upon your agency, says Andrews. "I've seen commission-only sales staff and salaried staff," she says. To improve motivation, salaried staff members usually have a bonus structure that is tied to goals met for new referrals or other aspects of the business, she adds.

Once you have hired the right person, be sure to provide the tools that he or she needs to do the job, warns Andrews. "If you do hire someone with no home health experience, arrange for her to go on several home visits that represent your core business as well as any special programs you offer," she says.

Even if you hire people with clinical experience, they won't know everything about every type of care, so be sure they have a list of resources within the agency for questions. Also, make sure they have access to data that helps identify potential sources of new admissions, says Andrews. "We have preconceived ideas about who our best referral sources are, but when a sales and marketing person evaluates the data carefully, other sources may prove more valuable," she says.

Have your marketing person look for the referral source, the type of patient typically referred, and any referral trends, Andrews suggests. The "A" list of contacts should include sources who frequently refer patients and represent a great deal of volume, who refer patients who do have insurance or other means to pay, who have the potential to refer more patients, or who see patients that are appropriate for the agency's specialty services. Your "B" list may include sources that have potential but not as great as the sources on the "A" list. "Market to both the A and B lists, with the emphasis on the A list at the beginning," says Andrews.

Make sure your sales and marketing person knows when to drop a source from the marketing list, recommends Andrews. "If you haven't received a referral from a source that you are visiting two times a month over six months, give up," she says. She adds, "You don't want your sales staff wasting their time, not when there are other sources for new referrals." ■

SOURCE

For more information about managing a sales staff, contact:

• **Lucy Andrews**, RN, MN, Chief Executive Officer, At Your Service Home Care, 1221 Farmers Lane, Suite C, Santa Rosa, CA 95405. Telephone: (707) 573-1003. Fax: (707) 573-3675. E-mail: heartofhomecare@sbcglobal.net.

Show the value of telemedicine services

Offer free 'trials' to establish credibility

Three years ago, Visiting Nurse Services of the Northwest in Mountlake Terrace, WA, began offering telemedicine services to a wide range of patients. The new technology not only improved patient care but also allowed staff members to efficiently manage visits while still offering continuous monitoring of vital signs for patients with ongoing cardiac, respiratory, or diabetic conditions.

The benefit of using telemedicine for Medicare patients is that you can better manage the number of visits needed to ensure good outcomes; therefore you can control costs, points out **Patricia Mulhern**, RN, MN, vice president of patient services for the agency. The agency didn't limit the use of telemedicine to Medicare patients, however. "We saw an opportunity to use telemedicine as a marketing tool to attract new referral sources," she says.

"Our No. 1 market is our referral sources, which are physicians and payers," explains Mulhern. "We must have physician orders for telemedicine; so we do spend time explaining telemedicine to physicians and their staff," she says. Because a physician's support of the technology is important not only to getting the referral but also to the patient being receptive, Mulhern's staff carry a telemonitor to the physician's office so that the physician and staff members can see how easy it is for the patient to operate. "The hands-on demonstrations are very important," she adds.

At Presbyterian Healthcare Services in Albuquerque, staff members' constant communications with physicians and written reports of the results of the patient's monitoring increase physician support of the program. "We are part of an integrated health system; so we don't have to do a lot of marketing to physicians but it is important that they are supportive of their patients who are on telemedicine," explains **Cheryl Reese**, BSN, MBA, clinical education specialist at the agency.

"We have also found that the most important part of marketing a telemedicine program is to make sure your staff members understand the program so that they can speak positively about it when asked," says Reese. Telemedicine is discussed at staff meetings and reports about positive outcomes for telemedicine patients are shared.

"We do market telemedicine to the community, at all of our events for the senior members of our health plan," she says. Flyers, educational displays, and demonstrations explain the program and how it works, Reese says.

Another market that Mulhern's agency is pursuing is managed care and private insurance. "It is easy to gather data on Medicare patients who are on telemedicine, but the data doesn't always apply to patients of other payers," says Mulhern. "We did not want to wait until we had enough data on non-Medicare patients to approach payers about reimbursement for telemedicine; so we go to a payer and offer to add telemedicine to the care of one patient for no charge," she says.

Once the patient is discharged from care, the agency and payer look at the savings and improved outcome for the patient. "We point out the savings and suggest that they share the savings with us by reimbursing us for the telemedicine portion of the care," Mulhern says. Medicare does not reimburse for telemedicine but because agencies can reduce costs with reduced visits for the same outcome, the agency does see a savings, she points out. "Because private payers tend to pay per visit, they are not set up to reimburse telemedicine as a separate service," she says.

Telemedicine reimbursement is not part of any payer's standard contract so it does take time to work out details, says Mulhern. To avoid giving away telemedicine for a long period of time, be sure to set the parameters of the test case at the beginning, she suggests. "We usually say the test will run for one episode of care, or 60 days," Mulhern explains. "If you let it run indefinitely, there is no reason for the payer to make a decision, and when you do finally stop the service, your staff may feel as if they are abandoning the patient." She adds, "By defining the length of time for the test case, all parties involved understand when it will end." ■

Get more by adopting technological advances

Telehealth offers new ways to improve bottom line

Hospice agencies still provide personalized care for patients in their homes, just as they always have, but technological advances have improved the way that agencies manage and doc-

uments that care. Point-of-care computers, cell phones, automated billing systems, and electronic medical records are all technology-related advances that have improved efficiency and productivity for home health agencies.

While hospice managers are upgrading their technological capability to offer telemedicine services and make it easier to collect and manage the increasing amount of information needed for each patient, there is less attention paid to the use of electronic marketing activities and Internet-based staff education.

Even with the number of hospice agencies that are increasing their use of technology to support staff activities, the home health industry is behind the curve compared to the way other industries and other areas of health care use technology to promote home health services and reach referral sources, says **Michael Ferris**, partner, Home Care Marketing Resource Group, a Chapel Hill, NC-based consulting firm. "At this time, the typical home health patient is not computer-savvy and does not use the Internet to find an agency; but as we see more adult children who are computer-savvy take a greater role in finding care for their parents, home health agencies are finding that electronic promotion is one way to get a lot of bang for their buck."

The most obvious first step in marketing your agency electronically is development of a web site. If you are a hospital-owned agency and your web page is part of the hospital's overall web site, check it out carefully, suggests Ferris. "The most important part of marketing on the Internet is to make your web page easy to find," he explains. Unfortunately, for most home care agencies that are included on their hospital's web site, it is not easy to find the home care page, he says.

One way to see how accessible your information is to the public is to pretend you are not familiar with the web site and look for your hospice page, suggests Ferris. You also can ask a neighbor or friend who is not familiar with the web site to find information on the hospice agency. "If you discover that your page cannot be easily found, talk to the hospital's webmaster to see what changes can be made," he suggests.

"You can also find out if the agency can set up its own web site to make information more accessible," he adds.

Market web site

Once you set up a web site, or make your page easier to find on the hospital's site, be sure to include the web address in all marketing materials, says Ferris. "You want to use your web site to gather information as well as give information," he says. "A good web page starts a conversation with the consumer." Offer consumers a chance to request information about your agency and offer something free that you can mail or e-mail to the consumer, he says. That offering could be a list of tips for selecting the best home health agency, he suggests.

"Collect names, addresses, and e-mails, but include a disclaimer that this information will not be sold or used by any other organization," Ferris recommends. This information can be used to build a list of names to which you can send newsletters, tips for hospice patients, or any other useful information that will keep the person connected to your agency, he explains.

To make your web site most effective, keep it simple, emphasizes Ferris. "People usually try to do too much," he says. "Be sure you focus on the message you want to communicate and don't cram too much extra information onto the site." To establish your credibility, include mentions of any awards, statistics that demonstrate good outcomes and high-quality care, and comments from patient satisfaction surveys, Ferris suggests.

If you offer a specialized program that focuses on care for certain conditions, or if you offer special services such as telemedicine, be sure to describe them in your web site, he says. Because all hospice agencies offer the same basic care, don't describe those services in detail, but spend time on the things that differentiate your agency, Ferris adds.

Not only does the Visiting Nurse Services of the Northwest in Mountlake Terrace, WA, offer telemedicine as part of their services, but it also is an important part of their marketing effort, says **Patricia Mulhern**, RN, MN, vice president of patient services for the agency. "We are the only agency in our area that uses a telemedicine system that measures a wide range of vital signs on a daily basis; so this is a service that differentiates us from others," she says.

While telemedicine is included as part of the description of services on their web site, Mulhern points out that most of her marketing of the telemedicine service is directed at referral sources such as physicians and payers. **(For tips on marketing telemedicine, see story on p. 42.)**

Cut costs with e-learning

Another area that more home health agencies are beginning to use is web-based staff education,

says **Debbie Scholl**, RNC, BSN, MSN, managing director of CHEX, the e-learning division of The Corridor Group, an Overland Park, KS-based consulting firm. "Home health managers are constantly challenged to find ways to cut costs without compromising quality and that is hard when costs such as gasoline and salaries are going up at the same time staff sizes are decreasing," she points out. There is a limit to the ways you can cut costs in many areas, Scholl adds.

Because staff education is an integral part of any agencies' overhead costs, web-based learning for some required courses offers agency managers a way to meet training requirements without using staff educators to teach mandatory, basic courses, explains Scholl. "E-learning programs free up your staff educator to focus on specific needs of the agency and to spend more time with staff members who may need one-on-one training," she says.

Web-based programs also give employees the flexibility to take the required courses without having to come into the office at a specific time, which might disrupt their visit schedules, points out Scholl. The flexibility of the time and place at which employees can take the test is a great benefit to employees and is one way management can demonstrate that the agency is sensitive to employee needs, she says.

"Not only is this type of program great for recruitment and retention of employees now, but it positions the agency to meet the needs of future employees," Scholl says. "Younger employees and staff members we hire in the future will demand the flexibility that this technology offers." ■

ID theft in health care emerging as major risk

Health care records are a "treasure trove of information" for identity thieves because they typically contain more detailed personal information on people than could be found in any other business, according to experts who help health care providers avoid identity theft.

Risk managers should make prevention of identity theft a top priority, says **Thomas McShane**, JD, regional managing director of the New York City office of the investigative firm SafirRosetti, which specializes in the area of financial investigative services and integrity monitoring. His unit implements legal, auditing, investigative, research, and technical support, and they recently used many of these services to uncover a major Medicaid fraud case at Staten Island University Hospital that led to several convictions. As a result of that case, SafirRosetti was appointed to a 12-year monitorship by the hospital's insurance company.

McShane works on identity theft issues with **James Murray**, a forensic accountant and managing director with SafirRosetti in New York City. Murray says instances of identity theft are increasing in all types of businesses, but health care organizations are proving to be a particularly fertile hunting ground for criminals in search of personal financial data. There is no way to guarantee that patients' confidential information will not be divulged, he says, but there are steps you can take to minimize that risk.

Murray points out that health care organizations are doubly burdened when it comes to protecting confidential information because they have data on employees and patients. Staten Island University Hospital has 3,500 employees. "There have been instances where employees of that hospital have had their identities stolen," Murray says. It's important to include employee data in discussions about identity theft, he says. "You probably have as much confidential information on your employees as you do on your patients, if not more."

McShane notes that if a criminal obtains personal information about a hospital employee, that person's identity can be stolen, but the information might also be used to gain access to secure areas of the hospital computer system, where much more information can be stolen.

Screening employees for criminal history is critical, the experts say. Murray recalls working with a company that hired a director of sales and promoted him quickly to president of a subsidiary company, then called in SafirRosetti to investigate financial improprieties. They found out that the man had written his application for the sales job from prison. Once he had access to information on the company's employees, he stole their identities and leased five cars in their names.

"We recommend to all our clients that they do at least a basic background check on all new hires, and the more senior the person or the

Steps for preventing identity theft in health care

Thomas McShane, JD, regional managing director of the New York office of the investigative firm SafirRosetti, and **James Murray**, a forensic accountant and managing director with the firm, recommend these risk reduction strategies for identity theft:

- **Build on the strategies you already have in place to comply with the Health Insurance Portability and Accountability Act (HIPAA).** While HIPAA focuses more the accidental release of information, many of the same policies and procedures in place for HIPAA compliance will give you a good starting point to enact additional steps to prevent the theft of data.
- **Work closely with your information technology (IT) department to develop the appropriate technical defenses, such as firewalls, encryption, and password policies.** While the IT techies may have the know-how about defensive procedures, the risk manager must impress upon them the importance of preventing identity theft and the potential liability for a breach. Make sure the IT department knows it will be a very bad day if a multimillion-dollar liability following an identity theft scandal is traced back to poor computer security. **(See p. 44 for more information on the potential liability from identity theft.)**
- **Educate all employees, including and especially the front line clerks and office workers, about simple steps to reduce identity theft.** Examples include never walking away from a computer and leaving sensitive material on the screen, and never writing down a password where it can be found easily.
- **Perform a risk assessment to determine what information is available on the system and where.** How many different computer systems contain sensitive data? Can it be centralized into one system where you can pour all your security resources? A key goal is to ensure that computers — whether they are desktop or laptop — do not contain any unnecessary data that could be useful to an identity thief.
- **Assess compliance with your own policies and procedures.** It is common for health care organizations to have safeguards that look great on paper but aren't followed by employees. Employees must be reminded and re-educated about the importance of these security steps on a regular basis.

When you test compliance, you're likely to find out 30% of the employees aren't following your procedures, McShane says. "They're doing it the old way because they don't want to change, or they think the new procedure is too much trouble, or they're just careless," he says. "Don't depend too much on the fact that you've put out this policy and you're assuming everyone follows it." ■

more sensitive the position, the more you should a very thorough investigation," McShane says. "Anyone who will have access to sensitive information should be screened, and that can be a lot of people in health care. The entire billing department, for starters."

In addition to a criminal background check, it may be appropriate to do a credit check on people in sensitive positions such as the billing department.

Murray says a bankruptcy or other financial hardship could put the person at higher risk of criminal activity, including identity theft. Remember that it usually is necessary to obtain permission from the applicant before doing a credit check. **(See article for more advice on how to reduce the risk of identity theft.)**

Stolen laptops

One of the biggest risks when trying to protect patient information involves the use of laptop computers.

Murray and McShane says risk managers must work closely with their information technology staff to ensure that laptops contain only the data necessary for the user and that the information is protected by passwords or encryption. Employees also must understand that the laptops are at a high risk for theft and should be protected at all times.

It is all too easy for someone to walk off with a laptop that contains sensitive information. For instance, Murray points to a recent incident at Vassar Brothers Medical Center in Poughkeepsie, NY, which reported that a laptop computer stolen from the facility contained a copy of the hospital's entire master patient database. That database made it a gold mine for any identity thief.

In announcing the theft, the hospital did not say exactly how many names were contained in the database but noted that 257,800 of those whose names were in the database were at risk of becoming identity theft victims. They were at risk because the database contained other personally identifiable information on those patients, such as Social Security numbers and addresses.

The hospital reported that the computer theft occurred during a hospital disaster planning exercise. The hospital copied its master database to several laptops for a disaster drill, simulating the need to operate during a disaster without access to the facility's main computer system. The master database was placed on several laptop computers that were distributed throughout the facility.

The stolen laptop had been strapped to a cart in the hospital's emergency department and used to collect patient data at the bedside during admission. The hospital reports that since the theft, it has erased copies of the database that were on other laptop computers. The hospital notified those whose information was on the laptop and advised them to place a fraud alert on their credit reports.

Laptops are like treasure chests for identity thieves, especially if they know that kind of database is on them, Murray says. "They can just walk out with it and work on cracking passwords and so forth at their leisure," he says. "You should exercise extreme caution, using your best security procedures, with any laptop that has sensitive information." ■

Heart failure patients present challenges

Comorbidities, patient attitudes make care difficult

Patients with heart failure may be among the most challenging for case managers who are coordinating their care. Patients with heart failure must take multiple medications, eat a low-salt diet to keep their condition under control, and monitor their condition constantly. And even if they do everything right, they are likely to find themselves back in the hospital or emergency department several times a year.

"Heart failure has substantial quality-of-life implications for patients. It has a higher mortality rate than most cancers, and it's difficult to get patients to manage their condition because they think it's an episodic event and not a chronic disease," says **Jill Howie-Esquivel**, PhD, RN, FNP, associate clinical professor at the University of California-San Francisco School of Nursing.

It's also an expensive disease. The American Heart Association estimates that heart failure will cost $26.9 billion in direct and indirect costs in 2006 for the 5 million people with the condition. The organization estimates that about 500,000 patients are diagnosed with the condition every year. Heart failure deaths have doubled since 1979 and average 250,000 a year.

"Congestive heart failure is one of the largest admitting diagnoses to acute care hospitals. It's a diagnosis with a high mortality rate, and patients with heart failure consume a lot of health care resources, says **Pam Hagley**, RN, BSN, MSHA, ACN, director of clinical resources at New Hanover Regional Medical Center in Wilmington, NC.

A telephonic case management program for heart failure patients who have been discharged from the hospital has cut readmissions and reduced length of stay, Hagley says.

Many heart failure patients also suffer from depression, a condition that makes it difficult for them to manage their condition, points out **Rick Precord**, MSW, director of clinical care management at Health Alliance Plan (HAP) based in Detroit.

HAP's case managers screen all their heart failure patients for depression and refer those who screen positive to the health plan's behavioral health specialists.

When Howie-Esquivel conducted a study of heart failure patients to determine what factors can be used to predict which patients would be readmitted to the hospital, she found that an astonishing 50% of the 72 patients she followed were readmitted within 90 days.

The average age of the patients was 61, and 50% were anemic upon admission and scored 3.25 on the New York Heart Association Classification for Congestive Heart Failure, a four-point scale for classifying heart failure patients.

She looked at clinical factors and activities of daily living, such as how far the patient could walk in six minutes. Her studies showed that women and people who are not white are more likely to be hospitalized.

"I was surprised to find that gender and ethnicity were stronger predictors of outcomes than hard clinical data," she says.

One factor may be that the women patients were more frail than the men. They couldn't walk as far, an indicator that they might have problems taking

care of themselves at home, Howie-Esquivel says.

Another factor could be that many heart failure patients do not understand their disease. They don't understand that they have a chronic illness that won't ever go away.

"Patients don't understand that when they leave the hospital, they still have heart failure. They think it's like pneumonia. You have it and you're treated and then you're cured," says **Renee Slater**, RN, a case manager with New Hanover Medical Center's telephonic heart failure case management program.

Case managers should work to help heart failure patients understand that they must think about their disease every day, monitoring their sodium intake at every meal, weighing themselves every day, and calling their doctor if they gain weight, Howie-Esquivel says.

"Heart failure patients are notorious for having high rates of readmission around the holidays and in the winter months when they may be eating a lot of canned soups, gravies, and broths. Case managers should caution them to be particularly careful about their diets during the holidays," she says.

Case managers should urge patients to write their weight down and to understand that gaining three pounds in a day or five pounds in a week is a signal that they are going to have problems, she adds.

Another indication that their condition may be exacerbating is when their belt or waistband is tighter than the day before or their ankles begin to swell.

"Case managers should remind patients that if it's harder to sleep at night or they're more short of breath, this could be an indication that they are getting in trouble and may need their diuretic dosage adjusted," she says.

Get a sense of the patient's condition by asking them specific questions about activities of daily living, Howie-Esquivel suggests.

For instance, ask if they can put their groceries in the cabinet, because raising the arms upward takes more energy that doing something that involves the lower body.

If you feel that a heart failure patient could benefit from exercise, talk to the physician about ordering an exercise program. "We know that exercise benefits patients with heart failure, but it's extraordinarily rare to find a heart failure patient involved in an exercise program. Being involved in an exercise program can't harm the patients, and it can help keep them out of the hospital," she says.

CNE *questions*

13. According to **Thomas McShane**, JD, regional managing director of the investigative firm, SafirRosetti, and **James Murray**, a forensic accountant with the firm, one of the biggest risks when trying to protect patient information involves the use of laptop computers.

A. True

B. False

14. What is the best way to protect data contained on a laptop or handheld device, according to **Robert W. Markette Jr.,** an attorney with Indianapolis, IN-based Gilliland, Markette & Milligan law firm?

A. Password required for login

B. Encryption

C. Clear policies on employee responsibilities for equipment and data

D. All of the above

15. Who should conduct the investigation within an agency when data is stolen, according to **Robert W. Markette Jr.,** an attorney with Indianapolis, IN-based Gilliland, Markette & Milligan law firm?

A. Agency manager

B. Health system risk manager

C.HIPAA security officer

D. Supervisor of employee who lost data

16. What aspect of home health sales provides the biggest challenge for many clinicians, according to **Lucy Andrews**, RN, MN, chief executive officer of At Your Service Home Care in Santa Rosa, CA?

A. Identifying potential referral sources

B. Closing the sale

C. Describing the services

D. Meeting sales goals

Answer Key: 13. A; 14. D; 15. C; 16. B.

(For more information, contact Jill Howie-Esquivel, PhD, RN, FNP, e-mail: jill.howie-esquivel@nursing.ucsf.edu; other resources include: The Heart Failure Society of America, www.hfsa.org. The American Heart Association, www.americanheart.org.) ■

NEWS BRIEF

Patient safety FAQs released

A total of 147 new or revised frequently asked questions (FAQs) related to the 2007 National Patient Safety Goals are posted on the Joint Commission website. The FAQs represent the most common questions submitted to the Joint Commission by accredited organizations.

Many of the FAQs raise the bar on what is required to demonstrate compliance with National Patient Safety Goals, according to experts. FAQs are considered requirements and surveyors refer to them during site visits. To review the FAQs related to the 2007 National Patient Safety Goals, go to www.jointcommission.org, select patient safety on the top navigational bar, and then choose National Patient Safety Goals. The FAQs are listed in the middle of the page. ■

CNE objectives

After reading each issue of *Hospital Home Health*, the reader will be able to do the following:

1. Identify particular clinical, ethical, legal, or social issues pertinent to home health care.
2. Describe how those issues affect nurses, patients, and the home care industry in general.
3. Describe practical solutions to the problems that the profession encounters in home care and integrate them into daily practices. ■

CNE instructions

Nurses participate in this continuing education program by reading the issue, using the provided references for further research, and studying the questions at the end of the issue. Participants should select what they believe to be the correct answers, then refer to the list of correct answers to test their knowledge. To clarify confusion surrounding any questions answered incorrectly, please consult the source material. After completing this semester's activity with the **April** issue, you must complete the evaluation form provided in that issue and return it in the reply envelope provided to receive a credit letter. ■

AHC Media LLC

Dear *Hospital Home Health* subscriber:

This issue of your newsletter marks the start of a new continuing nursing education (CNE) semester and provides us with an opportunity to review the procedures.

Hospital Home Health, sponsored by AHC Media LLC, provides you with evidence-based information and best practices that help you make informed decisions concerning treatment options and physician office practices. Our intent is the same as yours — the best possible patient care.

The objectives of *Hospital Home Health* are to:

- identify particular clinical, ethical, legal or social issues pertinent to home health;
- describe how these issues affect nurses, patients, and the home care industry in general; and
- describe practical solutions to the problems that the profession encounters in home care and integrate them into daily practices.

Each issue of your newsletter contains questions relating to the information provided in that issue. After reading the issue, answer the questions at the end of the issue to the best of your ability. You can then compare your answers against the correct answers provided in an answer key in the newsletter. If any of your answers were incorrect, please refer back to the source material to clarify any misunderstanding.

At the end of each semester, you will receive an evaluation form to complete and return in an envelope we will provide. Please make sure you sign the attestation verifying that you have completed the activity as designed. Once we have received your completed evaluation form, we will mail you a letter of credit. This activity is valid 24 months from the date of publication. The target audience for this activity is nurses, directors, and management involved in hospital-owned home care agencies, including health care professionals involved with home care issues such as end-of-life-care, pain management, multicultural issues, elder care, and similar issues.

Those participants who earn nursing contact hours through this activity will note that the number of contact hours is decreasing to 15 annually. This change is due to the mandatory implementation of a 60-minute contact hour as dictated by the American Nurses Credentialing Center. Previously, a 50-minute contact hour was used. AHC Media LLC is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

If you have any questions about the process, please call us at (800) 688-2421, or outside the U.S. at (404) 262-5476. You can also fax us at (800) 284-3291, or outside the U.S. at (404) 262-5560. You also can email us at: customerservice @ahcmedia.com.

On behalf of AHC Media, we thank you for your trust and look forward to a continuing education partnership.

Sincerely,

Brenda L. Mooney

Brenda Mooney
Senior Vice-President/Group Publisher
AHC Media LLC