CCH Health Care Compliance LETTER

Volume 7, Issue 21 health.cch.com October 18, 2004

Waiver of cost-sharing amounts for municipal ambulance services

by Gené Stephens Connolly, JD, Contributing Editor

The OIG concluded that a proposed arrangement to waive federal health care program cost-sharing amounts for emergency medical services rendered to tax-paying residents of a municipality would not generate a prohibited remuneration under the Anti-Kickback Statute.

The *Medicare Benefit's Policy Manual* provides a special rule that allows a "state or local government facility" provider of services to waive or reduce its charges for patients who are unable to pay for medical services. The municipality's operation of an ambulance service through its fire department constituted a "facility" within the meaning of the *Manual* provisions as a Medicare Part B supplier.

While the "insurance only" billing arrangement would typically implicate the Anti-Kickback Statute to the extent that it would constitute a limited waiver of federal health care program cost-sharing amounts, the Centers for Medicare and Medicaid Services (CMS) allow cost-sharing and waiver amounts for patient medical services when the supplier is a governmental unit. The OIG commented that their concerns over potentially abusive waivers of Medicare cost-sharing amounts have been longstanding. In previously issued Special Fraud Alerts, the OIG reiterated that providers who routinely waive Medicare cost-sharing amounts for reasons unrelated to "individualized, good-faith assessments of financial hardship" will be held liable under the Anti-Kickback provisions (see Special Fraud Alert, 59 FR 65374 (Dec. 19, 1994)). The OIG believed that since Medicare would not require the municipality in this case to collect cost-sharing amounts from residents who utilized the city's ambulance services, the waiver arrangement and proposed legislation would not subject the municipality to civil money sanctions under the Statute. The OIG emphasized, however, that the special waiver rule would not apply to situations in which a municipality contracts with an outside ambulance provider unless the municipality pays the cost-sharing amounts owed or otherwise makes provisions for the payment of such cost-sharing amounts.

The OIG concluded that it would not impose sanctions for cost-sharing waivers by a municipality that categorically provided ambulance services for *bona fide* residents of the city. Thus, the municipality's proposed ordinance that would authorize the city to bill residents only to the extent of their insurance coverage and that would treat the revenue received from local taxes as payment of any otherwise applicable cost-sharing amounts due from residents would not constitute an illegal remuneration. ■

OIG Advisory Opinion No. 04-12, September 21, 2004

Letters to the Editor

The CCH Health Care Compliance team welcomes comments or questions regarding articles published in the CCH Health Care Compliance Letter. Send comments to Sharon Sofinski, Coordinating Editor, at sofinsks@cch.com. For more information about the CCH Health Care Compliance Portfolio visit our online store at http://health.cch.com.

Establishing effective HIPAA auditing programs

by Catherine Hubbard, MA, Contributing Editor

Health care organizations need to establish effective HIPAA auditing and monitoring systems before the Security Rule becomes effective next April. "You need to get busy," Chris Apgar, CISSP, principal with Apgar & Associates said during a recent audio conference. "If you haven't started developing an audit program, if you haven't conducted a risk assessment, it's a good idea to jump on that right now and get moving so that you have at least something rudimentary in place come the compliance deadline," he recommended.

By April 21, 2005, security audits and monitoring are mandatory, noted Apgar, a former HIPAA compliance officer for Providence Health Plans, Oregon. "It is actually mandated that you audit your systems for electronic protected health information," he said during a September 21 audio conference, entitled, "HIPAA Security Auditing and Monitoring: Creating, Building and Testing a Strategy to Ensure Your Organization's Compliance," sponsored by the Healthcare Intelligence Network, Manasquan, New Jersey, (732) 528-4468.

In addition, Apgar said, the Security Rule requires that all covered entities implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking. "Now, you're required to demonstrate that you're actually doing this."

Organizations will have to show they are auditing regularly, Apgar noted. "This isn't something that is a one-time-only shot," he said. "It's something that needs to be documented and it needs to be viable and active."

Risk assessment. Assessing risk for security breaches is one of the foundations of any solid audit program, Apgar said, noting that if a compliance officer doesn't know where the protected health information is and where the risks reside, it's difficult to create an effective audit program. "You need to start out with a good, solid risk assessment."

Mikel Lynch, privacy officer with the University of Missouri, suggested that when conducting a risk assessment, compliance teams look at both outside access and inside access. However, he noted that inappropriate access to data usually comes from inside the organization. "The real risks to PHI that we're facing today seem to come more from the inside," he said.

Apgar also recommended that when developing an audit program, the organization should be viewed as a whole. He recommended involving a broad spectrum across the organization when creating an audit program, noting that e-PHI travels across all departments. "It's not something that's just relegated to your information technology department," he said.

Audit logs. Many organizations have legacy systems that don't have audit logs, systems that make it impossible to look back and find out what data was entered, when it was entered and who entered it, Apgar said, adding that the ability to create these logs is "one of the keys to a successful audit program." He also recommended talking with vendors to ask whether they can add the ability to create the audit logs necessary to monitor activity.

Developing a sound way of tracking who accesses the information will help the organization prove its innocence if it is ever challenged, Lynch added. In a couple of cases, patient information made public actually came from outside the healthcare institution that was given the black eye, he said. "You've got to be able to show that you were not the one releasing information, and an audit program can help with that."

Keep the audit simple. Audit programs should not be too complex, Apgar emphasized. "An audit program needs to also be simple, repeatable, and understood," he said. "This is not intended to be rocket science," he added. "If it is simple and people understand what your end goal is in the audit program, they're more likely to buy in. They're more likely to cooperate with the person responsible for the audit activity."

The program also needs to be repeatable, said Apgar. "If I do an audit on January 1st and then I do another audit on July 1st, it needs to be consistent," he said. Both audits should follow the same set of rules and the same processes, so that the organization can look at trends and changes over time, he said.

And the process needs to be understood, Apgar said. If there are too many audit logs, he cautioned, "You end up with

CCH Health Care Compliance Letter

Managing Editor
Pamela K. Carron, J.D.

Coordinating Editors
Angela Fanelli, J.D.
Sharon Sofinski

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard
Tax–Jeff Carlson, David Hansen

Designer
Patrick M. Gallagher

Comments from readers are welcome and should be directed to Sharon Sofinski at SOFINSKS@CCH.COM, Tel. 847-267-7860, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

so much information that it becomes, in a lot of respects, meaningless." Instead, he recommended collecting meaningful information that lets the auditor know if things are running smoothly or if action needs to be taken to fix a problem.

Organizations should give auditors the authority, either directly or through a superior, to take action when needed, for instance, when a system needs to be reconfigured or when a rogue employee needs to be disciplined. "If the person does not have the authority that goes along with the responsibility of the audit, then that position loses meaning within the organization," he cautioned.

Lynch added that it is usually the line managers and supervisors' responsibility to discipline rogue employees. "We certainly don't want our staff being seen as the sheriff in town," he said. "What we do is develop the information necessary for managers and supervisors to make good decisions and to take whatever action's appropriate."

In addition, Apgar and Lynch recommended organizations:

- Develop an audit schedule that establishes when the audits will occur. "Regular audits and regular audit process reviews are essential," Apgar said.
- Develop a plan for staff training. Auditors need to show employees that audits are not intended to punish the staff, but are there to help the organization create a better way of doing things, Apgar said. Staff should be trained continuously, he said. "You're going to have new staff coming in and out," he noted. "It's something that is a continuous process."
- Review audit criteria periodically to make sure that it addresses the risks that will change over time.
- Accommodate random and targeted audits. Targeted audits will become more prevalent, Lynch predicted, noting that he has seen success locating security breaches by following up on employee tips. "We're going to have to move more towards targeted audits, he said." Apgar added that it's also a good idea to audit when major system changes occur.
- Assign responsibility for conducting the audit. Apgar noted that it might be more than one person.

In addition, Lynch discussed some red flags auditors can look for. While these should alert the auditor to suspicious behavior, they do not necessarily indicate a breach, he said.

"Regular audits and regular audit process reviews are essential."

Auditors should pay particular attention:

- To all new employees during the first 60 days.
- When a user is logged in at more than one location.
- When a record is accessed more than 30 days before or after date of service.
- When the accesses aren't appropriate for the employee's job responsibilities. For example, if a nurse who works on the fourth floor is accessing patient information on the seventh floor, then "it's certainly worthy of asking the questions," he said.
- When there is a change in the pattern to accesses. For example, if an employee has always accessed patient information during the workweek and then suddenly accesses the information Saturday morning at 2:00 a.m., that might look suspicious, he said.
- When an employee has had discipline problems.
- When a department has an environment that's not very conducive to security or privacy. "We look at them more closely and more often," he said. For example, former President Clinton during his hospital stay reportedly had a number of people who accessed his record inappropriately.
- When coworkers are accessing information about workforce members who are patients, particularly coworkers in the same department. Lynch said this might lose patient business when employees are worried that their patient information will be accessible by the coworkers. ■

CCH Washington Bureau, October 11, 2004

Best practices for securing PHI

by Catherine Hubbard, MA, Contributing Editor

Compliance with the HIPAA Security Rule is not simply a technical problem to be solved by technical solutions. It's an organizational and a management issue that must be addressed in a comprehensive way, according to Robert Nied, an expert on the subject who spoke during an audio conference sponsored by the Health Care Compliance Association in September. Compliance with the rule is a continual process and "requires the support and buy–in of everyone in the enterprise," he said. Security programs have to evolve as the organization's environment and business conditions change and technology evolves, he noted.

Access Control

Controlling employees' access to personal health information is key to creating a successful security program, said Nied, CISSP, who, along with health care attorney Paul Litwak, has written a book on the subject, entitled *A Path to Compliance with the HIPAA Security Rule.*

"Everyone in an organization needs access to certain data that they need to legitimately perform their jobs, but no more," Nied emphasized. "Access control is the most important component of your security program. It is the principle that all of your technical security controls are designed to enforce," he said.

Access control should be enforced at all levels of the information technology infrastructure: at the network level, where people log on to the network, at the server level, at the workstation level, and the application level, Nied said. "There may be medical records that 100 people need to access, but they all may need to access only part of that information."

For example, Nied said, an employee who works at the front desk of a hospital needs access to records like patient names, phone numbers and insurance information. But under most circumstances, that person does not need access to detailed clinical records and physician notes, he said.

Litwak noted that the HIPAA Privacy Rule is consistent with the Security Rule, noting the similarity between the Privacy Rule's minimum necessary standard and the Security Rule's access control provisions. "They tie together nicely," he noted.

Unique Identifiers

Under the Security Rule, effective on April 21, 2005, anyone who has access to electronic health information must have a unique identifier. Currently, most organizations require employees to enter a personal password before logging in to a computer or system that contains personal health information (PHI).

Nied said that most employees use passwords that technically comply with HIPAA, but that are too easy to guess, such as the name of a child or a pet. Organizations should encourage employees to establish passwords that are difficult to guess but easy to remember, he said. He encouraged people to use password phrases. For instance the phrase, "My son likes to play soccer," would remind the person that the password is "msltps". Some simple substitutions, like turning an "s" into a dollar sign, would further increase the complexity of the password, he said. "It makes for a far more robust, far more resistant password, but it's still reasonable for the individual to remember," he noted.

Moreover, computers should time out within 15 minutes without use, Nied suggested, so that if an employee leaves his or her desk, others cannot access the electronic PHI. "Work stations should not be a portal to information for anybody. It should only be the source of access for the person who has a specific need for the information," he said. When the computer times out, it should not be reactivated unless someone re-enters the login information.

Biometrics

In addition, identifiers will become more secure in the future, Litwak predicted. Use of biometric forms of identification, such as retina scanning and other new technologies, is becoming more prevalent and may be required legally someday, he said. "That may become the standard of care for protection of confidential information," he added.

Nied noted a lot of industries that have stewardship of sensitive data are moving away from a simple password authentication method. The new technologies that Litwak mentioned "ultimately may represent best practices," he said, advising health care organizations to stay aware of current best practices. "Somewhere down the line to demonstrate due diligence, you may need to use things like biometric devices," he said.

Granting Access to PHI

There also needs to be a well-defined, well-documented process in place for requesting and granting access to electronic PHI. In a lot of organizations the process is informal, where an executive will call up the IT department and ask it to grant access to a new employee. The problem with this approach is that it's difficult to produce a defensible document trail to show the organization granted access in a reasonable, consistent way, Nied said. "Access requests should follow a very consistent process flow," he said, noting that the requests need to be approved by an appropriate person, and need to be documented. In addition, the documentation needs to be retained.

Access also should be periodically reviewed to confirm whether the person granted access has changed work groups, has changed titles, has retired or has been terminated. "Access privileges that people need to perform their job can change and evolve," Nied noted. "Make sure that people don't have access privileges in excess of what they need to do."

"Access control is the most important component of your security program. It is the principle that all of your technical security controls are designed to enforce."

Updating access privileges is particularly important when an employee is terminated, said Litwak. "You don't want an unhappy person to be able to get at your data," he said.

New Technologies

New technology developments will help organizations improve their security programs, said Litwak, noting that they are becoming more affordable. In New York, for instance, the state Medicaid agency gives people who need access to sensitive electronic data a temporary password combination that expires after about 90 seconds. "Even though it's more expensive than the current technology, it's getting cheaper every day."

When talking with software vendors, Nied said, compliance officers should ask whether the software provides the type of access control necessary to enforce privileged access across the enterprise. In addition, he noted, the IT department will need the training to configure the access controls.

Viruses and Spyware

"Antivirus software is absolutely vital in every workstation," said Nied. "It should be installed, activated and updated," he said. The updates should ideally be handled in a way that doesn't require intervention by users, for instance, a requirement that employees go to a website in order to update their virus definitions. "This should be done automatically," he said.

Spyware also is becoming a larger problem, often unaddressed in older antivirus software, Nied said. Its original purpose was to collect marketing information, but it also can be used for nefarious purposes. A lot of antivirus software that's a couple of years old is not catching the spyware, even when it's updated regularly, he cautioned. "The impact on an organization can be huge," he said. "It could impact ultimately the confidentiality of sensitive information." Spyware also slows down the network as it consumes bandwidth, and it can be a conduit for other infections. "It's very important that you look at the antivirus software you have, find out whether it's effective against spyware and if it's not, you need to either upgrade it, or augment it," he recommended.

Every year, organizations are struck with thousands of infections resulting from weaknesses in commercial operating systems. Organizations must deal with these weaknesses and develop a patch management system. "You need to have some systematic approach to patch management," Nied said. He recommended the IT infrastructure, when possible, install the patches without requiring action on the employees' part. "If you require user intervention, then chances are, human nature is going to miss things and your protection is not going to be current."

Litwak noted that all patches must be installed among all users, including those who work onsite and remotely.

Portable Computers

Organizations should develop a set of security standards for portable equipment, including laptops and even PDAs, said Nied, noting that laptops have become the principal vector of infection on corporate networks. "They are the principal way in which networks get infected," he said. "It's really important that you begin to develop a process for dealing with portable equipment," he said, noting that portable computers are only becoming more popular.

Laptops also increase exposure to physical theft, Nied said, suggesting that e-PHI should be encrypted. "Ultimately, a laptop may get stolen or lost. The only way to protect that information is to encrypt the information on the hard drive," he said.

In addition, Nied and Litwak offered the following advice to health care organizations:

- Make sure that all PHI is scrubbed from hard drives before disposing of them. Simply deleting files and folders is often not enough.
- Encrypt PHI in e-mails and don't include the name of the patient in the subject line. "Remember that the Internet

continued on page 8

Privacy Rule's first year: Good news and bad

by Sharon Sofinski, Coordinating Editor

A Government Accountability Office (GAO) study on first-year experiences with the HIPAA Privacy Rule reveals that while implementation of the HIPAA Privacy Rule went smoothly overall, problems still remain.

The study focused on the experience of providers and health plans in implementing the Privacy Rule; the experience of public health entities, researchers, and representatives of patients in obtaining access to protected health information (PHI) under the Rule; and the extent to which patients seem aware of their rights and protections under the Rule. The GAO gathered information by interviewing representative from a wide range of national organizations, and from the organizations' websites, surveys, and reports.

The GAO discovered that, during the first year covered entities were required to comply with the Privacy Rule, implementation went more smoothly than expected, initial confusion has diminished, and new privacy practices have become routine.

The organizations the GAO interviewed found many Privacy Rule provisions—for example, creating a notice of privacy practices and limiting disclosures for marketing—"straightforward and relatively easy to implement." Initial misunderstandings and questions about the Rule's provisions have subsided, they reported.

However, participants in the study noted that two Privacy Rule provisions continue to be difficult and burdensome:

- the requirement to account for certain information disclosures, and
- the requirement to develop business associate agreements with downstream users of PHI.

Accounting for disclosures. Study participants explained that creating and maintaining systems to track PHI disclosures requires a great deal of time and resources. They also expressed concern about the volume of disclosures that must be accounted for, and whether the accounting provision really benefits patients.

Business associate agreements. Participants are also concerned about the amount of resources needed to comply with the business associate agreement requirement. Some complained about the high costs for legal counsel to negotiate and customize such agreements, especially in organizations that have numerous business associates.

Entities that rely on access to PHI reported other problems under the Privacy Rule:

- According to public health entities interviewed, some states have had to take concerted action to ensure that providers' concerns about complying with the Rule do not impede the flow of important information to state health departments and disease registries.
- Research groups say the Rule has delayed clinical and health services research by reducing access to information.
- Consumer advocacy groups say that the friends and family of patients have had extreme difficulty in assisting patients because although providers and plans are permitted to disclose a patient's PHI in certain situations, they are reluctant to do so.

In addition, many patients and providers contend that the general public is not well informed about their rights under the Privacy Rule. Patients remain confused about the privacy notices they receive. In fact, of the approximately 2700 complaint cases that the Office for Civil Rights has closed as of April 13, 2004, almost two-thirds fell outside the scope of the Privacy Rule.

GAO recommendations. To improve the Privacy Rules' effectiveness, the GAO recommends that the Department of Health and Human Services (HHS):

- modify the Privacy Rule to require privacy notice to state that, when required by law, PHI will be disclosed to public health authorities;
- exempt public health disclosures from the accounting for disclosures provision of the Rule;
- improve the public's understanding of their rights under the Rule by launching an information campaign.

In a reponse letter dated August 26, 2004, HHS emphasized that it is aware of covered entities' concerns about the accounting for disclosures provision, and that it "continues to monitor experience with this aspect of the Rule, along with the benefits to consumers it affords, to determine whether modification of the Rule may be required." HHS also stressed that OCR will continue efforts to raise the public's understanding of their rights and protections under the Privacy Rule.

Study details. The GAO interviewed individuals from 23 national organizations representing health care consumers, health care providers (including the American Hospital Association and the American Medical Association), health plans (including America's Health Insurance Plans, The Centers for Medicare & Medicaid Services, and Blue Cross Blue Shield Association), state officials, public health agencies, researchers, privacy professionals, and a health care accrediting body (JCAHO). The study was conducted from March through August 2004. To view the GAO's complete report, visit the GAO website at www.gao.gov/cgi-bin/getrpt?GAO-04-965. ■

CCH Chicago Bureau, October 11, 2004

Unscheduled absenteeism rises to five-year high

by Theresa Houck, Contributing Editor

The rate of unscheduled absenteeism has climbed to a five-year high of 2.4 percent, up from 1.9 percent in 2003, according to the findings of the 14th annual *CCH Unscheduled Absence Survey*. The average annual per-employee cost of absenteeism declined slightly to $610, from $645 in 2003.

The survey also found that low morale continues to take a toll on higher costs and unscheduled absence rates. In addition, four generations now are in the work force and may require employers to take a fresh look at their work force demographics if they want to retain their top talent in the long term.

Most employees who fail to show up for work, however, aren't physically ill, according to the survey. In fact, only 38 percent of unscheduled absences are due to personal illness, while 62 percent are for other reasons, including family issues (23 percent), personal needs (18 percent), stress (11 percent) and entitlement mentality (10 percent).

Each year, CCH asks HR professionals to share information about absenteeism at their organizations. Key findings from this year's survey include the following:

- The unscheduled absenteeism rate has risen to a five-year high of 2.4 percent, up from 1.9 percent from in 2003.
- The average per-employee cost of absenteeism dropped to $610 in 2004, down from $645 in 2003.
- Personal illness and family issues continue to be the leading reasons for unscheduled absences.
- Employers now use an average of 8 work-life programs, up from 7 in 2003.
- Alternative work arrangements are used by 58 percent of survey respondents and rated as most effective in helping to reduce unscheduled absences, along with disciplinary action.
- Paid leave banks, also called paid time off (PTO), continue to be rated as the most effective method for controlling unscheduled absenteeism.
- Employers with higher morale in the workplace continue to benefit from fewer unplanned absences and lower costs.
- The number of employers allowing workers to carry over sick time from one year to the next has decreased from 51 percent in 2000 to 37 percent in 2004.
- Employers set aside an average of 4.7 percent of their budgets for absenteeism.
- The annual cost of employee no-shows can range from an estimated $60,000 for small employers to over a million dollars annually for large companies.

"The tight economy seems to have helped companies in holding the per-employee cost of absenteeism steady, but with the rate of unscheduled absences increasing, the overall out-of-pocket cost to employers rises accordingly," said Lori Rosen, an attorney, CCH workplace analyst and author of *HR Networking: Work-Life Benefits*. "This trend makes it all the more important to closely examine why employees aren't showing up for work and what work-life and absence control programs can be used to help stem the tide."

Morale continues to make a difference. Employee morale can affect absenteeism rates. In fact, rates of unscheduled absenteeism are more than one-third (35 percent) higher among companies with poor/fair morale (2.9 percent) than those with good/very good morale (1.9 percent). Similar to last year, 60 percent of respondents indicated morale at their company as good/very good while 40 percent rated morale as poor/fair.

Low morale has a high price tag. Overall, the CCH survey found that employers set aside an average of 4.7 percent of their budgets for absenteeism. When morale is factored in, however, organizations with good/very good morale set aside 4.0 percent of their budgets to cover the costs of last-minute no-shows, while poor/fair morale set aside 4.9 percent.

Morale influences reasons people call in sick at the last minute. Organizations reporting poor/fair morale were more likely to experience unscheduled absenteeism because of stress (15 percent) than organizations reporting morale as good/very good (10 percent). Also, while only 17 percent of organizations reporting good/very good morale believe that unscheduled absenteeism is a serious problem for them, 43 percent of organizations reporting low morale find it a serious issue.

Additionally, more than one-third (37 percent) of companies with poor/fair morale reported an increase in unscheduled absences over the past two years while only 15 percent of companies with good/very good morale reported an increase.

Work-life programs provide flexibility. According to the survey, organizations now use an average of 8 work-life programs, up from 7 in 2003. The increase in work-life programs is across the board. Notable are the overall increases in programs that offer employee flexibility and those related to health and fitness, and the increase in eldercare programs.

Worker flexibility helps them deal with family issues. Of the programs ranking highest in curbing unscheduled absences, the top programs, including alternative work arrangements, leave for school functions, telecommuting and compressed workweek, provide employees with greater control over when and where they work. Each of these programs showed an increase in use from 2003.

Employers are recognizing need for eldercare. The number of employers offering eldercare programs also has significantly increased, from 20 percent in 2003 to 32 percent in 2004. AARP and the National Alliance for Caregiving estimate that of the more than 44 million caregivers providing unpaid care to another adult and of those that work, an estimated 59 percent either work or have worked while providing care, and more than 60 percent have had to make adjustments in their work life or quit their jobs.

According to the CCH survey, the increased adoption of eldercare programs now puts it on par with both emergency childcare (offered by 31 percent of organizations) and on-site childcare (offered by 29 percent).

However, when asked if demographic changes in the work force would affect

continued on page 8

Human Resources (cont.)

their work-life programs, three-in-four companies (77 percent) believed it would not.

Absence control programs effective to a point. While respondents reported an increase in the use of work-life programs, they have decreased the use of absence control programs, now using 5.0 such programs, down from 5.6 last year.

Disciplinary action remains the single-most used absence control program, with 91 percent of surveyed organizations reporting use. The other leading absence control programs in use are:

- Yearly review (79 percent);
- Verification of illness (76 percent);
- Paid leave banks (63 percent); and
- Both no fault and personal recognition, each used by 59 percent of organizations.

The use of paid leave banks (PTO) continued to climb in popularity from 59 percent in 2003 to 63 percent this year.

PTO and disciplinary action were rated as the most effective absence control programs, each earning a rating of 3.5 on a scale of 1 to 5. PTO provides employees with a bank of hours to be used for various purposes instead of traditional separate leave programs for sick, vacation and personal time. Disciplinary action, as the name implies, penalizes employees for being absent.

Notably, organizations with good/very good morale rated the overall effectiveness of both their absence control policies and work-life programs 42 percent higher, at 3.8, than did their counterparts with poor/fair morale, at 2.2.

This year's survey found that full-time employees were offered less sick time on average last year, but continued to use about the same amount of sick time as in the year before. On average, companies granted 6.9 sick days to employees in the past year, down from 7.6 days in 2003, and employees used 5.8 days compared to 5.6 in last year's survey.

Employees are still coming to work sick. Presenteeism—a situation in which employees come to work even though they are ill and pose potential problems of contagion and lower productivity—continues to be an emerging area of concern. Similar to last year, the first time when employers were asked about this issue, 39 percent of respondents indicated that presenteeism is a problem in their organizations.

Despite higher rates of unscheduled absenteeism overall, companies with low morale have more ill workers showing up for work. In fact, 52 percent of organizations with poor/fair morale reported presenteeism was a problem, while just 31 percent of organizations reporting good/very good morale saw presenteeism as an issue.

"Obviously employers want their employees on the job and using as few sick days as possible. But a sick employee may not be doing their employer or co-workers a favor if their illness jeopardizes the health or productivity of their colleagues," said Rosen. ■

CCH Chicago Bureau, October 8, 2004

On The Front Lines (cont.)

is essentially an open network," said Nied. "Encryption of e-mail containing PHI is an absolute necessity."

- Be aware of gaps in physical security, such as unlocked doors, that can pose a threat to patient privacy.
- Develop firewalls that are consistent with best practices.
- Follow industry best practices. "If best practice approaches are adopted by your organization, the security of your organization is enhanced, confidentiality of sensitive information is protected and, ultimately, HIPAA compliance will be a natural byproduct," Nied said.

"The Security Rule is just a reflection of industry best practices, and a best practice approach makes perfect business sense regardless of your regulatory compliance imperatives," Nied said. "When you take a best practice approach to information security, the overall security of your infrastructure is improved, you reduce risk, you limit losses, you enhance branding and marketability and it's far more cost effective then ultimately picking up the pieces after an unfortunate incident," he concluded. ■

Catherine Hubbard is a writer/analyst in CCH Incorporated's Washington, DC, office. She holds a Master's Degree in Government and covers developments in health care, tax, banking and other areas for CCH publications. For more information on HCCA audioconferences, visit www.hcca-info.org.