CCH Healthcare Compliance LETTER

Volume 7, Issue 11 health.cch.com June 1, 2004

On The Front Lines

EMTALA compliance: Practical considerations by Sanford V. Teplitzky, Esq., and Steven R. Smith, Esq.

Compliance officers shift focus to monitoring compliance, improving education

by Catherine Hubbard, MA, Contributing Editor

Most health care organizations have accepted corporate compliance as a key part of their framework. They are increasing staff training, focusing on creating policies and procedures to improve compliance and are hoping to improve monitoring and evaluation of their organizations' compliance efforts.

However, when asked what specific goals they hope to achieve with their compliance programs in the next three years, a recent survey of compliance officers reveals a shift in focus away from HIPAA. Only 58 percent of the 624 officers who responded to the Health Care Compliance Association poll said HIPAA compliance is a chief goal, compared with 89 percent in 2002 and 84 percent in 2001. In contrast, 69 percent of officers selected creating new or revised policies and procedures as a key goal for the first time since the survey began in 1999. The poll was conducted from January 5 to February 5 and was released in April.

The top two goals—monitoring and auditing (87 percent) and education and training (75 percent)—have been in the top three list since the survey's inception in 1999. Sixty-eight percent of the respondents said monitoring and auditing is one of the biggest issues they face, while 63 percent reported keeping up with government regulations and 61 percent reported assessing compliance program effectiveness.

Regarding education and training, most officers (91 percent) said they conduct compliance training beyond the initial training and seventy-percent conduct annual training. Half said their employees spend between one and three hours in compliance training each year.

Most compliance officers use instructor-led training (73 percent) while 55 percent use computer-based/web-based training and 41 percent use video training. Thirty percent said they have a budgeted line item for training. Of those, one-fourth have a training budget of between $50 and $5,000 and 22 percent have a training budget of between $5,001 and $15,000.

Almost all officers report compliance activities to a governing board or owner and about half said they report quarterly. More than half of the officers said they spend at least 31 hours on compliance per week. For the full report, "6th Annual Survey: 2004 Profile of Health Care Compliance Officers," visit http://www.hcca-info.org. ■

CCH Washington Bureau, May 19, 2004

$430 million settlement in Warner-Lambert Neurontin case

by Sharon Sofinski, Coordinating Editor

Warner-Lambert has agreed to plead guilty and to pay over $430 million to settle charges in connection with its Parke-Davis Division's fraudulent marketing of the drug Neurontin. The investigation began when Dr. David Franklin, a former Warner-Lambert medical liaison, filed a whistleblower suit under the federal False Claims Act. Franklin will receive approximately $24 million of the settlement.

Off-label (unapproved) uses. Under the Food, Drug, and Cosmetic Act, a company must specify the intended use of a drug in its new drug application to the FDA. Once approved, the drug may not be marketed for any use that was not specified in the application. The FDA approved Neurontin in 1993 solely for adjunctive or supplemental antiseizure use by epilepsy patients. However, Neurontin was marketed to treat a range of illnesses, including pain disorders, bipolar mental disorder, attention deficit disorder, ALS (Lou Gehrig's disease), migraine headaches, seizures associated with drug/alcohol withdrawal, restless leg syndrome and as first-line monotherapy for epilepsy.

Furthermore, Warner-Lambert continued to promote Neurontin for for epileptic seizures and for treating bipolar disease *after* studies had shown it was ineffective. According to U.S. Attorney Michael Sullivan, "This illegal and fraudulent promotion scheme corrupted the information process relied upon by doctors in their medical decision making, thereby putting patients at risk."

Illegal marketing tactics. According to the U.S. Department of Justice, Warner-Lambert engaged in the following tactics as part of its "widespread, coordinated national effort to implement an off-label marketing plan" for Neurontin:

- Encouraged its sales reps to approach doctors with one-on-one sales pitches promoting unapproved uses of Neurontin, which often included false or misleading statements regarding the drug's efficacy and whether the FDA had approved it for those uses.
- Used "medical liaisons" who represented themselves as scientific experts in a particular disease in order to promote unapproved uses of Neurontin.
- Paid physicians to attend "consultants meetings," which included presentations about unapproved uses for Neurontin.
- Held teleconferences in which doctors were recruited by sales reps to call a number where they would listen to a doctor or a Warner-Lambert employee speak about unapproved uses of the drug.
- Sponsored "independent medical education" events on unapproved uses of Neurontin, often misleading members of the medical community about the content of the events, and going so far as to plant people in the audience to ask questions about Neurontin's benefits.

The illegal marketing techniques were quite successful in increasing prescriptions for Neurontin for unapproved uses. For example, sales of Neurontin to the Department of Veterans Affairs jumped from $287,000 to $43.2 million from 1994 to 2002, according to Bruce Sackman, Special Agent in Charge of the Northeast Field Office of the Office of Inspector General for the Department of Veterans Affairs. As a result of the marketing scheme, doctors wrote Neurontin prescriptions for Medicaid patients when the drug was not eligible for Medicaid reimbursement. Since the prescriptions were obtained fraudulently through false statements to doctors and by payment of illegal kickbacks, which included "consulting fees" and trips for doctors, state Medicaid programs were harmed.

Reaction to settlement. Dara Corrigan, Acting Principal Deputy Inspector General for the Office of Inspector General of the Department of Health and Human services, commented that the settlement " demonstrates the government's continued scrutiny of sales and marketing practices by the pharmaceutical industry to ensure that those who do business with our programs act properly."

Mark McClellan, Administrator of the Centers for Medicare & Medicaid Services said the settlement " sends a strong message in advance of implementation of the Medicare prescription drug benefit that our first priority will be protecting beneficiaries and the programs that serve them."

In a statement, Pfizer, the parent company of Warner-Lambert, assured that it "is committed to compliance with all healthcare laws and FDA requirements and to high ethical standards in all aspects of it business practices." Pfizer acquired Warner-Lambert in 2000.

For more details on the settlement, see the Department of Justice press release at http://www.usdoj.gov/opa/pr/2004/May/04_civ_322.htm. ■

CCH Chicago Bureau, May 14, 2004

CCH Healthcare Compliance Letter

Managing Editor
Pam Carron

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
Jason Wommack

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 Healthcare 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 Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Record $35 million settlement announced

by Sharon Sofinski, Coordinating Editor

The University of Washington physician practice plans have agreed to pay $35 million in restitution, damages, and penalties for overbilling Medicare and Medicaid, announced John McKay, U.S. Attorney for the Western District of Washington. The settlement amount is the largest ever paid by a practice group related to a teaching hospital for noncompliance with federal billing regulations.

University of Washington auditor Mark Erickson filed a whistleblower complaint in 1999 alleging that officials within the University's plans knew of billing problems involving departments associated with the University's medical school, yet did not take appropriate steps to correct those problems. Erickson's complaint launched a four-year federal investigation into the University's billing practices. Erickson will receive $7.25 million of the settlement under the *qui tam* provisions of the False Claims Act.

In addition to the settlement, the plans will also enter into a Compliance Agreement with the Department of Health and Human Services Office of Inspector General (OIG).

McKay stressed that "The quality of care provided by the University of Washington has never been in question. Settling this case allows everyone involved to move forward, while compensating the state and federal government for the errors of the past."

The OIG, Department of Defense Criminal Investigative Service, the FBI, and the state of Washington's Medicaid Fraud Control Unit took part in the investigation. The U.S. Attorney's press release is at http:www.usdoj.gov/usao/waw/press_room/2004/apr/UW.htm. The University of Washington has posted questions and answers regarding the settlement on its website at http://depts.washington.edu/hsnews/settlement/qa.html. ■

CCH Chicago Bureau, May 14, 2004

Laboratory, owners to pay $10 million to settle fraud charges

by Sharon Sofinski, Coordinating Editor

The U.S. Attorney for the Northern District of California announced that a clinical laboratory and its owners have agreed to pay $10 million to settle claims that they defrauded Medicare and Medicaid from 1996 to 2003.

Two former salesmen for Health Line Clinical Laboratories filed a whistleblower lawsuit alleging that the lab's owners, Aramais Paronyan, MD, and Natella Lalabekyan, added unnecessary blood tests to comprehensive blood test panels and profiles that physicians had ordered for Medicare and Medicaid patients. Paronyan and Lalabekyan did not disclose the additional tests to the physicians.

U.S. Attorney Kevin V. Ryan commented, "The allegations in this case suggest a systematic effort to take money designed to aid the elderly and ill and to line the defendants pockets instead." He added that such fraud and abuse is "fraud and abuse against the American taxpayer."

A copy of the U.S. Attorney's press release and related court documents are at http://www.usdoj.gov/usao/can. ■

CCH Chicago Bureau, May 11, 2004

Record state prison sentence obtained in Medi-Cal fraud case

by Angela M. Fanelli, J.D.

Tahir Saeed Sherani (Sherani), 38, was sentenced to 18 years and eight months in California prison for his part in a crime ring that defrauded California's Medi-Cal system of more than $20 billion. An Orange County jury convicted

continued on page 8

Letters to the Editor

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

On The Front Lines

EMTALA compliance: Practical considerations

by Sanford V. Teplitzky, Esq. and Steven R. Smith, Esq.

In this article, the authors review the requirements of The Emergency Medical Treatment and Active Labor Act ("EMTALA"), discuss how organizations should adopt a comprehensive policy that addresses each of those requirements, and stress that organizations need to educate employees about the policy as well any changes to their practices that may result from the policy.

The Emergency Medical Treatment and Active Labor Act ("EMTALA" or the "Act") was passed by Congress in 1986. The purpose for passage of the Act was stated by the Department of Health and Human Services in the preamble to the Final Rule on the Responsibilities of Medicare Participating Hospitals in Treating Individuals with Emergency Medical Conditions published September 9, 2003:

> Congress enacted these antidumping provisions in the Social Security Act because of its concern with an "increasing number of reports" that hospital emergency rooms were refusing to accept or treat individuals with emergency conditions if the individuals did not have insurance:
>
> the Committee is most concerned that medically unstable patients are not being treated appropriately. There have been reports of situations where treatment was simply not provided. In numerous other situations, patients in an unstable condition have been transferred improperly. [1]

As a result of these concerns, Congress passed the Act, which requires, in broad terms, that for hospitals with emergency departments, if an individual comes to the emergency department and a request is made on the individual's behalf for examination or treatment for a medical condition, the hospital must provide an appropriate medical screening examination and, if an emergency medical condition is found to be present, the hospital must also provide necessary stabilizing treatment or arrange for a transfer of the individual as permitted by the statute.[2] However, each of these broad requirements includes numerous details that must be adhered to in order for the hospital to be in compliance with the Act. In addition, the Act (and implementing regulations[3]) also contains many other requirements that a hospital must satisfy. Some of these other requirements are:

- To post signs in the emergency department that explain the rights of individuals with emergency medical conditions and women in labor who come to the emergency department for health care;[4]
- To create and maintain a list of physicians who are on call and to make certain decisions about conflicts that may be presented for physicians who may be on call at the same time for different hospitals or who want to perform elective surgeries while they are on call;[5]
- To maintain a central log on individuals who come to the emergency department;[6]
- To not delay the performance of a medical screening examination or the initiation of stabilizing treatment to inquire about insurance or payment for care;[7]
- To report other hospitals who inappropriately transfer patients to the hospital in violation of the Act; and[8]
- To comply with the various documentation requirements for transfers, consents and refusal to consent to treatment.[9]

Policy Development

Compliance with the Act requires a thorough understanding of its requirements and the applicable regulations. The best way to approach compliance with the Act is through the development and adoption of a comprehensive policy that addresses each of the Act's requirements.

"The initial charge of the committee should be to understand how the emergency department actually works in regard to the requirements of the Act regardless of what policies may exist currently."

The development of the policy is almost as important as the final policy. Key stakeholders should be involved in the development of the policy. This includes representation from emergency department physicians; the part of the medical staff responsible for the development of on call physician schedules, nurses and other professionals in the emergency department; the hospital's business department or office; and administrative personnel in charge of the emergency department. At some point, the hospital's legal counsel should also be involved to review the completed policy (at a minimum) or at an earlier point in the process to ensure that the individuals responsible for drafting the policy have a complete understanding of the requirements of the Act.

The initial charge of the committee should be to understand how the emergency department actually works in regard to the requirements of the Act regardless of what policies may exist currently. By having individuals who work in the emergency department as part of the committee responsible for policy development this task will be greatly facilitated. It is possible that a hospital's actual practice is significantly different from what a policy says it should be. By understanding the current practice, a hospital can assess how far it has to go to ensure that its practices are compliant.

The next step is to compare the actual practices in the emergency department with whatever policies exist at the hospital. It is imperative that the practices in the emergency department be consistent with the policies of the hospital because the personnel in the emergency department will change over time. The policy should be the constant in this equation so that any questions regarding practice can be resolved by reference to the policy.

The policy should bear a title that accurately describes the substance to follow. Too many hospital administrators and directors believe that the Act is designed to simply regulate how and when patients are transferred to and from hospitals. Policies are created and entitled as "transfer" policies with the intent that they satisfy the requirements of the Act. This is not only wrong, it is also dangerously misleading to employees of the hospital who may believe that their only obligation under the Act is to be concerned with transfers.

The policy should begin with a clear statement of the hospital's intent to comply with all aspects of the Act. This affirmatively puts employees and providers on notice of the scope of the policy and should eliminate any surprise at the detail that is encompassed within the policy. The policy should contain definitions of key words and phrases that are important to understanding the policy and the obligations of individuals under the policy. The policy should address the various requirements imposed by the Act on hospitals and physicians and the procedures the hospital chooses to put in place to deal with them. Some provisions of the Act allow the hospital flexibility in how it will address those provisions so it is important that a hospital make decisions about these issues either before or during the policy development process. This again emphasizes the need for guidance from an individual that is well versed in the requirements of the Act.

Education

After the policy has been completed, the hospital should ensure that all members of the emergency department, and other relevant individuals and departments, are educated about the policy and any changes to practice that will result because of the policy. One of the benefits of having the involvement of representatives of providers and other groups in the emergency department on the committee during development of the policy is to secure their buy-in to the final product. Those persons on the committee should also be involved in the education of others to the policy. It is likely that an explanation on any controversial issues from a representative of the same group will be more easily accepted than one from hospital administration.

"One of the benefits of having the involvement of representatives of providers and other groups in the emergency department on the committee during development of the policy is to secure their buy-in to the final product."

Hospitals should also consider periodic random audits to determine if the policy is actually being followed. Enforcement of the Act is driven by complaints. It only takes one complaint for an investigation to begin and the scope of the investigation will not be limited to the single complaint made. By performing random periodic audits, a hospital can ascertain for itself what weaknesses are occurring in its processes and practices and implement corrective measures.

Conclusion

EMTALA is a complex and important law that is applicable to most hospitals. Failure to comply with the requirements of the Act can lead to fines and decertification from Medicare. Compliance with the Act is best achieved by the development and adoption of a comprehensive policy that addresses all elements of the Act. The policy should be developed by a committee of individuals that is representative of the groups of providers that are most affected in practice by the requirements of the Act. The committee should also have advice from counsel that is knowledgeable in this area of the law in order to ensure that all of the requirements of the Act are addressed. Once an appropriate policy has been developed, the hospital should ensure that all relevant persons are educated about the policy. Finally, hospitals should consider periodic random audits to determine whether the practice in the hospital is consistent with the requirements of the policy.

Mr. Teplitzky is a Principal and Chairman of the Health Law Department of Ober, Kaler, Grimes & Shriver and is resident in the Baltimore office of the firm. Mr. Teplitzky offers his experience to clients—typically large health care companies and delivery networks—who seek help with fraud and abuse problems and representation in federal or state investigations. He is a former president of the American Health Lawyers Association and a frequent writer and lecturer on various health care fraud and abuse issues. Mr. Teplitzky can be contacted at (410) 347-7364 or by email at teplitzky@ober.com.

On the Front Lines (cont.)

Mr. Smith is a Principal of Ober, Kaler, Grimes & Shriver and is resident in the Washington, D.C. office of the firm. He has more than twenty years of experience focusing on general corporate matters and employment and labor law issues in a health care setting. Mr. Smith was the former Senior Vice President & General Counsel for a significant health care system where he was responsible for, among other things, insurance and risk management issues. He can be contacted directly at (202) 326-5006 or by email at ssmith@ober.com.

[1] 68 Fed. Reg. 53222, 53223 (quoting H.R. Rept. No. 99-241, Part 1, 99th Cong., 1st Sess. (1985), p. 27).

[2] 42 USC §1395dd (a) and (b).

[3] 42 CFR §489.24 and 42 CFR §489.20.

[4] 42 CFR §489.20 (q)(1).

[5] 42 CFR §489.24 (j)(1) and (2); 42 CFR §(r)(2).

[6] 42 CFR §489.20 (r)(3).

[7] 42 CFR §489.24 (d)(4).

[8] 42 CFR §489.20(m).

[9] See, e.g., 42 CFR §489.24(d)(3), (d)(5) and (e)(1)(ii)(B).

[10] See, e.g., 42 CFR §489.24 (j)(1) (requiring that hospitals maintain an on call list of physicians on its medical staff in a manner that best meets the needs of the hospital's patients).

HIPAA

Wireless communications and security: Special challenges

by Harris Beach, LLP

The core principles of the HIPAA Security Rules require covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and ensure compliance by the workforce. Although the Security Rules allow for significant flexibility, that does not mean the rules are any less stringent.

Wireless networking, known as WiFi (short for wireless fidelity) in the industry, has the potential to cause problems for entities attempting to meet the standards of the Security Rules. As the technology becomes more popular, wireless local area networks (WLANs) could be at the center of communications within hospitals and other medical groups, generating the security concerns. There are many ways that wireless devices can and will be used in health care delivery and administration, such as in accessing relevant medical records and other data so that health care professionals need only log in to check such data as prescriptions. Wireless technology will also be used in areas from checkout to billing.

Technology already in use. In a recent survey of Chief Information Officers, 72 percent of respondents reported that their facilities were currently using some form of wireless information system. According to the survey, wireless networks continue to be the technology that most respondents would like to implement in their facilities in the next two years. Obviously, this could lead to potential problems if the issue of compliance with the Security Rules is not seriously considered. In fact, the issue of stolen data has already been the subject of the commencement of a lawsuit. Thieves broke into the offices of Department of Defense contractor TriWest Healthcare Alliance and stole hard drives containing medical information of 562,000 Army personnel. A class-action lawsuit was subsequently filed against TriWest on behalf of the individuals whose data were stolen.

"In a recent survey of Chief Information Officers, 72 percent of respondents reported that their facilities were currently using some form of wireless information system."

WLANs use radio waves to transmit data. WLAN radio waves extend up to 300 feet beyond the walls of the buildings where access points are deployed. That means that hackers can scan for radio waves from a WLAN to hijack the radio signals. This is not a major security risk if the data transmitted across such WLANs are adequately encrypted.

Many provisions in the general Security Rules seem to be particularly relevant to WLANs, including the "addressable" standard of safeguarding equipment from unauthorized physical access, tampering and theft. Accordingly, it seems obvious that WLAN security features must make it difficult for a thief to access PHI by using a laptop or PDA stolen from an authorized user. The password standard of the Security Rules requires that, at a minimum, users must authenticate themselves using passwords before they use a portable device, and the portable device must be authenticated to a server before access is granted to the WLAN. Furthermore, the cryptographic keys used by portable devices to access the WLAN must be frequently changed.

Encryption. A fundamental safety measure necessary to protect the PHI transmitted through WiFi is to make the data transmitted meaningless to any intentional or unintentional attack. Encryption—scrambling the information by combining it with another piece of data called a key—and running them both through an algorithm (a mathematical operation) is the best way to protect the data.

All WiFi equipment is able to provide a basic type of encryption called Wired Equivalent Privacy (WEP). To use WEP, a key of 10 or 26 characters is entered into the wireless access point or router (the hub of the network) and

into each computer on the network. The wireless device and the individual computers the wireless device communicates with both use the WEP key as a password to recognize one another. At the same time, the WEP encrypts the data sent over the air and decrypts the data received. This only be done the first time, because once WEP has been activated and the key has been established, it does not need to be re-entered each time it is used, but rather the software retains the WEP to be activated each time.

WEP in its most basic form requires users to enter "hexadecimals"— combinations of numbers zero to 9, and letters A to F. Of course, utilizing a 26-key entry that combines such numbers and letters is not as easy as remembering one's mother's maiden name. This complicated entry process in a profession that is time-driven does not make for a user-friendly environment, despite its necessity.

Another problem is that most makers of WiFi equipment disable WEP by default, or even hide its existence. The idea of not confusing low-end users has removed a covered entity's ability to protect its data without an expert to set up WEP, as most WiFi units do not even include the process for utilizing encryption in the setup wizard or quick-start booklet, the two most common ways users begin. Only a thorough read of the instruction booklet will reveal how this can be accomplished. Unfortunately, most health care providers simply want to get up and running, without regard to detailed learning of how WEP and its encryption standard can act as the firewall necessary to protect PHI.

A newer encryption system called WiFi Protected Access (WPA) is both easier to use and much more secure than WEP. The home and small office user version of the product requires only a password called a "pre-shared key." WPA differs from WEP in that it uses the key as a starting point to generate a series of more complicated keys. The access point and the devices connected to it regularly generate new keys, rather than using the same one repeatedly as WEP does.

Of course, the danger is that a hacker may be able to guess a pre-shared key, though that would take some time. A simple process of utilizing a case-sensitive password and mixing in a few numbers or symbols can make WPA both easier and safer to use.

However, as is true in WEP, vendors are hiding the security feature. Of the five major access points offered through vendors, only one reveals WPA in the basic setup wizard.

Network. Because the WiFi is going to be part of a network, every piece of WiFi equipment must be connected and protected. Thus, all equipment must be verified to determine if it is capable of being used with WPA. For example, if the personal computers connected to the WiFi are running Windows XP operating system, the computers must have installed "Service Pack 1" and "patch Q815485" to add WPA to the wireless networking utility. Although it is simple enough to download the necessary plug-ins from Microsoft's website, the users must know what is needed. Older versions of Windows simply do not have wireless utility, so updated software from the wireless card of the laptop's built-in wireless chip must be updated.

Away from the covered entity's site. When WPA or WEB is utilized from a "hot spot" (a place other than in the basic location where it normally operates), keeping information secure is even more difficult. Currently, the mobile technology companies providing the hot spots are able to avoid the requirement of a pre-shared key. Instead, the central server of the company will generate encryption keys and send them directly to the computers of registered customers upon log-on. In addition, in virtual private networks (VPN) both the individual computer and the server to which it connects run software that provides both encryption and decryption, thus protecting the data as it is transmitted.

Furthermore, a network for health care professionals who log in from home or on the road is available in the form of a virtual private network. A common interface is provided for access to dozens of different WiFi hot-spot services, so that as long as the wireless device taps in through one of the services, the data would be protected. The problem, of course, is determining whether or not the covered service is being utilized; if it is not, the data will not be secure.

Another alternative when away from the covered entity is secure sockets layer (SSL). SSL can establish encryption for traffic between applications that communicate over the Internet, offering security when passwords or credit card numbers are entered, for example. The good news for covered entities is that SSL is standard in many recent versions of Web browsers, and even in some e-mail programs. When a connection with a home site using SSL is established, there is an icon (a closed padlock) at the bottom of the browser window showing the user that the security is in place.

continued on page 8

Healthcare jobs among the largest- and fastest-growing occupations

Healthcare jobs are among both the largest-growing and fastest-growing occupations in the United States, according to Bureau of Labor Statistics (BLS) projections for 2002-2012. The biggest increase will be for registered nurses (RNs), rising from 2.284 million in 2002 to 2.908 million in 2012, a jump of 27 percent. The BLS forecasts that medical assistant numbers will climb at a faster rate than any other occupation, from 365,000 to 579,000, up 59 percent. Five other healthcare occupations are among the 10 fastest growing: physician assistants, home health aides, medical records and health information technicians, physical therapist aides, and physical therapist assistants.

HIPAA (cont.)

Unfortunately, websites are not automatically utilizing SSL for everything on the site. For example, Yahoo allows SSL to be turned on, but it is not active in a user's in-box or when e-mail is sent.

Complete security. Even if the wireless technology is secured, it is critical to ensure that other standard safety measures remain in place. Thus, one cannot forget to utilize a standard firewall program. The bottom line, however, is that wireless technology is simply not as secure as hard line technology. Covered entities must ensure that the wireless technology that has become a normal part of doing business avoids the security pitfalls, and that the continued advances to secure wireless technology are integrated as they become available. ■

Adapted from the CCH HIPAA Security Guide

Fraud & Abuse (cont.)

Sherani on 21 felony counts, including identify theft, Medi-Cal fraud, grand theft, conspiracy and tax evasion. He was ordered to pay criminal penalties of $5 million as well as $2.5 million in restitution to Medi-Cal and $903,000 in back taxes to the state.

The criminal complaint was filed in 2002 after a three-year investigation into Medi-Cal fraud by the California Attorney General's Bureau of Medi-Cal Fraud and Elder Abuse (BMFEA). Twenty-three of 29 defendants in the case have been convicted of charges, including endangering public health, identity theft, submitting false claims to Medi-Cal and Medicare, money laundering, tax evasion and grand theft. The ring-leader of the operation, Surinder Singh Panshi, of South Orange, New Jersey, was sentenced in California in September 2003 to 16 years in prison on four felony counts including Medi-Cal fraud, grand theft, acts injurious to public health and tax evasion. He also was ordered to pay $2.5 million in restitution and $124,000 in back taxes to the state.

Medi-Cal fraud scheme. The crime ring operated a complex scheme using more than 15 clinical labs in Los Angeles, Orange and Riverside counties to illegally bill government health programs for tests that were never authorized by doctors, nor performed. Medical clinic employees were paid to draw excess blood from unsuspecting patients, and other blood was purchased from runaway children, homeless individuals and drug addicts.

The blood was tested at labs controlled by the crime operation, which then billed Medi-Cal using stolen confidential patient information that was shared between the labs. The scheme also involved the theft of doctors' identities to create false records showing the physicians authorized the labs to perform the tests. The crime ring also fostered a black market for blood and the stolen identities obtained by the defendants.

Money laundering. Some of the money stolen from Medi-Cal and Medicare was laundered through a small market in Jersey City, New Jersey. Checks issued by California, totaling approximately $15.5 million, were paid to the labs for fraudulent services, then cashed at the New Jersey market using fake identification. The funds also were laundered through several clinical labs, including four that Sherani operated.

Sherani was convicted in New Jersey in 1999 of conspiracy, kickbacks, Medicaid fraud and money laundering. The criminal activity for which he was convicted today occurred while he was on bail and on probation in the New Jersey charges.

For more details on the sentence, see the Department of Justice press release at http://www.usdoj.gov/opa/pr/2004/May/. ■

CCH Chicago Bureau, May 24, 2004