

# Indiana Security & Privacy Network Privacy Report

**November 17, 2011**

Posted: 31 Oct 2011 07:33 AM PDT

The number of large breaches reported to OCR continues to climb.

Close to 360 entities have [reported breaches of unsecured PHI](#) affecting 500 or more individuals, a spike of about one per day over the last month. On as late as September 23, the number stood at 330. It is 358 as of Oct. 28.

OCR began posting entities reporting the large breaches in February 2010, capturing breaches dating back to September 2009.

OCR has averaged about 18 entities per month on its list over the 20 months the website has been live.

## **Medical Records Found On Detroit Road**

POSTED: Tuesday, October 18, 2011

UPDATED: 6:51 pm EDT October 18, 2011

### **DETROIT --**

Thousands of medical records including names, addresses and Social Security numbers were found dumped on the side of a Detroit road.

The files were marked the property of Carpenter Health Center, which used to be located in Ann Arbor. The center closed about seven years ago.

The pile of records includes pictures of Dr. Irwin Lutwin, who worked at the center.

Lutwin said he had no idea how the records ended up on a road in Detroit.

"We put them into storage," he said. " ... (the records) shouldn't have been there. I really don't know what to do about it."

Melissa Woodside, 19, of Ypsilanti, said her files were among the pile. The records were from treatment she received as a 10-year-old girl.

"That's me. All my information. Social Security number. Birthday. Residence. Parents," Woodside said, as she sifted through the file. "It's really unacceptable."

The city of Detroit picked up the files after Local 4 contacted it. The city now has custody of the files.

City officials will work with Lutwin in disposing of the documents.

## [Unencrypted computer backup tapes go missing](#)

Posted: 18 Oct 2011 09:00 PM PDT

A pediatric health system in Wilmington, DL, [reported on its website](#) this month three missing unencrypted backup tapes from a computer system it phased out in 2004 are missing.

Nemours has notified affected individuals by mail and is offering one year of free credit monitoring and identity theft protection for those affected.

The health system reports no indication that someone stole, accessed, or misused the tapes. Independent security experts retained by Nemours say that highly specialized equipment and specific technical knowledge would be necessary to access the

information stored on these backup tapes, according to its statement on the website. No medical records are stored on the tapes.

Nemours learned of the incident September 8 when it discovered a locked tape storage cabinet containing computer backup tapes was missing. Nemours officials believe the cabinet was removed from a Wilmington facility on or about August 10 during a remodeling project.

The backup tapes contain patient billing information, including name, date of birth, insurance information, medical treatment information, and Social Security number. [2,000 patient records lost](#)

Posted: 17 Oct 2011 09:00 PM PDT

A New England dermatology system with offices in four cities lost more than 2,000 patient records when someone stole a computer flash drive from an employee's car, *The Metrowest Daily News* of Framingham, MA, [reported October 11](#).

Adult & Pediatric Dermatology, with Massachusetts offices in Marlborough, Westford, and Concord, and one in Wolfeboro, N.H., said someone stole the drive containing PHI for 2,200 patients.

According to the *Daily News*, the data stolen included:  
Digital photographs of surgical skin cancer procedures  
Operation reports and copies of consultation letters to referring doctors

A company spokeswoman told the newspaper someone stole the flash drive from inside a locked car outside the employee's home in Lowell, MA.

### **OIG releases HIPAA compliance target areas**

By [Dom Nicastrò](#) October 14, 2011

The OIG cited four HIPAA target areas it will review in the next 12 months:  
States' data security requirements under business associate agreements  
Medicaid security controls over state web-based applications

- OCR oversight of the HIPAA Privacy Rule
- OCR oversight of the HITECH breach notification rule

### **[Military Health Plan Data Breach Threatens 4.9 Million](#)**

Posted on: [10-11-2011](#) Posted in: [AHIMA](#), [Electronic Health Record](#), [Fusion Suite](#), [Healthcare](#), [HIMSS](#), [HIPAA](#), [HIT](#), [Uncategorized](#)

### **TRICARE says lost backup tapes fall under FTC jurisdiction, not HIPAA, so only offers 90 days of fraud protection.**

By Neil Versel for [InformationWeek](#)

A data breach involving nearly 5 million people treated at military healthcare facilities over a 19-year period is raising questions about whether U.S. Federal Trade Commission (FTC) rules supersede Health Insurance Portability and Accountability Act (HIPAA) regulations.

Last week, TRICARE, the managed care arm of the U.S. government's Military Health System, disclosed that contractor Science Applications International Corp. (SAIC) had lost backup tapes containing personally identifiable information—including some health data—of about 4.9 million people. The tapes contained data from electronic health records (EHRs) used at military hospitals, clinics, and pharmacies in the San Antonio area from 1992 until Sept. 7, 2011.

According to a statement from TRICARE, the records may include Social Security numbers, addresses, and phone numbers, as well as clinical notes, prescription information, and some lab data. TRICARE said that the tapes did not hold any financial information.

"The risk of harm to patients is judged to be low despite the data elements involved since retrieving the data on the tapes would require knowledge of and access to specific hardware and software and knowledge of the system and data structure," according to the TRICARE statement. "Since we do not believe the tapes were taken with malicious intent, we believe the risk to beneficiaries is low."

TRICARE said that SAIC reported the breach on Sept. 14. Citing a police report, the San Antonio Express-News reported that the tapes were stolen from an SAIC employee's car during a burglary the night before.

The TRICARE statement said that the U.S. Department of Defense and SAIC are working to identify all individuals whose data were compromised and that TRICARE will send notifications by mail. The process is expected to take 4-6 weeks.

People affected will not be provided with any private credit monitoring services. "The risk of harm to patients is judged to be low despite the data elements involved," the TRICARE notice said. TRICARE is directing enrollees to a FTC site where individuals can place a free, 90-day fraud alert on their personal credit ratings.

"It's clear that TRICARE is trying to position this under Federal Trade Commission regulations, not under HIPAA regulations," Ruby Raley, director of healthcare solutions at IT integration and security company Axway, Scottsdale, Ariz., told InformationWeek Healthcare.

Unlike HIPAA, FTC regulations don't require entities to sign agreements with "business associates" that hold third parties to the same standards when handling sensitive data. Also, HIPAA regulations require organizations to provide a year of credit monitoring to anyone who may have been affected by a breach. "They're only [offering] fraud protection for 90 days," Raley said of TRICARE.

Posted: 12 Oct 2011 09:00 PM PDT

*Editor's note: The following excerpt from the September [Briefings on HIPAA](#) is the fifth in a series of questions about the HITECH-required Office for Civil Rights (OCR) HIPAA compliance audits answered by Susan McAndrew, JD, deputy director of health information privacy for OCR.*

### **Will enforcement be an audit component?**

The audits won't be incident-driven, so a breach or violation won't be necessary to trigger an audit. "With audits, there is no necessary precipitating event," says McAndrew. "Audits are a type of review that serves more as a compliance improvement tool than an investigation of a particular violation that may lead to sanctions and penalties."

However, OCR isn't ruling out enforcement actions in response to audit results.

"Vulnerabilities and weaknesses found during the audit may need to be addressed through corrective action, and if serious compliance issues are uncovered in the course of the audits, those also must be addressed," she says. "Audits may uncover compliance issues that may trigger an enforcement action."

OCR also must decide whether to continue its audits beyond 2012.

OCR will evaluate the audit program and determine whether it is a good use of resources, McAndrew says. These determinations will influence future decisions about what to do with the findings beyond the end of the current contract in 2012.

### [Patient information discovered, removed from website](#)

Posted: 10 Oct 2011 09:00 PM PDT

Stanford (CA) Hospital & Clinics in [reported on its website](#) October 3 that it found a vendor's electronic file that included certain patient information on a student homework website and removed it the following day. But the information was out there for nearly a year.

According to Stanford, Multi-Specialty Collection Services, LLC (MSCS), a vendor, received encrypted patient information from the hospital for business purposes. MSCS decrypted the data and used it to create a spreadsheet. Then an MSCS staff member provided it to an unauthorized person who posted it on a student homework website to get help creating a bar graph and charts. SHC immediately suspended all work with the vendor and demanded that MSCS lock down all patient information. SHC terminated the vendor relationship. The vendor's file, posted September 9, 2010, included limited information about 20,000 patients treated in SHC's emergency department from March 1 through August 31, 2009, including:

- Patient's name
- Medical record
- Hospital account numbers
- Emergency department admission/discharge date
- Diagnosis codes related to the emergency department visit
- Billing charges

### [OCR official answers audit questions](#)

Posted: 26 Sep 2011 09:00 PM PDT

*Editor's note: The following excerpt from the September [Briefings on HIPAA](#) is the third in a series of questions answered by Susan McAndrew, JD, deputy director of health information privacy for the Office for Civil Rights (OCR).*

### **What is the anticipated scope of these OCR HIPAA audits?**

"OCR will look at overall compliance efforts as a way to ensure that effective protocols are in place for the audits of both the Privacy and Security Rules," says Susan McAndrew, JD, deputy director of health information privacy for HHS' OCR. Thus, rather than focusing its audits on a specific set of issues, OCR will be taking a general look at an entity's compliance.

Organizations selected for an audit will receive notification beforehand.

"The audit process will include standard components associated with most audits," says McAndrew.

For example, preliminary steps, such as document requests, will occur, she says. After on-site visits, auditors will send audited organizations reports and will communicate with CEs to ensure that everyone understands these reports, says McAndrew. "Audit reports generally describe how the audit was conducted, what the findings were, and what actions the covered entity is taking in response to those findings," she says.

### **Randy Trzeciak: Who's stealing information in your system?**

By [Dom Nicaastro](#) September 21, 2011

HIPAA Summit West nuggets from [Randy Trzeciak](#), technical team lead, Software Institute CERT Program, Carnegie Mellon University, Pittsburgh:

- Who's sabotaging information from your system? And what are the details? These are results from a CERT "insider threat" analysis across several industries:
  - **What:** 35 percent of cases are IT sabotage
  - **Current or former employees:** Former
  - **Type of position:** Technical
  - **Gender:** Male
  - **Target:** Network systems data
  - **Access used:** Unauthorized
  - **When:** Outside normal working hours
  - **Where:** Remote access
  - **Collusion:** None
- On the fraud front:
- Credit card on black market: \$1
- Patient information authorized record: \$14 to \$18

Categories : [HIPAA Summit](#)

### **Angel Hoffman: Educate, make policy around social media**

By [Dom Nicaastro](#) September 21, 2011

HIPAA Summit West nuggets from [Angel Hoffman, RN, MSN](#), corporate quality/compliance officer, Kane Regional Medical Centers; and principal, Advanced Partners in Health Care Compliance, Pittsburgh:

- Hoffman began her presentation by pulling out of her purse a Droid, Blackberry, thumb drive and Tablet, illustrating all the portable devices we carry on us these days.
- The Pittsburgh Pirates fired an employee for inappropriate Facebook posts about the organization. But the Pirates did not have a policy for social media use, and because of that, had to rehire the employee.
- Hoffman said it's important to have a sanctions policy along with everything else because what good is a policy without enforcement?
- Remind employees that when something's written, it never goes away. Organizations cannot ban social media use among its employees, but they must have a policy for it and educate employees.

### **Ali Pabrai: United Nations was hacked; you could be, too**

By [Dom Nicaastro](#) September 21, 2011

HIPAA Summit West nuggets from [Ali Pabrai](#), MSEE, CISSP (ISSMP, ISSAP), of HIPAA Academy and efirst out of Newport Beach, CA:

- Pabrai said 97 percent of chief information officers are concerned about data security. "My question is who are these other three percent?" Pabrai also said one in four organizations have reported a data breach. Last year, there were between 250,000 to 500,000 medical identity thefts.
- In August, McAfee reported that hackers broke into the United Nations data system and hid there for two years unnoticed. "How do we know that someone isn't hiding in our systems, and how long have they been there?" Pabrai asked the audience. "Do we have appropriate controls? What is the state of our information security?" Do you have intrusion protection and intrusion prevention in place?
- "This is not just a compliance issue," Pabrai said. "This will have significant risk to the organization and will impact your facility in the seven figures."
- Pabrai reports seeing skill sets in organizations' IT departments lacking. "We're falling behind," Pabrai said. "What do we need to do to enhance those skills and that knowledge?"
- Social media and portable devices are concerning, Pabrai said, because they're transmitting information across a 3G or a 4G network and not through an organization's firewall system. "You make take a photograph now, and you're transmitting that information about patients across a network structure that even the best organizations with the best security controls cannot" protect. Social media, Pabrai said, is an "area of significant challenge."
- Protected Health Information (PHI) is critical, but take a look at Personally Identifiable Information (PII) as well. Go beyond PHI, and think beyond your physical assets and view data itself as an asset.

- The important information security ventures for an organization in 2012 will be encryption, authentication and encryption, Pabrai said. And right behind encryption? Authentication. “There too many generic accounts across the industry where you cannot trace an action back to an individual,” Pabrai said. “The user has to be able to trace things back to individuals, and you just cannot do that with generic accounts.”

### **Michael Kruley: 34,000 PHI breach reports affecting 500 or fewer individuals**

By [Dom Nicaastro](#) September 20, 2011

HIPAA Summit West nuggets from [Michael Kruley](#), OCR regional manager, San Francisco:

- Regarding breaches of unsecured PHI, OCR has received more than 300 reports of cases affecting 500 or more individuals since September of 2009 (330 to be exact as of today).
- OCR has received about 34,000 reports of breaches affecting fewer than 500 individuals
- Some great numbers on the 500-or-more breaches and the type of breach:
  - Theft: 50%
  - Unauthorized access disclosure: 20%
  - Loss: 16%
  - Hacking/IT: 7%
- And some great numbers on where those breaches are coming from:
  - Paper records: 24%
  - Laptop: 23%
  - Desktop computer: 17%
  - Portable electronic device: 16%
  - Network server: 10%

### **Adam Greene: HHS has received 60,000 privacy complaints**

By [Dom Nicaastro](#) September 20, 2011

HIPAA Summit West nuggets from [Adam Greene, JD, MPH](#), lawyer at Davis Wright Tremaine and former OCR lawyer, who opened up the HIPAA Summit West today:

- Since the inception of HIPAA, the government has received 60,000 complaints regarding privacy issues.
- Greene also said he expects more enforcement out of OCR like the UCLA case which cost that medical facility \$865,000 for employees who snooped at records.
- He doesn't expect enforcement to be at a “speeding ticket” pace, but OCR is not going to be lax, he said.
- As for final rules on the HITECH Act due out from OCR, Greene guesses it will take OCR at least another two months.
- One proposed rule — the accounting of disclosures rule that came out in May — has received 400 comments, Greene said.

### **OCR's new head: Leon Rodriguez**

By [Dom Nicaastro](#) September 14, 2011

Leon Rodriguez, the new leader of the government's HIPAA privacy and security enforcer, last served as chief of staff and deputy assistant attorney general for the Department of Justice Civil Rights Division.

HHS Secretary Kathleen Sebelius formally announced Rodriguez' appointment as the new director of the Office for Civil Rights (OCR) in a [September 13 press release](#).

Here is some more background on Rodriguez:

- Served as the county attorney for Montgomery County, MD, leading efforts to provide legal advice and services to county departments, agencies, boards, and commissions, as well as the County Council
- Was shareholder in the Health Law department of Ober, Kaler, Grimes & Shriver
- Named "Outstanding Health Care Litigator" by *Nightingale Health Care News*
- Served on the board of the Montgomery County Primary Care Coalition, an organization that developed and implemented healthcare programs for uninsured county residents
- Served as federal and state prosecutor in various jurisdictions
- Was the first assistant U.S. attorney, serving in Pittsburgh, PA, and assigned to the prosecution of healthcare fraud cases Served as the first assistant U.S. attorney, Chief of the White Collar Crimes Section
- Served as a trial attorney in the Criminal Section of the U.S. Department of Justice, Civil Rights Division
- Was assistant district attorney in Brooklyn, NY for six years
- Graduated from Brown University and Boston College Law School
- Fluent in Spanish and French

### **Miami couple faces lengthy sentence for Medicare fraud-September 13, 2011**

***A Miami couple who owned a South Florida chain of mental health clinics face spending the rest of their lives in prison for ripping off millions from Medicare.***

#### **BY JAY WEAVER**

Lawrence Duran was a Miami healthcare executive who regularly lobbied Congress in favor of legislation to boost government subsidies for his industry: community mental health centers. He visited with U.S. Rep. Ileana Ros-Lehtinen in Washington to drum up support. He, his girlfriend and other members of his lobbying organization threw a fundraiser for another Miami congressman, Rep. Kendrick Meek, when he ran for the U.S. Senate.

But Justice Department officials paint a far more sinister portrait of Duran and his girlfriend, Marianella Valera. They say the lobbying work was all a front to help them steal more money from the taxpayer-funded Medicare program.

Now Duran and Valera, who each pleaded guilty this year to Medicare fraud charges of running the biggest mental-health racket in the nation, face the prospect of spending the rest of their lives in prison for orchestrating the \$205 million scam.

If U.S. District Judge James Lawrence King sides with prosecutors at a sentencing hearing Wednesday, Duran, 49, and Valera, 40, could be imprisoned for 50 and 40 years, respectively. Those sentences would be the longest prison terms ever for Medicare fraud offenders in the country, surpassing 30 years given to a convicted Miami doctor for her role in an \$11 million HIV-therapy scheme.

Duran and Valera, who once lived together in a waterfront condo, traveled overseas and owned luxury cars, co-owned American Therapeutic Corp. Until the feds shut down the Miami-based company last October, it operated a chain of seven mental-health clinics in South Florida and Orlando that duped Medicare into paying the couple's business \$87 million during the past decade.

In the past year, Duran and Valera were charged along with 32 other American Therapeutic employees, psychiatrists, counselors, nurses, marketers, patient recruiters and others who supplied Medicare beneficiaries in exchange for kickbacks. American Therapeutic billed Medicare for thousands of patients, including many with dementia and Alzheimer's disease, who had no way of benefiting from the company's costly group-therapy sessions, prosecutors said.

Duran and several of the employees also held "charting" parties, where they would falsify the medical records of beneficiaries to make it look like they needed therapy when they actually didn't.

## **Report: Breach Leads to Online Data Posting**

Published September 09, 2011

NEW YORK – Stanford Hospital in California has confirmed that a privacy breach led to medical information for thousands of emergency room patients to be posted online, according to the New York Times.

The data for 20,000 patients, including names and diagnosis codes, remained on a commercial website for nearly a year until the breach was discovered last month, the newspaper reported on its website Friday.

The Palo Alto hospital has been investigating how the material made its way from one of its vendors to a website that allows students to solicit paid assistance with their schoolwork.

Gary Migdol, a spokesman for Stanford Hospital and Clinics, told the paper that the data first appeared on the site on Sept. 9, 2010, as an attachment.

Even as government regulators strengthen oversight by requiring public reporting of breaches and imposing heavy fines, the Times reports that experts on medical security said the Stanford breach spotlighted the persistent vulnerability posed by legions of outside contractors that gain access to private data.

The material also included admission and discharge dates and billing charges for patients seen at Stanford Hospital's emergency room during a six-month period in 2009,

Migdol said. It did not include [Social Security](#) and credit-card numbers or other information used to perpetrate identity theft, he said.

"It is clearly disturbing when this information gets public," he said. "It is our intent 100 percent of the time to keep this information confidential and private, and we work hard everyday to ensure that."

Migdol said Stanford had concluded that "there is no employee from Stanford Hospital who has done anything impermissible."

He said he expected the federal Department of Health and Human Services to conduct its own investigation. Susan McAndrew, a deputy director in the department's Office for Civil Rights, told the newspaper that she could not discuss whether an investigation was in progress.

### **AHIMA E-ALERT - Chronology of Data Breaches-September 11, 2011**

Data security breaches can happen anywhere and anytime with our nation's many technological advances. But how can we find out about those violations and information on how they were remedied? The [Privacy Rights Clearinghouse](#) has developed a central, easy-to-search Web site that contains security breaches from all of the United States. It also includes information on what to do if you discover your personal information may have been compromised. This list is updated every two days and can be queried by state.

### **NFL quarterback believes in HIPAA**

By [Dom Nicaastro](#) August 30, 2011

We never thought we'd link to ESPN on this blog, but lo and behold, we found a way.

Peyton Manning, future Hall of Fame quarterback for the Indianapolis Colts, cited HIPAA when approached by reporters about the status of an ailment.

"I don't know what HIPAA stands for," [ESPN reported Manning telling the media](#), "but I believe in it and I practice it."

And kudos to ESPN for linking to the Office for Civil Rights website on HIPAA.

Hey Peyton — it's Health Insurance Portability and Accountability Act, for the record. We bet Tom Brady knows that.

8/23/11

An Indiana prosecutor [will ask](#) the Office for Civil Rights to investigate the apparently intentionally circulated medical records of a city judge following his stay at IU Health Ball Memorial Hospital.

### **Lost Thumb Drive Causes Data Breach**

Joseph Goedert  
HDM Breaking News, August 15, 2011

St. Francis Hospital in Wilmington, Del., has notified 474 former maternity patients who had participated in a prenatal and maternity care program a decade ago that a lost thumb drive contained their names and some medical information.

The information was in two files of the thumb drive that were not password protected, and the drive was not encrypted. *The News Journal* in Wilmington reports a physician lost the drive during the spring and didn't realize it was missing until an unknown sender mailed it to the physician's home.

The drive did not contain such information as Social Security numbers, home addresses, phone numbers, billing or insurance information, or babies' names.

St. Francis in a statement says it's reviewing its policies regarding thumb drives, reeducating staff members and considering use of software that automatically encrypts files transferred from hospital computers to a thumb drive.

### **OCR: Walgreens HIPAA investigation continues**

By [Dom Nicaastro](#) August 11, 2011

An Office for Civil Rights investigation into the nation's largest drugstore chain for potential HIPAA violations that cost the industry's second- and third-largest chains millions of dollars in settlements one year later is still just that – an investigation.

Last August, OCR confirmed its investigation into Walgreens based on the same television media reports that led to million-dollar settlements with CVS and Rite Aid for potential HIPAA violations.

### **HIPAA auditor involved in own breach**

By [Dom Nicaastro](#) August 8, 2011

The company hired by the Office for Civil Rights (OCR) to conduct nationwide HIPAA privacy and security compliance audits was responsible for a breach that includes the loss of an unencrypted flash drive and affects more than 4,500 patient records.

OCR's request for audit proposals came in February 2011, about eight months after KPMG, LLP, reported its breach to the New Jersey healthcare system.

KPMG, which won OCR's \$9.2 million contract for HITECH-required HIPAA audits in June 2011, told the Saint Barnabas Health Care System of West Orange, NJ, in June 2010 that a KPMG employee lost an unencrypted flash drive that may have contained a list with some patient names and information about their care, Saint Barnabas reported on its [website](#).

The potential breach affected individuals at two facilities—3,630 patients at Saint Barnabas Medical Center in Livingston, NJ, and 956 patients at Newark Beth Israel Medical Center in Newark, NJ—according to a report on the OCR [breach notification website](#). The website lists entities reporting breaches affecting 500 or more individuals, a HITECH requirement that went live in February 2010.

The flash drive did not include patient addresses, Social Security numbers, personal identification numbers, dates of birth, financial information, or other identifiable information, according to the report on the Saint Barnabas website.

KPMG reported the matter to the New Jersey healthcare system June 29, 2010. KPMG believes the flash drive was misplaced on or about May 10, 2010, according to Saint Barnabas.

“KPMG believes that it is possible that the patient data was deleted from the flash drive prior to the time when it was lost,” according to the healthcare system’s report. “KPMG has also concluded that there is no reason to believe that the information on the flash drive was actually accessed by any unauthorized person. ... KPMG has told us the company is implementing measures to avoid similar incidents in the future, including additional training and the use of improved encryption for its flash drives.”

### **OCR undecided on including BAs in HIPAA audits**

By [Dom Nicaastro](#) – 8/5/11

The Office for Civil Rights (OCR) is undecided whether to include business associates (BAs) in its HIPAA-compliance audit plans per a \$9.2 million contract it awarded last month.

Susan McAndrew, JD, OCR’s deputy director of health information privacy, says the contractor, KPMG, LLP, will be developing protocols to support business associate audits.

However, “OCR has not yet determined whether it will audit business associates in addition to covered entities during the audits that are anticipated to take place in 2012,” McAndrew says.

### **HEALTH DATA MANAGEMENT – JULY 2011**

#### **ALLINA TERMINATES 32 FOR SNOOPING**

Minneapolis-based Allina Hospitals and Clinics have fired 32 employees for improperly accessing treatment records of a dozen teenagers who overdosed on a synthetic drug on March 17, the Minneapolis Star/Tribune reports. Twenty-eight employees at Unity Hospital were fired, as were four others at Mercy Hospital. An Allina spokesperson told the newspaper that the employees worked in patient care but did not have legitimate reasons for accessing the information.

### **HIPAA UPDATE – HCP<sub>ro</sub> – SEPTEMBER 30, 2011**

#### **FAKE PHYSICIAN PLEADS GUILTY IN \$1.2M FRAUD SCHEME; INCLUDES HIPAA VIOLATION**

A fake physician who treated more than 1,000 people in two states, collected approximately \$1.2M for the “care” he provided, and then tried to sell individuals’ health information, pleaded guilty in federal court in Atlanta last week to charges related to the scheme, according to a Dept. of Justice release.

Matthew Paul Brown, 30, formerly of Atlanta, GA and Nashville, TN, worked with licensed physicians in both states from November 2009 to April 2011 and used their provider numbers to collect approximately \$1.2M in false claims with Medicare, Medicaid and private insurance companies, federal prosecutors said.

Brown, who has never held a license to practice medicine, administered care in the physician's offices and at health fairs, with the physicians agreeing to pay Brown between 50% and 85% of the take. Federal prosecutors found no indication that the physicians who worked with Brown knew he was a fraud.

Brown was indicted in April. He pleaded guilty Tuesday, September 13, in U.S. District Court in Atlanta to charges that include 17 counts of healthcare fraud, each of which carries a maximum sentence of 10 years in prison and a fine of up to \$250,000.

### **Michael Leoz: HIPAA audits in developmental phase**

By [Dom Nicaastro](#) 9/20/11

HIPAA Summit West nuggets from Michael Leoz, OCR deputy regional manager, San Francisco:

- "Make those real," Leoz said about HIPAA privacy and security policies and procedures. Don't just have them sit on the shelf.
- In the case involving a laptop left on a subway by a Massachusetts General Hospital in Boston, Leoz said OCR found policies and procedures that weren't adequate for HIPAA privacy and security compliance. It led to a \$1 million settlement and a corrective action plan.
- **HIPAA HITECH audits:** Leoz talked about the upcoming audits by OCR contractor KPMG. He said the audits will review covered entities' approach to HIPAA compliance. He said the audits would lead to more preventative measures entities can take rather than creating a reactive culture. Leoz added there would be an increased potential for learning among covered entities because of these audits.
- **HIPAA HITECH audits:** 20 to 25 covered entities will be part of a testing phase. "We're going to try to look at different types of covered entities," Leoz said. OCR's contractor will be looking for what programs all kinds of covered entities have in place. "We will give an advance notice of the audit," Leoz said. "There will be a comprehensive data request and some on-site visits from OCR contractors who will interview covered entities' staffs."
- **HIPAA HITECH audits:** Now, OCR is in the developmental phase of the audits for the next three months. Next, there will be a testing phase, and Leoz said he doesn't see the actual audits starting before November.
- About eight questions came from the audience for this presentation: all, except two, on the upcoming HIPAA/HITECH audits. The other? Training.