Volume XII, Number 5 Monday, March 28, 2005

*From the Desk of R. Lewis Dark...*

# THE DARK REPORT

**RELIABLE BUSINESS INTELLIGENCE, EXCLUSIVELY FOR MEDICAL LAB CEOs / COOs / CFOs / PATHOLOGISTs**



**Restricted information, see page 2**

Commentary & Opinion by...

R Lewis Dark

Founder & Publisher

## *Is Your Lab at Risk from Patient Identity Theft?*

REMEMBER THE CASE OF THE PHLEBOTOMIST in San Francisco who was discovered reusing butterfly needles? This incident revealed how vulnerable a laboratory—and its public reputation for integrity—is to actions by a rogue or renegade employee.

That was back in 1999. A phlebotomist working for **SmithKline Beecham Clinical Laboratories** (SBCL) was found to be washing and reusing butterfly needles. *(See TDR, April 26, 1999.)* The incident generated national headlines. Tracing back to every patient service center where that phlebotomist had worked in previous years, between lab regulators and SBCL, some 15,000 people were offered testing to determine if they might have become infected because of this phlebotomist's actions.

In a similar fashion, you are about to learn how another phlebotomist, Richard Gibson, employed in the laboratory at **Seattle Cancer Care Center**, put his employer in the media spotlight when it was discovered he had stolen the identify of a critically-ill cancer patient and opened multiple credit accounts under the patient's name.

I'll bet you didn't hear about this story. Although it was national news when Gibson was convicted last summer as the first individual ever to be charged under HIPAA (Health Insurance Portability and Accountability Act), few people in the lab industry gave it more than passing interest. That changes with this issue of THE DARK REPORT.

We have been researching patient identity theft as a growing problem that will need a strategic response by labs and pathology group practices. During this research, THE DARK REPORT ferreted out a key fact overlooked in the Gibson case. He was a phlebotomist and committed the crime while employed by a hospital laboratory. This went unnoticed in the lab industry.

I believe the fact that the first person criminally convicted under HIPAA was a phlebotomist changes this story from something of mere passing interest to a high-priority alert for every laboratory and pathology group in the U.S. It's a major event that warrants the full attention of all laboratories and pathology group practices. To help you prepare your laboratory for this new risk factor, this issue of THE DARK REPORT gives you extensive intelligence and lessons learned from the people actually involved in dealing with the aftermath of this crime of patient identity theft. TDR

# Phlebotomist Convicted For Theft of Patient ID

*Yes, it was a phlebotomist! Labs should take steps to review and tighten their policies*

***CEO SUMMARY:*** ***Patient identity theft by a phlebotomist, prosecuted and convicted under HIPAA. This is a story whose true dimensions went unreported within the laboratory industry—until now! THE DARK REPORT is first to alert its clients to the possibility that every laboratory and pathology group practice may be at greater risk from internal patient identity theft than previously thought.***

HERE'S A NEWS FLASH that may shock laboratory administrators and pathologists all over the country. Federal prosecutors have convicted their first violator of the HIPAA law—and it's a phlebotomist who stole a patient's identity!

The implications of this situation are profound. Every laboratory and pathology group practice may be at greater risk for patient identity theft than from violations of HIPAA. This is a story exclusive to THE DARK REPORT.

The intelligence briefings in this issue are designed to help clients and regular readers in three ways. First, to understand the facts behind this case. Second. to learn about overlooked flaws in laboratory procedures that give employees an opportunity to commit patient identity theft. Three, to identify strategies and policies that can reduce risks from laboratory employees who intentionally attempt to steal patients' identities.

The facts in this case are simple. Richard W. Gibson was a phlebotomist once employed in the lab at **Seattle Cancer Care Alliance** (SCCA), part of the **University of Washington Medical Center** system in Seattle, Washington.

In October 2003, Gibson began using protected identity data that he had stolen from a patient receiving treatment for a rare and often fatal form of cancer at SCCA. *(See pages 9-10.)* When the patient began receiving letters from banks and credit card companies thanking him for his business—and, not long after, bills for over $9,000 worth of mer-

THIS PRIVATE PUBLICATION contains restricted and confidential information subject to the TERMS OF USAGE on envelope seal, breakage of which signifies the reader's acceptance thereof.

THE DARK REPORT Intelligence Briefings for Laboratory CEOs, COOs, CFOs, and Pathologists are sent 17 times per year by The Dark Group, Inc., 21806 Briarcliff Drive, Spicewood, Texas, 78669, Voice 1.800.560.6363, Fax 512.264.0969. **(ISSN 1097-2919.)**

R. Lewis Dark, Founder & Publisher. Robert L. Michel, Editor.

SUBSCRIPTION TO THE DARK REPORT INTELLIGENCE SERVICE, which includes THE DARK REPORT plus timely briefings and private teleconferences, is $11.90 per week in the US, $12.50 per week in Canada, $13.65 per week elsewhere (billed semi-annually).

chandise that he had not purchased—from his hospital bed he immediately began to question these developments. His efforts triggered a police and FBI investigation which eventually nailed the perpetrator.

## Well-Liked Phlebotomist

Richard Gibson is an experienced phlebotomist who was well-liked by patients at SCCA. Every day, the cancer patient who became a victim of Gibson's crime, observed him from his hospital bed. The police investigation into the patient identity theft case was solved when Gibson was finally identified by co-workers. They recognized Gibson after a local news station broadcast footage from a surveillance camera videotape that showed Gibson making a purchase with one of the fraudulently-obtained credit cards. Gibson was fired shortly after SCCA learned of the incident.

Following his termination, Gibson had the gall to apply for unemployment benefits. The administrative law judge did not believe his story that he had retrieved the protected patient information from a piece of paper on the floor of a rest room at SCCA. The judge denied his claim, stating that it was his belief Gibson had obtained the information from the patient's confidential files inside SCCA.

## Charged Under HIPAA

A number of factors in the Gibson case caught the attention of federal prosecutors as a violation of HIPAA laws. "Once it was known that the person identified was a healthcare worker, our office and the FBI asked to take over the case from the local authorities," stated Assistant U.S. Attorney Susan Loitz, of the **United States. Attorney's Office of the Western District of Washington**.

Gibson's case did not take long to resolve. In August, 2004, he agreed to plead guilty to charges to "wrongful disclosure of individually identifiable health information for economic gain." At this time, the national media covered the story because it was the first criminal conviction under the HIPAA law.

Then, on November 5, 2004, Gibson was sentenced by U.S. District Court Judge Ricardo S. Martinez in Seattle. He was sentenced to 16 months in prison and at least $15,000 in restitution. Again, this story caught the attention of national news media. But until this issue of THE DARK REPORT, no one in the laboratory industry had made the connection that Gibson was a phlebotomist—and that this was a case of patient identity theft to which any laboratory and pathology group practice could be vulnerable.

## Federal Attorney's Decision

"We could have charged Mr. Gibson with unlawful identity theft," explained Loitz, "but the healthcare connection made it more important that a HIPAA crime should be charged."

Loitz, who prosecuted the case, noted that Gibson "is a phlebotomist who was employed by a covered entity. Mr. Gibson had direct contact with patients. It was...a violation of HIPAA's criminal provisions since the information had been collected from [the patient] because he was a patient."

According to Loitz, the sentencing range would not have been any smaller or larger if Gibson had been charged with identity theft alone, or along with the HIPAA violation. "By charging him with HIPAA," stated Loitz, "we brought attention to the most troubling aspect of the case...that a vulnerable cancer patient was taken advantage of by someone who he had looked to to care for him, not to harm him."

As is true in many federal convictions, Loitz revealed the broader reason for prosecuting under the HIPAA criminal provisions. "We also brought atten-

tion to the HIPAA criminal statute itself," she said. "And perhaps this will raise awareness and help deter future crimes."

Lab directors and pathologists should know that some healthcare attorneys questioned the decision by the **Department of Justice** (DOJ) to prosecute this case of patient identity theft under the HIPAA statutes. They were concerned about whether the DOJ might be shifting its overall approach to considering any individual or entity—whether or not a "covered entity" under HIPAA—as being subject to criminal prosecution.

***Given the facts of the Gibson case, it is reasonable to assume that laboratories and pathology group practices have greater exposure than previously thought.***

Loitz responded to these concerns, stating that the Gibson case was an easy call. "Gibson clearly violated the HIPAA criminal statute" she declared. "He knew what he was doing; he did what he intended to do; he was caught in the act of improperly disclosing the patient information; and so we prosecuted him under HIPAA."

Loitz also made a point of clearing the employer, Seattle Cancer Care Alliance, of any wrongdoing or noncompliance. "The defendant's employer cooperated completely with us in the investigation," stated Loitz. "We did not believe that the employer had culpability for Mr. Gibson's conduct. We did review the patient protection policies and procedures of the employer, and we were satisfied that there was no fault with the employer," added Loitz.

THE DARK REPORT considers Loitz's comments about SCCA to be particularly insightful. It was a healthcare provider which law enforcement authorities and federal investigators considered to be in full compliance with HIPAA mandates and requirements. Yet phlebotomist Richard Gibson was still able to rather easily steal the information needed to successfully commit patient identity theft.

Given the facts of the Gibson case, it is reasonable to assume that laboratories and pathology group practices have greater exposure than previously thought. Obviously, the greatest risk would involve laboratory employees who daily work with sensitive patient information. That would include phlebotomists, data entry people in accessioning, and the coding, billing, and collections staff, among others.

To help laboratory managers and pathologists better gauge the implications of the Gibson identity theft case to their own situation, THE DARK REPORT provides two stories which follow. First is a dual interview with the attorney for SCCA and the privacy director of SCCA. They have advice and insight on how labs and pathology groups can better protect themselves from this type of crime.

## "Everyman" Lab Employee

Second is a profile of Richard Gibson and his actions. He was an "everyman" type of employee who surprised everyone by his crime, since he was not under financial pressure.

THE DARK REPORT recommends that every laboratory and pathology group practice take note of Gibson's conviction under the HIPAA statue. It is timely to reconsider policies and procedures governing access to, and use of, confidential patient information. Your goal should be to take the lessons learned in the Gibson-SCCA case and make it even tougher for employees in your laboratory to commit the crime of patient identity theft. TDR

*Contact Susan Loitz at 206-206-553-4110.*

*—By Pamela Scherer McLeod*

# Privacy Officer Shares Lessons on ID Theft

## *Labs and pathology groups can take proactive steps to increase protection*

***CEO SUMMARY:*** ***"Nothing teaches like experience." That adage aptly describes the lessons learned at a Seattle hospital after a case of patient identity theft surfaced. Laboratories and pathology groups must be just as alert to the potential for patient identity theft as they are to inappropriate disclosures of a patient's health record. It's one of the fastest-growing crimes in the Internet era.***

FOR THE PAST TWO DECADES, laboratories and pathology group practices have concentrated on protecting patient health records. Well-established compliance programs to protect patient privacy are widespread.

Probably the most familiar example is HIV testing. Labs go to great lengths to ensure that only authorized individuals have access to the results of an HIV test.

However, how many laboratories and pathology groups have reviewed their patient privacy policies and procedures in the context of patient identity theft? This a relatively new threat and there's been an explosion in the number of identity theft cases. It is a crime which is relatively easy, carries minimal risk of prosecution (at this time), and can be accomplished by people with few resources.



Identity theft is finding its way into healthcare. THE DARK REPORT predicts that protecting patient information from identity thieves will rapidly become the most important function of patient privacy policies and procedures. If this proves true, then laboratories and pathology group practices will want to be ahead of this trend—not behind it.

To help in this effort, THE DARK REPORT conducted exclusive interviews with two individuals. Julie Hamilton is the Corporate Integrity Officer at **Seattle Cancer Care Alliance** (SCCA). James J. Fredman, III, an attorney with **Foster Pepper & Shefelman**, served as outside counsel for SCCA during the federal investigation into the case of phlebotomist Richard W. Gibson, who committed patient identity theft and was

convicted under the HIPAA statute. *(See pages 2-4 and pages 9-10.)*

With the help of Hamilton and Fredman, lab managers and pathologists will get answers to three basic questions triggered by this landmark case. First, how does law enforcement investigate these types of crimes? Second, why was the decision made to prosecute phlebotomist Gibson under HIPAA, instead of other criminal statutes? Third, what lessons has this hospital learned about improving its defense against patient identity theft?

## Call To Privacy Hotline

Julie Hamilton laid out the story of this case, as it affected SCCA. "In early 2004, a patient telephoned the privacy hotline at SCCA, alleging that he had been the victim of identity theft involving credit cards and a Seattle address," she stated.

In public statements, the patient, who lived in California, has stated that he traveled to Seattle to seek treatment at SCCA for acute lymphoblastic leukemia, an often fatal form of cancer, not often seen in adults. "This patient felt strongly that his critical privacy data had been stolen during his stay in Seattle," recalled Hamilton.

## TV News Broadcast

"Our privacy coordinator here at SCCA returned the patient's call. On his own, the patient was deep in an investigation and provided us with a stack of information," explained Hamilton. "About the time the patient contacted us, he had also caught the attention of a reporter at **KING5 Television**. They were preparing to broadcast a videotape the patient obtained from a local retailer's surveillance tapes. The patient had obtained the cooperation of a retail store that had film of the suspect making a purchase at the cash register with a fraudulent credit card.

"Within minutes of the videotape's broadcast, SCCA fielded calls from individuals who identified the suspect on the tape as one of our employees," Hamilton recalled. "In fact, this tape was aired repeatedly. So we received calls from several people offering useful tips. We turned all that information over to the Seattle police.

"Within the hospital, we immediately investigated the situation," said Hamilton. "We could not find any irregularities or unauthorized access to our multiple computer systems. We also audited scheduling and medical records systems and found nothing."

"When we confirmed that the suspect was one of our employees, actions were taken to terminate the employee for cause," stated Hamilton.

Once it was known that the suspect was Richard W. Gibson, newscasts began to broadcast his name and picture over several days. The suspect, in the company of his attorney, eventually turned himself in to the Seattle Police Department.

"The patient was not happy with the lack of response by the local police," said Hamilton. "The patient informed us that he was contacting other government agencies, such as the FBI. After the FBI contacted us, we worked with them, providing education about our policies and procedures for patient privacy protection.

"To build their case, the FBI needed to know our policies, job functions of various personnel, which staff members have access to patient information, and why they need access to this information. We also took them through our electronic and paper-based systems so they could understand at what point a given employee would see critical identity data," Hamilton noted.

"Throughout this phase of the investigation, we could never pinpoint

how this patient's information was obtained," she added. "Between our internal audits and the FBI's scrutiny, every aspect of our policies, operational practices, and documentation was intensely reviewed.

"In fact, because we could not pinpoint the breach, after the FBI investigation was completed, we hired our own investigator—a retired FBI investigator—to do forensic analysis of our systems and the perpetrator's computer," she continued. "There was no unusual electronic access that we were able to find. Nor did we find evidence that other patient information might have been compromised."

Because the patient had stirred up a large amount of publicity in Seattle about the theft of his identity by a phlebotomist while he was a severely-sick patient in a hospital bed, SCCA took proactive steps to assure its patients about the situation.

"Immediately we posted posters in the lobby which communicated our concerns about protecting patient privacy," said Hamilton. "We also placed extra notices at all front desks regarding our privacy practices.

## Communicating With Staff

"At the same time, we communicated with our staff. They were given 'talking points' to help them discuss privacy concerns with patients and their families," she stated. "Because we had fielded several calls once the story broke on the news, I knew the concerns and questions to which our employees would need to respond."

"Next was the issue of Social Security numbers (SSNs). SCCA does not use SSNs as patient identifiers. We assign unique patient numbers. But SCCA must obtain the SSN for patient safety and billing reasons. So it is in our system, although SSNs do not appear on a lot of paper," emphasized Hamilton

"For example, blood centers use SSNs, so we must use them for patient safety," she continued. "Many insurance companies use SSNs as an identifier, although some are now eliminating that practice.

"To protect SSNs and other critical information, we took additional steps," noted Hamilton. "We are further limiting the number of employees throughout our health system who have access to screens that contain SSNs.

## Blinding The SSN

"One step we've taken is to upgrade our systems to blind the first several numbers of the SSN. For instance, laboratory personnel who only have access to the laboratory system can now see only the last four digits of the number," she said. "We started with our LIS because it was a manageable system with a manager who could immediately implement the upgrade.

"SSNs in our electronic medical record system were also blinded in a similar fashion," she explained. "We continue to upgrade other systems in our hospital with this blinding feature.

"Another change we implemented was to put temporary employees through the same training as permanent employees," stated Hamilton. "In fact, training and awareness on this issue has been increased in all areas of our hospital. Now that a case of patient identity theft has occurred, it's caught everyone's attention. This type of crime is no longer theoretical for our staff. It's real and people are on the alert."

THE DARK REPORT observes that SCCA's experience offers three critical lessons that labs and pathology groups can use to better protect against patient identity theft. First, raise the awareness of staff, patients, and their families through ongoing education. This must include how to protect against patient identity theft and what to do whenever it

# Attorney Stresses Importance Of Effective Compliance Procedures

IN THE **HIPAA CONVICTION** involving patient identify theft by phlebotomist Richard W. Gibson, one individual with a front-row seat was attorney James J. Fredman, III, of Foster, Pepper, & Shefelman in Seattle, Washington.

As outside legal counsel to the Seattle Cancer Care Center (SCCA), Fredman worked with FBI investigators and the U.S. Attorney's Office during the course of the investigation. He gained direct experience in how such agencies work with a provider to resolve these types of crimes.

"We wanted to be as cooperative as possible with the federal investigation," stated Fredman. "Our fundamental argument was that the perpetrator acted outside the scope of his employment when he committed the identity theft," he explained. "Susan Loitz, the Assistant District Attorney who prosecuted the case *(see pages 2-4)* was amenable to our position. One major reason for this outcome was both the tight compliance of SCCA on HIPAA polices and SCCA's cooperation throughout the investigation.

"SCCA is an organization that does as well as any provider can to maintain a high level of compliance," he added. "It was also helpful that the patient victimized by the identity theft testified that, once he alerted SCCA to the crime, it responded appropriately to support him and his efforts to identify the criminal and bring him to justice."

For Fredman, there is one key lesson to add to others identified by Julie Hamilton, Corporate Integrity Officer at SCCA. "It is important for each provider to regularly reassess its risk to these types of crimes on an ongoing basis. It is just as important that these assessments trigger proactive action on the issues identified.

"For SCCA, it was both its solid compliance program and an effective policy of ongoing risk assessment that played an important role in the decision by federal prosecutors to hold neither the institution nor individual managers responsible for the HIPAA violations committed by Gibson.

"That should send a clear message to all healthcare administrators and physicians," offered Fredman. "A provider's best defense in these situations is a well-executed compliance program. This is the best and most effective way to protect the provider and its management team, in the event that a renegade employee commits crimes that violate the HIPAA statute."

is suspected that a case of patient identity theft has occurred.

Second, limit access to SSNs and other sensitive patient information. Blocking some of the nine digits of the SSN on computer screens is one method that can add protection.

Third, in the event of a patient complaint involving possible identity theft, take immediate action and assure the patient that the provider will provide support in response to the situations. When the U.S. Attorney's office evaluated SCCA's compliance program, the fact that the patient said positive things about SCCA's response and support may have been a determinant in the decision to pursue only the suspect as the guilty party. TDR

*Contact Julie Hamilton at 206-288-1000 and James Fredman at 206-447-2909.*

*—By Pamela Scherer McLeod*

# Phlebotomist Gibson Steals Patient's Identity

*It's a warning to labs and path groups: risk of patient ID theft may be increasing*

***CEO SUMMARY:*** ***It was a case of a well-liked lab worker acting in rogue fashion to steal and use the identity of a patient to commit financial fraud. Within laboratories, employees in phlebotomy, accessioning, data entry, coding, billing, and collections often have access to sensitive patient information. In positions with low hourly wages and high turnover, they may, like Gibson, find the temptation to be too much to resist.***

TODAY PHLEBOTOMIST Richard. W. Gibson sits in a federal jail serving a 16-month sentence for patient identity theft. He must also pay no less than $15,000 in restitution.

His crime raises a fundamental question that must be answered by every responsible laboratory and pathology group: "how good is our lab's system and organization at protecting us from a lab employee who intends to commit similar types of fraud and patient identity theft?"

To help answer that question, THE DARK REPORT offers a profile of Gibson, who worked for several years in laboratories around Seattle, both as a phlebotomist and doing processing work in the laboratory.

By his own admission, Gibson stole patient identity information from the hospital where he worked in the laboratory. His employer at that time, the **Seattle Cancer Care Alliance** (SCCA) is a hospital which is part of the **University of Washington Medical Center** in Seattle, Washington.

At the time of his crime Gibson, 42, was a resident of SeaTac, Washington. To patients and co-workers, he was considered polite and good-natured. He was also good enough at his profession, that, in recent years, he taught classes in phlebotomy at a local community college.

## Charged Under HIPAA

Once identified as the suspect in this case of patient identity theft, the **United States Attorney for the Western District of Washington** charged Gibson with "disclosing individually identifiable health information of a patient" receiving treatment at the health care provider at which Gibson was employed, with intent to use that information for personal gain. Specifically, the U.S. Attorney's office cited Gibson's disclosure of the protected information to **AT&T Universal Card** for the purpose of obtaining a credit card for his personal use.

In fact, Gibson used the identity data he had stolen to open credit card accounts in the patient's name with four different companies, including

AT&T Universal Card, **First USA** Visa, **Chase Manhattan Bank**, and **Fleet Credit Card Services**. Using the AT&T card and the First USA Visa card, he ran up $9,139.42 in charges for everything from video games and porcelain figurines to home improvement supplies and Christmas presents for his wife and five children.

Eric Drew, 35, who was undergoing chemotherapy treatment for acute lymphoblastic leukemia, started getting mail from banks and credit card companies in response to new accounts that had been opened. During the next several months, often from his hospital bed and in a weakened state from therapies, Drew investigated this case. Drew's breakthrough came when he caught the attention of a local TV news reporter.

## Suspect Identified

When that television station broadcast a video of Richard Gibson allegedly in the act of using one of the fraudulently obtained credit cards, fellow-employees recognized Gibson and turned him in. Gibson was fired from his job shortly thereafter. A recording was made of Drew making a victim's statement from his hospital bed and was played in court when Richard Gibson was sentenced to 16 months in prison for violating HIPAA (Health Insurance Portability and Accountability Act).

For laboratories and pathology groups, the actions by Gibson, a laboratory employee, to steal a patient's identity and open credit accounts under that name is a warning. At the time he committed this crime, he was not under financial or other pressure. Managers and co-workers had no hint of either his intent nor of his crime.

Lab employees who are paid a low hourly wage in positions that have high turnover are a definite source of risk for patient identify theft. In areas such as phlebotomy, accessioning and data entry, coding, billing, and collections, these type of employees often have access to a patient's personal information. It would be timely for labs and pathology groups to review their exposure to this type of crime. TDR

*—By Pamela Scherer McLeod*

## Patient Eric Drew Battles Cancer & Fraud

IT WAS THE FINANCIAL IDENTITY of patient Eric Drew which was stolen by phlebotomist Richard W. Gibson.

Now 35, Drew, a resident of Los Gatos, California, had been diagnosed with acute lymphoblastic leukemia (ALL). In the fall of 2003, he traveled to the University of Washington Medical Center and the Seattle Cancer Care Alliance (SCCA) to receive advanced treatments for his disease. Drew's disease was treated with advanced molecular therapies and he is familiar with several molecular diagnostic tests.

On the same day in 2003 that Gibson was alleged to have opened a new credit card account with AT&T Universal Card under Eric Drew's name, Drew was posting the following update on his Website, which he used to stay in touch with family and friends and to support fund raising for acute lymphoblastic leukemia (ALL):

"I have had to become an overnight molecular biologist to figure out how I want to get through this. If you are interested, they do these tests (very expensive) to see if my bone marrow has any bad stuff in it. One is called a FISH test where I think they spread out 1,000 cells and look though an infrared computerized microscope that looks inside cells and scans the DNA for abnormalities. Pretty cool technology! The other is an even more sensitive PCR test.I have no clue as to how that one works. I should do some Internet surfing I guess."

## Managed Care Update

# Medicare Managed Care Is Poised to Double in Size

*For local laboratories and pathology groups, this represents both a threat and opportunity*

MEDICARE MANAGED CARE PLANS are poised to double in size. This can be both a threat and an opportunity for regional laboratories.

The **Center for Medicare and Medicaid Services** (CMS) recently reported that it had received 141 applications for new local Medicare Advantage plans for 2005. The applications included 55 HMOs, 73 PPOs, and 13 private fee-for-service plans. At least 51 of the new applications are from insurers that currently offer no Medicare plan.

This is a significant development. If all the applications are approved, it would almost double the number of Medicare managed care plans in operation, from the existing 185 to 326. This is the largest number of plans since 1999. It would also increase the number of states with at least one Medicare Advantage plan from 35 to 39.

### Congress Increases Funding

Medicare Advantage was formerly called Medicare+Choice. The current flood of new plan applications is a direct result of increased funding by Congress in the Medicare Modernization Act of 2003. Congress wants to reverse the decline in the number of Medicare managed care beneficiaries. In 1999, 16%, or 6.3 million, were enrolled in Medicare managed care plans. Currently that number is 11%, or 4.6 million Americans.

For local laboratories and hospital laboratory outreach programs, this development represents both a threat and an opportunity. THE DARK REPORT expects that, as payers establish a new Medicare managed care plan, they will sign an exclusive contract with their existing laboratory provider panel.

### Local Labs Locked Out in FL

THE DARK REPORT has tracked this trend in recent years in Florida, where Medicare managed care has remained active. Lab directors there report that, whenever a new Medicare managed care plan is developed, the payer tends to award that business to its existing lab panel. As fee-for-service Medicare patients enroll in these managed care plans, local labs and pathology groups not on the panel lose access to those patients.

Balancing the threat of loss of access to existing Medicare fee-for-service patients is the opportunity for strong local labs and hospital lab outreach programs to negotiate a contract to provide lab testing services for the new Medicare managed care plans. To accomplish this, such labs must identify health insurers in their area which are in the process of establishing such plans and begin building a business relationship.

Finally, local anatomic pathology groups have risk. With the national labs aggressively pursuing AP specimens, it is likely they will want to keep the AP specimens generated in Medicare Advantage plans and not contract this work to local pathology groups. TDR

# OIG May Be Investigating AP Laboratory Condos

*First evidence of an active OIG investigation has begun surfacing in the marketplace*

***CEO SUMMARY: Attorneys for one of the companies which sells and manages anatomic pathology condominium laboratories have recently sent correspondence to owners of these lab condos. This correspondence discloses that the Office of the Inspector General (OIG) is examining the company. Knowledge of this situation is only now surfacing and few other details have become public.***

DURING THE PAST TWO WEEKS, rumors about an investigation by the **Office of the Inspector General** (OIG) into at least one of the anatomic pathology laboratory condominium companies have been confirmed by THE DARK REPORT.

**Vincent & Elkins**, the law firm which represents **UroPath, LLC** has sent notification to owners of anatomic pathology (AP) laboratory condominiums managed by UroPath that the OIG is now looking at the company. Presumably the OIG is studying UroPath's business model, its contracts and documentation, and its operational practices.

## UroPath Is In FL and TX

UroPath is known to operate AP lab condo complexes in Leesburg, Florida and San Antonio, Texas. Another complex has been under construction in or around Dallas, Texas. Each pathology laboratory condominium is owned by a different urology, gastroenterology, or dermatology group.

Individuals who have either seen copies of this correspondence or have spoken to owners of AP lab condos confirmed this situation. These individuals say that the correspondence between UroPath's legal counsel and AP condo lab owners acknowledges that the OIG is looking into UroPath.

Further, these individuals say that the law firm is putting the best spin possible on this situation. The correspondence declares that the law firm "welcomes" this examination by the OIG because it is an opportunity to demonstrate that their business model and the operation of anatomic pathology laboratory condominiums meets appropriate regulations and laws.

It must be pointed out that this law firm did the original legal review of UroPath's business model. It has advised the company since its early days. Thus, any negative outcomes from the OIG's look into UroPath will reflect badly on this law firm.

Veteran laboratory executives and pathologists will consider the OIG's interest in UroPath's AP lab condo business to be much more serious. That's because a large number of labo-

ratories faced similar inquiries by the OIG during the past 20 years. They know the OIG does not come knocking just to do a little fishing.

To the contrary, the OIG is rather stingy with its time because it has limited resources. From this perspective, its interest in looking into UroPath portends more serious developments for UroPath and its anatomic pathology laboratory condominum owners.

## Attracted OIG's Attention

After all, during the past 12 months, several events have demonstrated that the federal government has taken notice of AP laboratory condos. First was the public statement last spring by a senior OIG official acknowledging its awareness of such a business model.

Next, in the fall, the OIG issued Advisory Opinion 04-17 addressing one specific proposed business model for AP laboratory condominiums and provided an unfavorable opinion on the scheme. The OIG also declared that its 2005 Work Plan would include a review of "pathology services performed in physician's offices...We will review the relationships between physicians who furnish pathology services in their offices and outside pathology companies." *(See TDR, November 1, 2004.)*

## Just The First Step

Now, only four months later, the OIG is actively reviewing such arrangements at UroPath. Based on how the OIG has investigated other laboratory testing service situations in the past, there is every reason to believe that the OIG intends to act upon whatever it finds.

THE DARK REPORT would like to offer some speculation. Over the past 20 years, a substantial area of enforcement action against laboratories was centered around over-utilization of laboratory tests. It is known that some promoters of these AP lab condo complexes did build their financial pro formas using the assumption of 100% utilization of 12-core prostate biopsies. *(See TDR, August 9, 2004.)*

As most lab executives know, CMS now has sophisticated software capability that can analyze laboratory testing patterns by lab test, by laboratory, by physician, and by several other factors. Since a number of these AP laboratory condominiums have now operated for between 12 and 24 months, it may be that the OIG has analyzed the test ordering patterns of specialist physician groups which currently operate an AP laboratory condominium.

## Before & After Utilization

Using this capability, it would not be difficult to look, by provider number, at utilization patterns of the anatomic pathology procedures ordered by physicians and groups before they owned their own AP laboratory condominium and after it came into operation. If this is true, let's return to the specific example of prostate biopsies.

If the OIG possessed data which showed increased utilization after the group or physician became owner of an AP laboratory condo, and if there was no relevant change in that physician's patient mix to justify the greater number of biopsies, then that medical group and/or physician would definitely catch the interest of the OIG.

THE DARK REPORT is first to alert the laboratory profession to what may be the early steps in a major enforcement effort by the OIG. It would be timely for pathologists to educate those physicians who persistently ask to share, through some arrangement, in the pathology technical or professional fees generated by their patient referrals. If past history is relevant, these types of arrangements—whether or not they were ever acceptable—are fast becoming compliance deathtraps for the unwary! TDR

# Labs in United Kingdom Pressured to Change

## *Healthcare trends push labs to better serve primary care, emergency, and POC*

***CEO SUMMARY: Across the United Kingdom, the physical layout, instrumentation, and operation of laboratories is very close to that of laboratories in the United States and Canada. The source of most differences is how the healthcare system in the United Kingdom funds clinical services and sets priorities. The latest National Health Service initiative is to have selected pharmacies collect specimens and perform lab tests.***

**By Robert L. Michel**

SITE VISITS TO LABORATORIES in the United Kingdom last month provided insights into how U.K. laboratories are responding to pressures to improve the support they provide to primary care clinics, emergency departments, and point of care testing sites.

Of particular interest to laboratory administrators and pathologists will be the news that the **National Health Service** (NHS) is launching a major pilot project to collect specimens and perform laboratory testing in pharmacies. This seems to reinforce similar initiatives in the United States and is a trend which should be watched.

THE DARK REPORT was in England to co-produce and participate in the third annual *Frontiers in Laboratory Medicine* (FiLM) conference. Held in Birmingham, England on February 1-2, 2005, it brings together laboratory directors and pathologists to share innovations in laboratory and pathology management.

Following the FiLM program, we had time to journey to London and visit two laboratories. The first site visit was to the laboratory at **North Middlesex University Hospital** (NMUH). Located in suburbs in the Northern London metropolitan area, this hospital services primarily a working-class and immigrant population. NMUH's Laboratory Manager, David Ricketts, will be at this year's *Executive War College* in New Orleans on May 3-4, 2005 to present a case study.

### Site Visits to Two Labs

The second site visit was to **The Doctor's Laboratory**. This is one of only two privately-owned laboratory companies in the United Kingdom. It is located in the center of London.

One notable aspect of The Doctor's Laboratory (TDL) is that it has a lab joint venture with a prestigious academic center hospital. **University College London Hospital** and TDR recently built an automated laboratory. It had just opened in January 2005, so our site visit came just weeks after it became operational.

There is not much difference in the physical layout and instrumentation of laboratories in the U.K. from those in the United States and Canada. One point of differentiation is that the software products used in the laboratory are mostly from European vendors.

One major difference is the transportation challenges in a metropolitan area like London and the surrounding countryside. It takes a prohibitive amount of time to move specimens by surface vehicles. For this reason, hospitals in each neighborhood are the primary source of laboratory testing for primary care clinics nearby. Specialists tend to practice within hospitals, so their specimens are testing within the hospital lab.

## Reference/Esoteric Labs

During the site visits, I asked questions about how reference and esoteric testing is handled in the United Kingdom. In particular, I asked when new assays would become available and how it was decided which laboratory would provide that testing for the country.

It turns out that the United Kingdom doesn't have well-established sources for new esoteric and reference assays. Instead, if a pathologist in one laboratory has a clinical interest in an assay and begins to run it for the benefit of his hospital and physician staff, news that this test is available at this site gets out to other hospital laboratories.

They can then refer specimens to that laboratory. A transfer price is established and paid by the referring laboratory. In the United Kingdom, regional health trusts establish budgets for each clinical service, like laboratory testing. So it is up to the referring laboratory to make decisions on how much testing to refer to outside laboratories.

There is another consequence to this arrangement. In the United States, many laboratory companies concentrate on developing new assays, educating clinicians about the benefits, and then performing the tests as specimens are referred to their laboratory.

In the United Kingdom, there are many fewer of these "home brew" tests. There are no comparable testing centers to match **ARUP Laboratories**, **Mayo Medical Laboratories**, and their peers here in the United States.

## Lab Tests In Pharmacies

The demonstration project to put specimen collection and laboratory testing into pharmacies will take place in Manchester, England. Several large pharmacies in Manchester are currently being remodeled to accommodate these services.

The objective behind this project is two-fold. First, the NHS believes it will lead to more efficient delivery of care (read: save money). Second, NHS is responding to patient dissatisfaction about waiting times and poor service within the healthcare system.

In-pharmacy laboratory testing will be designed to allow the patient to accomplish two things on a single visit. In one location, a specimen can be collected and the lab test done on-site. When the results are available, the pharmacist can then adjust the prescription as appropriate.

## Integrated Patient Record

One of the requirements to make this type of arrangement successful is an integrated patient record. The lab results most post into that patient's record and the pharmacist must similarly update the file so the attending physician knows both the test results and any change in the patient's prescription.

The interest in performing lab tests within a pharmacy is something I consider significant. Every year, I see more examples in the United States of specimen collection and laboratory testing being done within pharmacies. TDR

*Contact Robert Michel at 512-264-7103.*

Dark Index

# Year-end Financials Released For Quest, LabCorp & LabOne

*It's a stable marketplace, as major public labs report modest growth in revenues and earnings*

In RECENT WEEKS, public laboratory companies have released earnings reports for the year-ending December 31, 2004.

It was generally a good year for the three largest lab companies that have a major emphasis on providing lab testing services to office-based physicians. In this year's review, THE DARK REPORT looks at **Quest Diagnostics Incorporated**, **Laboratory Corporation of America**, and **Lab*One*, Inc.**

At Quest Diagnostics, full-year revenues climbed by 8.2%, to $5.1 billion in 2004 compared to $4.7 billion in 2003. **Unilab**, acquired by Quest Diagnostics on February 28, 2003, generated 1.5% of this growth.

Net income for 2004 was $507.1 million compared to $436.7 million in 2003. This was growth of 16.2%. During 2004, Quest Diagnostics spent $735 million to repurchase 8.3 million common shares.

## Fourth Quarter Growth

During fourth quarter 2004, Quest Diagnostics reported revenue growth of 6.6% over fourth quarter 2003. It attributed specimen volume growth to be 4.1% of this total and growth in revenue per accession to be 1.9%. The balance of revenue growth came from non-clinical testing business.

LabCorp reported full-year 2004 revenues of $3.1 billion. This was a 4.9% increase over 2003's revenues of $2.9 billion. Net earnings at LabCorp for 2004 were $363 million, representing growth of 13.1% over the $321 million the company earned during 2003.

LabCorp stated that the 4.9% growth in revenue was comprised of 3.6% increase in specimen volume and 1.3% from an increase in the average price per accession.

Similar to Quest Diagnostics, LabCorp repurchased shares during the year. It spent $378 million to repurchase 8.8 million shares during 2004.

## Stable Lab Marketplace

The financial performance reported by both Quest Diagnostics and LabCorp is evidence that the laboratory testing marketplace has been fairly stable during the past 24 months. Up through 2002, both lab companies grew rapidly, primarily because they regularly acquired laboratories.

However, by the end of 2002, the two blood brothers had acquired most of the publicly-traded laboratory companies which were the easiest acquisition opportunities. During 2003 and 2004, both companies have had no "easy" options to boost specimen volume and revenue. It has required them to focus on improvement to operations (internal) and better execution of their national sales and marketing programs (external).

Fast-growing Lab*One* has a different story relative to its larger peers. Lab*One*'s revenue comes from testing activities in "risk assessment services" (life insurance testing), healthcare (clinical testing provided to office-based physicians), and substance abuse testing.

## 35% Growth In Revenues

For full-year 2004, Lab*One* reported revenues of $468.2 million, a growth of 35% from its 2003 revenues of $346.0 million. Lab*One* notes that $69.5 million of this growth during 2004 came from its acquisitions of **Alliance Laboratory Services, Inc.** in Cincinnati, Ohio and **Northwest Toxicology**, located in Salt Lake City, Utah. *(See TDR, February 23, 2004.)*

In each of its testing segments, Lab*One* reported the following growth rates during 2004: risk assessment services–$261.1 million (13%); healthcare–$166.7 million (88%); and, substance abuse–$40.4 million (51%).

As a point of comparison, revenues from testing provided to office-based physicians at LabOne was $166.7 million. At **Bio-Reference Laboratories, Inc.** (BRLI), based in Elmwood Park, New Jersey, revenues for its fiscal year ending October 31, 2004 were $136.2 million.

## Second And Third Largest

Lab*One* and BRLI are the second-largest and third-largest public laboratory companies in the United States, as measured by revenues generated from testing provided to office-based physicians. Lab*One* reports larger revenue totals than BRLI because of its involvement in providing testing to the life insurance industry and its drugs-of-abuse business.

However, BRLI has posted steady and substantial rates of growth over the last four years. It may overtake Lab*One*'s clinical testing business sometime in the the next 18 to 24 months.

## AmeriPath Reports 2004 Financials

**In the first full year following** its acquisition by **Welsh Carson Anderson & Stowe**, **AmeriPath, Inc.** is showing modest growth in revenues and specimen volumes.

Now with headquarters in Palm Beach Gardens, Florida, AmeriPath posted total net revenues of $507.3 million for full year 2004. This contrasts with 2003 revenues of $485.0 and is an increase of 4.6%. Its EBITDA (earnings before interest, taxes, depreciation and amortization) for 2004 was $67.8 million, representing little change from its 2003 EBITDA of $66.5 million.

AmeriPath attributes its increased costs as "primarily due to increases in physician compensation both from adjustments to existing contracts and from additional physicians added in select specialties, and from increased courier and distribution costs associated with the increased revenues from physicians' offices."

Across the pathology profession, it has been consistently speculated that AmeriPath's original "employment model," used to acquire its constituent pathology group practices, would trigger the need to pay increased salaries in downstream years. That would be particularly true as the older pathologists in a group which sold itself to Ameripath retire. Replacing these experienced hands would require more aggressive compensation to attract new pathologists.

For lab administrators and pathologists competing against these public laboratory companies, one conclusion stands out: overall, these companies are in good financial health and are generating adequate margins on their testing business.

This should encourage hospital laboratory outreach programs seeking to expand. The market environment is favorable and professionally-managed and marketed outreach programs should enjoy success. TDR

# INTELLIGENCE

## LATE & LATENT

*Items too late to print, too early to report*

For lab managers and pathologists tracking the growth of e-commerce, here's a revealing statistic. The **Federal Reserve Bank** released numbers showing that 2003 was the first year where the number of electronic payment transactions exceeded the number of transactions paid by check. During 2003, there were 44.5 billion electronic payment transactions compared to 36.7 billion checks. "It's all about convenience," noted Richard Yamarone, an economist at **Argus Research**. "No longer do consumers want to write checks with two forms of identification. It's too cumbersome. It's much easier to swipe and sign." Changing consumer expectations will mean that labs should be preparing to handle electronic payment transactions.

### AEL'S NEW EXECUTIVE

**American Esoteric Laboratories, Inc.** (AEL) announced on March 21, 2005 that it had hired Chuck Locke to be its Vice President, Development and Administration. Locke had been the Vice President of Operations for **MDS Diagnostics Services**.

### SEVEN MEDICAL GROUPS IN WASHINGTON POST PERFORMANCE INFO ON INTERNET

It's been a standing prediction of THE DARK REPORT now for several years: performance data on providers will be posted where it can be accessed by the public. Seven big medical groups in the state of Washington are in their fourth month of doing exactly that. These seven medical groups are posting data in 12 clinical performance categories and five measurement areas of their patient-satisfaction survey scores. This information is maintained and updated on the Web site of **Premera Blue Cross**. It includes graphs and side-by-side comparisons of all the groups together. The graphs also show statewide averages developed from aggregated data of other, unnamed providers in the state of Washington.

### ADD TO: *Provider Performance Data*

The participants include **Rockwood Clinic** (Spokane), **Wenatchee Valley Medical Center** (Wenatchee), **Everett Clinic** (Everett), **Virginia Mason Medical Center** (Seattle), **Pacific Medical Centers** (Seattle), and **PolyClinic** (Seattle). "What a gutsy move by these clinics," observed Dave Johnson, M.D., Medical Director at Premera. Over a three-year period, Johnson helped these medical groups develop their public "report card." In some cases, there is significant variation in the data. For example, in child wellness visits, there is up to a 21% spread between the highest and lowest performance among the seven medical groups. Over time, THE DARK REPORT predicts that laboratories and pathology groups will be included in similar types of rankings.

### WHERE ARE THEY NOW?

• Ever wonder what happened to the lab industry's self-defined "Rhino" and "Sherpa"? The irrepressible Doug Jaciow, who left **Bay State Healthcare** in Springfield, Massachusetts after several decades of service in its laboratory division, can now be found at **Microtest Laboratories, Inc.**, based in Agwam, Massachusetts. He is a Vice President at Microtest.

***That's all the insider intelligence for this report. Look for the next briefing on Monday, April 18, 2005.***

*PREVIEW #5*

## EXECUTIVE WAR COLLEGE

May 3-4, 2005 • Astor Crowne Plaza Hotel • New Orleans

### Learning About Lean from a Master

In a reprise presentation, Mark Jamrog, President of SMC Management Group, will update new and exciting developments in Lean quality management systems. Jamrog's experience is considerable. In addition to his substantial experience in industries such as aerospace and automobiles, Jamrog has also helped such healthcare corporations as Johnson & Johnson develop and implement corporate-wide Lean initiatives. Jamrog will show how Lean techniques are helping "turbocharge" clinical laboratory operations in a growing number of laboratories across the United States.

***Full program details available now!***
*visit darkreport.com*

# UPCOMING...

- ***Assessing Clinical Differences in Molecular Versus Existing Methods: How Lower Specificity Riles Clinicians.***
- ***Exclusive Interview: Patient Eric Drew Details His Experience with Patient ID Theft, and How Authorities Didn't Respond.***
- ***Pathologists Gain Legislative Wins at the State Level.***

*For more information, visit:*
**www.darkreport.com**