G2 Compliance Report

G2 INTELLIGENCE

For Hospitals, Laboratories and Physician Practices

Kimberly Scott, Managing Editor, kscott@G2Intelligence.com

Issue 11-04 • April 2011

Inside this issue

www.G2Intelligence.com

Washington G-2 Reports is now G2 Intelligence!

You may notice a new look, but the quality content hasn't changed. Our new name reflects our renewed commitment to research and advancing the business of diagnostic medicine. You can still count on thorough coverage of the lab industry and premium analytical content.

Be sure to check out our new Web site: www.G2Intelligence.com.

Feds Crack Down on Medicare Fraud, Arrest 111 in Largest Ever Health Care Sweep

In what was billed as "the largest ever federal health care fraud takedown," the Medicare Fraud Task Force in February brought criminal charges against 111 doctors, nurses, and health care executives in nine cities.

The defendants are accused of various health care fraud-related crimes, including conspiracy to defraud the Medicare program, criminal false claims, violations of the anti-kickback statute, money laundering, and aggravated identify theft. Collectively, the defendants are accused of cheating the government out of a total of $225 million.

The sweep of arrests was so massive that it took more than 700 agents from the FBI and the Department of Health and Human Services to round up the suspects, plus serve another 16 search warrants around the country in connection with ongoing strike force investigations.

"With this nationwide takedown and the expansion of the strike force to two additional cities, our message is clear: we are determined to

Continued on page 2

HIPAA Fine, Settlement Highlight Importance Of Comprehensive Privacy Policies

Two recent penalties resulting from violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy rule, resulting in a $4.3 million fine and a $1 million settlement agreement, underscore the importance of health care providers—including clinical laboratory and pathology groups—having carefully crafted privacy policies in place.

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) on Feb. 22 imposed its first-ever civil monetary penalty on a covered entity for violating the nearly eight-year-old privacy rule of HIPAA, ordering Cignet Health of Prince George's County, Md., to pay $4.3 million.

The bulk of the penalty—$3 million—was assessed for Cignet's failure to cooperate with HHS's investigation, a move that attorneys say signals that the agency is serious about exercising its expanded enforcement authority under the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Continued on page 9

Feds Crack Down on Medicare Fraud, *from page 1*

put Medicare fraudsters out of business," said Assistant Attorney General Lanny Breuer of the Department of Justice's criminal division.

Since their inception in March 2007, strike force operations in nine districts have charged more than 990 individuals who collectively have falsely billed the Medicare program for more than $2.3 billion, with nearly 750 of them already convicted in court. In addition, in 2010 alone the joint federal, state, and local task force recovered another $4 billion in fines and other restitution payments on behalf of taxpayers that had been lost to corruption.

Five defendants were charged in Los Angeles for their role in schemes to defraud Medicare of more than $28 million in false claims for durable medical equipment and home health care. In Baton Rouge, six individuals were charged for a durable medical equipment fraud scheme involving more than $9 million in false claims. In Chicago, charges were filed against 11 people associated with businesses that have billed Medicare more than $6 million for home health, diagnostic testing, and prescription drugs. G2

Administration Proposes Nearly Doubling Fraud and Abuse Program Funds for FY 2012

President Obama's Feb. 14 proposed budget for fiscal year 2012 includes $581 million in discretionary spending for the Health Care Fraud and Abuse Control (HCFAC) account, nearly doubling the $311 million contained in the annualized continuing resolution for FY 2011 and more than doubling the $259 million spent in FY 2010.

The administration had proposed $561 million in FY 2011 discretionary spending for the HCFAC program, which coordinates law enforcement activity related to health care fraud and abuse on the federal, state, and local levels, but Congress never enacted a budget. Congress instead passed a continuing resolution funding the government for FY 2011.

The increased fraud and abuse spending would lead to numerous savings, Health and Human Services (HHS) Secretary Kathleen Sebelius said during a Feb. 14 press conference, including efficiencies resulting from expanding the Medicare Fraud Strike Force program from seven cities to 20.

Overall, HCFAC spending would result in $10.3 billion in savings over the next 10 years, based on Centers for Medicare and Medicaid Services' (CMS) conservative projections that every dollar spent to prevent fraud and abuse saves $1.50.

Louis Saccoccio, executive director of the National Health Care Anti-Fraud Association, said "the increase in funding proposed is necessary not only to fund the expansion of the strike forces, but just as important is necessary to fund the deployment of the technology needed to prevent and detect fraud before payments are made. The return on investment for anti-fraud initiatives is significant, and therefore the increase in funding for these initiatives is consistent with Congress's focus on reducing government spending."

New Policy Proposals

The FY 2012 budget also proposed several policy measures designed to protect the federal health care programs from fraud, including requiring state Medicaid agencies to track and monitor prescription drug billing and utilization so as to detect any patterns of fraud and abuse.

Additional policy proposals include implementing fraud and abuse measures contained in the Patient Protection and Affordable Care Act, such as enhancing provider screening, improving data analysis, and mandating the inclusion of a National Provider Identifier on all provider enrollment forms for federal health care programs.

Out of the total proposed discretionary HCFAC spending, $390 million would be spent on program integrity initiatives for CMS, $98 million would fund fraud and abuse activities within the HHS Office of Inspector General, and $93 million would be allocated to the DOJ for fraud-related programs.

The discretionary spending is in addition to mandatory HCFAC spending, which would include $851 million for Medicare integrity programs, $130 million for Federal Bureau of Investigation fraud and abuse control, $291 million for other fraud and abuse control programs, and $22 million for predictive modeling technology. Combined mandatory and discretionary HCFAC spending for FY 2012 would total $1.9 billion, compared with $1.4 billion for FY 2010 and $1.6 billion for the FY 2011 continuing resolution.

The FY 2012 budget proposal for HHS is available at *www.gpo.gov/fdsys/pkg/BUDGET-2012-APP/pdf/BUDGET-2012-APP-1-11.pdf.*

Data Analysis Technology Can Detect Fraud Before Payments, CMS Official Says

A data analytics system soon to be implemented by the Centers for Medicare and Medicaid Services (CMS) would assign risk-based scores to Medicare transactions, enabling fraudulent patterns and trends to be detected before any payments are made, a CMS official said at a Feb. 15 Senate subcommittee hearing.

"Innovative risk-scoring technology applies a combination of behavioral analyses, network analyses, and predictive analyses that are proven to effectively identify complex patterns of fraud and improper claims and billing schemes," Peter Budetti, deputy administrator and director of CMS's Center for Program Integrity, said in testimony during the Senate Appropriations Subcommittee on Labor, Health and Human Services, Education, and Related Agencies hearing.

Budetti said that it was necessary to take in a wide range of data to generate each risk score, such as claims data, complaints to the Medicare hot line, and law enforcement information. Before implementation, he said CMS would thoroughly test the technology to ensure it provided a low rate of false positives and did not disrupt legitimate providers.

The hearing follows the announcement in late 2010 that CMS will significantly expand the use of predictive modeling tools to prevent fraudulent health care payments.

"This is new for us, and we're currently implementing it," Budetti said. "This approach is night and day from 10 years ago."

CMS issued a request for information in December 2010, asking vendors to provide information on their abilities to provide data integration technology.

Testimony from the hearing is available at *http://appropriations.senate.gov/ht-labor.cfm?method=hearings.default.*

N.Y. Gives Labs Amnesty Period To Unwind or Fix EHR Donation Agreements

The prohibition does apply to pathology groups holding a clinical laboratory permit. However, pathologists on staff at a general hospital or who contract with a general hospital to provide pathology services under the hospital's permit would be allowed to accept "computer services" from the hospital, including connectivity to a location off-site of the hospital.

The New York Department of Health (DOH) will give labs operating in the state until April 15, 2011, to unwind electronic health record (EHR) donation contracts or make other arrangements to ensure compliance with the state's ban on donations to referring physicians.

The DOH announced the amnesty period in mid-February in a frequently asked questions document distributed to laboratories. The FAQs follow a Sept. 27, 2010, letter stating that labs are prohibited from donating all or a portion of the cost of EHRs (even though federal law allows labs to donate or cost-share up to 85 percent of the cost of EHR software).

To minimize disruption of ongoing arrangements, DOH has set an amnesty period of 90 days (Jan. 15, 2011, to April 15, 2011) during which labs that have donated costs of EHRs to New York state clients may (1) take back the software and discontinue prohibited services (i.e., unwind contracts), (2) arrange for the one-time sale of donated software and EHR components to the referral source at fair market value and discontinue payment for the prohibited services and connectivity, or (3) leave donated software of EHR components in place and continue to pay for connectivity for the nonlaboratory components of the EHR, and discontinue accepting specimens for testing from the referral source. A laboratory must maintain documentation of the chosen corrective action and make it available to the department upon request.

The DOH will not set fair market value (FMV) thresholds and says FMV should be determined by the lab, possibly in consultation with the EHR manufacturer. After April 15, 2011, labs found to be in violation of the New York state rules on electronic medical records systems as communicated in the Sept. 27 letter can be referred for civil or criminal penalties and administrative action.

Among other questions addressed by the Department of Health:

Q. What are the implications, including false claim risks, for laboratories enrolled in the NYS Medical Assistance Program (Medicaid) whose EHR donation programs are compliant under federal anti-kickback safe harbors but may not satisfy the NYS requirement?

A. A laboratory's operations in NYS must comply with NYS rules, even if that laboratory participates in federal or federally supported programs (i.e., Medicare and Medicaid, respectively). Any suspect arrangements, including concern for false claims, will be referred to the NYS Office of the Medicaid Inspector General (OMIG), which may conduct its own investigation and impose sanctions.

Q. May a laboratory pay a third-party vendor for charges involved in sending reports from a laboratory information system to the practice's EHR (i.e., a referral source)?

A. A laboratory may not pay an EHR vendor a "per click" charge for transmitting test orders or reports whenever the laboratory has already incurred the expense of establishing the interface that makes possible the electronic transmission of orders and reports from and to a referring practitioner. Similarly, the laboratory may not pay "per physician" usage charges (as a separate cost or a cost component of a maintenance fee) as this is a cost that should be borne by the practice, which makes the decision on how many physicians have log-in privileges. A laboratory may, however, pay such charges to its own IT/LIS vendors who have no contractual relationship with either the EHR vendor or the referring provider even though the results of their work go to an EHR.

G2 INTELLIGENCE

COMPLIANCE PERSPECTIVES

David Gee is a health care attorney in the Seattle office of Garvey Schubert Barer. He represents laboratories across the country. Prior to joining Garvey Schubert Barer, he served as in-house legal counsel to Quest Diagnostics, Unilab, LabCorp, and National Health Laboratories.

Minimizing Risk in Lab Sales and Marketing

Without a strong engine the train won't leave the station; without working brakes the train won't stay on the tracks. Likewise, without a strong sales force, clinical laboratories won't succeed in their highly competitive marketplace, but without the understanding and commitment of the sales team to compliance in this highly regulated industry, otherwise successful laboratories can go off the rails.

It is significant that nearly all laboratory settlements in the last two decades resulted from a combination of billing and *sales* practices. With the federal government stepping up enforcement, there has never been a better time for clinical laboratories to review their sales practices to assure they have airtight compliance policies and practices in this high-risk area. Not only do new laws make a compliance program mandatory, but the Department of Health and Human Services Office of Inspector General (OIG) recently has stressed that it is "pursuing those individuals who solicit kickbacks, in addition to the payers of kickbacks." Specifically, OIG may exclude and impose a civil monetary penalty of $50,000 for each kickback, plus three times the amount of each kickback against any individual or entity that engages in kickbacks. (OIG Secretary Levinson, April 2010, *http://oig.hhs.gov/testimony/docs/2010/HCCAIGKeynoteSummary.pdf*).

To assist labs to stay safely on the rails, attached is a sample of the type of compliance checklist I have used (in various forms) with many clients throughout the past two decades to monitor and assess their sales policies and practices, and to provide specialized compliance training to lab sales personnel.

SAMPLE: SALES AND MARKETING PRACTICES RISK ASSESSMENT

This SAMPLE SALES AND MARKETING PRACTICES RISK ASSESSMENT is provided for educational purposes only. It is not comprehensive and does not constitute and should not be substituted for legal advice. Parties affected by the issues discussed herein should consult qualified legal counsel—the specific facts of any situation greatly influence the legal advice given. In addition, this sample addresses a volatile area of law that may have significant changes in the future that alter the applicability of this sample.

This sample is focused on compliance with federal laws and guidance. This sample does not address state and local laws and guidelines, which may vary significantly by jurisdiction.

ASSESSMENT AREA	✓	COMMENTS
1. All sales and marketing and client-services personnel (including managers and supervisors) receive lab's compliance plan and relevant compliance policies. All sales and marketing and client-services personnel receive initial and regular compliance training focused on sales and marketing practices. These measures are formally documented. **Documents: Signed acknowledgement of receipt of plans, policies, training.**		Compliance training should stress personal accountability and potential personal and company liability. Compliance should be a performance measure.
2. All sales representatives are employees of lab. (But if there are contract sales personnel, none are paid percent-of-sales compensation.) **Documents: Sales employment/contractor records.**		OIG has concern with percentage-based compensation for contractor marketing. See, OIG Advisory Opinions 98-1 and 99-3.

ASSESSMENT AREA	✓	COMMENTS
3. Any equipment provided to clients meets the following: A. The type of equipment provided is consistent with lab policy. B. Equipment tagged as lab property. C. Prior to placement, client signs agreement to use equipment solely for testing sent to lab. D. Lab maintains inventory and mechanism to track equipment placed. E. Equipment retrieved when testing with lab is terminated. F. Equipment unrelated to lab testing provided at fair market value (FMV) (not adjusted to reflect value of referrals). **Documents: Written Policy. Copies of logs, tracking mechanisms.**		1994 OIG Lab Fraud Alert
4. Computers/fax machines provided to clients dedicated and restricted to performance of lab testing. Each client receiving a lab computer has signed approved written agreement before placing equipment. Use monitored **Documents: Signed agreement. Monitoring policy and records.**		1994 Fraud Alert
5. If lab donates EHR software to referral sources: A. Lab does not donate EHR hardware (or informational technology and training services related to EHR hardware). B. Lab does not require referral sources who receive donated EHR software to refer patients. C. Lab's donation of EHR software to referral sources is not based upon volume or value of referrals. D. EHR software is "necessary" for referral sources to create, maintain, or receive EHR. Referral sources do not already possess equivalent software/services. E. Donated EHR software is used by referral source predominantly to create, maintain, or receive EHR. F. Donated EHR software is interoperable to (1) communicate and exchange EHR data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks, in various settings, and (2) exchange EHR data so that the clinical or operational purpose and meaning of the data are preserved without alteration. G. Lab pays vendor of the EHR software directly for EHR software. H. Referral sources receiving donated EHR software have reimbursed lab or software vendor for 15 percent of the EHR software cost upon or before receipt of software. Lab does not loan or finance the 15 percent cost to referral source. **Documents: Written Policy. Written authorization; documentation that software meets each requirement.**		Current Stark law exception and AKS Safe Harbor cease 12/31/13.
6. Lab has policy to identify types and amounts of supplies that may be provided to clients, an approval process, and mechanism in place to monitor amount and type of supplies provided. Types and amounts are compared against what is typically needed to submit testing to Lab. **Documents: Written Policy. Records of supplies provided to each client. Procedures used to monitor volume, type of supplies provided. Sample of documents (i.e., print screens, computer reports).**		CMS has stated that labs should not provide expensive items—or surgical gloves or other items readily usable for nonlab purposes. 66 Fed. Reg. 856, 948 (Jan. 4, 2001). CMS recently clarified that provision to physicians of single-use speculums constitutes a "compensation arrangement" under the Stark law (CMS-AO-2010-01).
7. Courier services limited to transporting lab's test orders, reports, supplies, etc. Signed written agreement of at least one-year term at FMV rates for each client receiving courier services unrelated to lab's testing; with services billed to and paid by client. **Documents: Written Policy. List of clients receiving courier services unrelated to lab testing. For each client, documentation of FMV, invoices/payment records.**		

ASSESSMENT AREA	✓	COMMENTS
8. Free pick-up, disposal of biohazardous waste strictly limited to waste resulting from lab specimen collection and processing; performed only through licensed waste carriers. **Documents: Written Policy. Waste contractor manifests.**		1994 Fraud Alert
9. Duties of lab phlebotomists within physician offices (where permitted by state law) strictly limited to specimen collection for lab services. Phlebotomists receive initial and periodic compliance training on this requirement. Sales and client service personnel and phlebotomy supervisor monitor compliance. **Documents: Written Policy. Signed acknowledgement of receipt of policies/training. Monitoring documentation**.		1994 Fraud Alert. Recommend signed agreement with phlebotomist and with client to confirm.
10. Draw station leases with clients meet state and federal requirements, including: A. Written lease for a minimum term of one year; signed by both parties before rental begins. B. Rent is set in advance and is consistent with FMV—OIG says not more than pass-thru rent for sublease. C. Lease is commercially reasonable without taking into account volume or value of the referrals between the parties. D. Lab has exclusive use of dedicated space. E. Shared space accurately measured and documented in accordance with 2000 OIG Special Fraud Alert formula. F. Renewal terms carefully followed. G. Each requirement carefully documented and monitored. **Documents: Written Policy. Signed lease, currently in effect. Documentation of FMV, shared space measurements, and calculations; commercial reasonableness; monitoring.**		Stark law; anti-kickback statute
11. Provision of ICD-9 codes to clients informational only; not instructional. Physician maintains complete freedom of choice in selection of ICD-9 codes. A. ICD-9 codes obtained only from ordering client or his or her authorized representative. B. Narrative diagnostic statements are translated to ICD-9 code only by trained billing employees. C. Use of ICD-9 codes from earlier dates of service is prohibited. D. If marketing personnel contacts the client for ICD-9 information, the date, information/code obtained, name of the person providing the information, and name of marketing employee who obtained it are documented. E. Marketing department refrains from supplying clients with or requesting clients to provide reimbursable diagnosis codes. **Documents: Written Policy. Requisitions; script pads. Any documents provided by lab to clients re ICD-9 codes and medical necessity.**		OIG Compliance Program Guidance
12. Old requisition forms removed from use whenever new requisitions are introduced. **Documents: Written Policy. Record of removal.**		
13. Lab obtains written acknowledgement from all clients who receive preprinted prescription pads requisitions ("script orders"). All script order forms have been reviewed and approved by compliance officer [or other officer]. **Documents: Written Policy. Sample of written acknowledgements; script order forms.**		

ASSESSMENT AREA	✓	COMMENTS
14. Lab has standing order policy—implemented and monitored. Standing orders are signed by ordering provider, for fixed term—periodically monitored. **Documents: Written Policy. Sample of standing orders and monitoring documents.**		OIG Compliance Program Guidance
15. Lab has procedure to review, approve all special profiles (and preprinted requisitions), and to document, collect, and maintain each physician request (signed physician authorizations). Annual written notices to clients. **Documents: Written Policy. Description of approval process; sample of profile requisitions and PALs.**		OIG Compliance Program Guidance
16. All profiles offered at a price above cost. If tests are added to profiles, the price for the enhanced profile is increased (i.e., 10 test profile costs more than nine test profile). **Documents: Written Policy. Sample of profiles with pricing.**		OIG Compliance Program Guidance
17. If lab offers discounts, lab has written discount policy that meets state and federal requirements. **Documents: Written Policy and procedures for setting and approving pricing discounts.**		Third-party and patient pricing is reasonable and above Medicare reimbursement. **Labs' client pricing policy should be reviewed by qualified legal counsel.**
18. Lab does not waive federal insurer copayments and deductibles. **Documents: Written Policy. Samples from patient account billing.**		1994 Fraud Alert
19. Charges to managed care plans waived due to exclusive contract with another lab only when the physician receives no financial benefit (i.e., bonus for meeting utilization thresholds, avoid financial penalties for utilization) and has signed certification to this effect. **Documents: Written Policy. Copies of certifications from clients for which managed care plan charges are waived pursuant to an exclusive contract with another laboratory.**		1994 Fraud Alert
20. Billing adjustments are made only for legitimate billing problems and are not used to provide indirect discounts. **Documents: Written Policy. Samples of client adjustments.**		
21. Testing for any physician, employee of the physician, or family member of the physician is billed to: A. The individual's insurer, B. The individual as a direct-pay patient, or C. Existing client bill account at existing client rates. **Documents: Written Policy. Copies of bills.**		1994 Fraud Alert
22. Does lab provide nonmonetary compensation to any physician, employee of the physician, or family member of the physician (i.e., flowers, tickets to sporting events, lunches, dinners, and other gifts)? If so, the gifts are not solicited by the physician. The value of the gifts is limited to $359 (in 2011, adjusted for inflation) per physician annually. Gifts are not given to a group practice. Lab has a mechanism in place for tracking these gifts—i.e., amount, timing, and nature of gifts involved—and compliance with annual limit. **Documents: Written Policy. Annual log of gifts to each physician who received gift(s) that year.**		CMS has said "The exception for nonmonetary compensation . . . only protects gifts to individual physicians. [G]ifts given to a group practice would not qualify for this exception [and the exception does] not apply to gifts, such as holiday parties or office equipment or supplies, that are valued at not more than [the annual limit] per physician in the group, but are, in effect, given or used as a group gift." 66 FR 921 (Jan. 4, 2001)

David Gee can be reached at Garvey Schubert Barer, 1191 Second Ave., Second & Seneca Building, 18th Floor, Seattle, WA 98101-2939; 206-816-1351; dgee@gsblaw.com.

HIPAA Fine, Settlement Highlight Privacy Policies, *from page 1*

Marcy Wilder, a partner at Hogan Lovells in Washington, notes that when Congress enacted the HITECH Act, it sent a message to HHS to "get serious" about HIPAA enforcement. HHS's action against Cignet showed that it has, in fact, gotten the word, she said.

Wilder, a former deputy general counsel at HHS and the lead agency lawyer on the HIPAA rules, said the CMP assessed against Cignet "sends a message" to covered entities that they had better cooperate in investigations concerning violations of the privacy rule. The final determination should put covered entities on notice that they will be subject to severe penalties if they fail to answer agency queries, she said.

Privacy Rule Violations

According to HHS, OCR found in October 2010 that Cignet violated patients' rights by refusing them access to their medical records when requested. The HIPAA privacy rule requires covered entities to provide patients with their medical records within 30 days from the date of a request. The agency assessed a $1.3 million CMP for these violations, in addition to the $3 million assessed for failing to cooperate with HHS's investigation, the agency said.

> ***"The CMP assessed against Cignet 'sends a message' to covered entities that they had better cooperate in investigations concerning violations of the privacy rule."***
> ***– Marcy Wilder***

According to HHS, the investigation began when a group of Cignet patients filed individual complaints with OCR. When the office requested the records, Cignet failed to respond. A subpoena met the same result, leading OCR to file a petition to enforce the subpoena in the U.S. District Court for the District of Maryland, *United States v. Uplift Medical* PC, D. Md., No. 10-59, *filed* 2/4/10. Cignet did not respond to the petition, and the court awarded HHS a default judgment April 1, 2010. Cignet subsequently produced the medical records but otherwise made no effort to resolve the complaints through informal means, HHS said.

OCR also found that Cignet failed to cooperate with its investigation on a continuing daily basis during the period of March 17, 2009, to April 7, 2010. The agency said, "Cignet's failure to cooperate with OCR's investigation of each complaint constitute[d] a separate violation of [the privacy rule], and each day that the violation continued . . . counts as a separate violation." Further, each "violation was due to Cignet's willful neglect of its obligation to comply" with the privacy rule, the release said. It noted that covered entities are required by law to cooperate with investigations.

"Covered entities and business associates must uphold their responsibility to provide patients with access to their medical records and adhere closely to all of HIPAA's requirements," says OCR Director Georgina Verdugo, adding that HHS "will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules."

Wilder believes the case could represent a "sea change" in the agency's enforcement practices. She noted that the case is not about a data breach or misuse of private health information—areas in which HHS has been more aggressive about enforcement in the past. Instead, this case is about a covered entity's failure to implement basic HIPAA privacy requirements and protecting basic individual rights—in particular, the right to access one's medical records.

Wilder noted that the HITECH Act made "very significant" changes with respect to enforcement of the HIPAA rules. Congress increased HHS's authority to impose CMPs for HIPAA violations and increased the amount of the penalty that could be imposed per violation, she said. The Cignet case is the first time HHS has used that enhanced authority.

The amount of the penalty was not surprising in light of Cignet's "profound" failure to cooperate, as documented in the notice of proposed determination, Wilder added. "HHS was concerned that Cignet's failure to provide patients with access to their medical records hindered the patients' ability to get health care they were seeking from non-Cignet physicians." She said the "failure to cooperate, combined with Cignet's willful neglect of the privacy rule, led to the significant penalty."

The amount sends a "very strong and serious message" to covered entities that violations of basic rights granted by HIPAA will not be tolerated, Wilder said.

Hospital to Pay $1 Million in Settlement

In a case announced just days after the Cignet penalty, a Massachusetts hospital agreed to pay $1 million to resolve allegations that a hospital employee took sensitive health information home, then lost it while commuting to work.

> ***"HHS was concerned that Cignet's failure to provide patients with access to their medical records hindered the patients' ability to get health care they were seeking from non-Cignet physicians."***
> ***– Marcy Wilder***

HHS said the General Hospital Corp. and Massachusetts General Physicians Organization Inc., collectively known as Mass General, agreed to pay the amount to the federal government to resolve allegations that the hospital violated the HIPAA privacy rule. Mass General did not admit liability or wrongdoing, according to the parties' Feb. 14 resolution agreement.

The hospital also must implement a three-year corrective action plan (CAP), the resolution agreement said. In return, the agency agreed not to pursue further action against the hospital regarding the incident involving the lost files.

The Mass General resolution agreement described a 2009 incident in which an employee removed files from Mass General's premises in order to work on them from home. The documents contained the name, date of birth, medical record number, health insurer and policy number, diagnosis, and name of provider for 66 patients. Also taken home by the employee were daily office schedules for three days that contained the names and medical record numbers for 192 patients.

While commuting to work on the subway, the agreement said, the employee removed the files from her bag and placed them on the seat next to her. The employee left the documents on the train and they were never recovered, HHS said.

HHS's Office for Civil Rights (OCR) began its investigation after receiving a complaint from a patient whose protected health information was lost. According to the press release, OCR's investigation indicated that Mass General failed to implement reasonable and appropriate standards to protect the privacy of patient information removed from the facility. OCR also found that Mass General likely impermissibly disclosed protected health information in violation of the HIPAA privacy rule.

Terms of Three-Year CAP

The CAP appended to the resolution agreement requires Mass General to develop and implement written policies to protect health information taken off premises and to submit to a three-year period of monitoring by HHS.

The agency said the hospital's procedures must address physical removal and transportation of protected health information, laptop encryption, and USB drive encryp-

Mark Your Calendar!

Spring

Molecular Diagnostics Spring 2011: MDX Goes Mainstream
April 13-15, 2011, Boston

Lab Outreach 2011
June 15-17, 2011, Las Vegas

Fall

Molecular Diagnostics Fall 2011
Sept. 22, 2011, San Francisco

Lab Institute 2011
Oct. 19-21, 2011, Arlington, Va.

Winter

LabCompete: Lab Sales and Marketing 2011
Dec. 12-14, 2011, Chandler, Ariz.

For information or to register, go to www.G2Intelligence.com

tion and must be consistent with federal standards that govern the privacy of individually identifiable health information.

At a minimum, the CAP said, the policies and procedures must include administrative, physical, and technical safeguards, as well as reasonable measures to protect health information from intentional and unintentional disclosures. If a disclosure occurs, Mass General must inform the monitor of the "reportable event" within 30 days, the CAP said. The new policies and procedures must be approved by HHS, it added.

The CAP also requires Mass General to provide training on the policies and procedures to all employees within 90 days of HHS's approval of the policies.

Mass General must, as a general rule, prohibit employees from physically removing protected health information from its premises. However, the CAP allows the hospital to make an exception when the information is removed by an employee to perform his or her job duties. The employee must be informed of the policy and reminded to take reasonable steps to safeguard the confidentiality of the information.

The CAP also calls for the appointment of a monitor who will assess the hospital's implementation of and compliance with the policies for maintaining the privacy of protected health information. The monitor must report to HHS on the hospital's activities on a semiannual basis for three years. Any significant violations of the CAP must be reported by the monitor to HHS within 10 business days of his or her discovery of the violation, the CAP said.

In addition, Mass General must make an annual report to both HHS and the monitor summarizing the status of its implementation of the privacy policies, the CAP said.

Red Flags Rule Challenge Now Moot

An American Bar Association lawsuit challenging the scope of the Federal Trade Commission's "red flags" rule has been rendered moot by a recent legislative fix, the U.S. Court of Appeals for the District of Columbia Circuit held March 4.

The American Medical Association (AMA), which along with a coalition of health groups filed a lawsuit in May 2010 challenging the "red flags" rule as applied to physicians, said in a March 7 statement that its lawsuit challenging the same rule "will now formally end" in light of the D.C. Circuit's decision.

The AMA said the decision "further validates the American Medical Association's longstanding argument to the Federal Trade Commission that physicians who bill after rendering services are not subject to the red flags rule as creditors." The rule requires financial institutions and certain creditors to implement identity theft prevention programs.

The D.C. Circuit in its decision said that, in light of the Red Flag Program Clarification Act, signed into law in December 2010, the FTC's previous assertion that the term "creditor" under the rule includes all entities, including law firms and health care providers, that regularly permit deferred payments for goods or services, no longer is viable.

News-At-A-Glance

LAB OWNER SENTENCED TO PRISON: A former owner and manager of a New York City blood testing laboratory who left the United States in 1998 has been sentenced to 18 months in prison for defrauding Medicare of nearly $200,000, prosecutors announced Feb. 25. At sentencing Feb. 25 before Judge Denise Cote of U.S. District Court for the Southern District of New York, the defendant, Zafar Chaudhry, was also ordered to pay Medicare $196,464 in restitution. He had pleaded guilty on Nov. 12, 2010, to one count of conspiracy to commit mail fraud and health care fraud and the submission of false statements on health care matters. Chaudhry was charged in February 2000 along with his uncle, Raza Chudry, who prosecutors said had together accounted for some 20 percent of all amino acid profile reimbursement claims submitted to Medicare in 1997.

NEW LAB ACCREDITATION STANDARDS: The Joint Commission has updated its "Comprehensive Accreditation Manual for Laboratory and Point-of-Care Testing" to provide clarity, additional specificity, and detail to the standards and elements of performance. A preview of the manual is available on the commission's Web site at *www.jointcommission.org*. Laboratories will be surveyed against the new manual beginning in July 2011. The Joint Commission says the standards and related elements of performance provide clearer compliance expectations to make the on-site survey process more transparent but continue to offer flexibility for laboratories to tailor the standards for their specific organization.

COURT CLEARS WESTCLIFF PURCHASE: Laboratory Corporation of America (Burlington, N.C.) can complete the purchase of Westcliff Medical Laboratories (Santa Ana, Calif.), a judge has ruled. U.S. District Judge Andrew Guilford Feb. 22 denied the Federal Trade Commission's request for a preliminary injunction. The agency had argued that the transaction would harm competition in Southern California. The FTC has appealed the court's ruling to the U.S. Court of Appeals. G2

G2 Compliance Report Subscription Order/Renewal Form

❑ ***YES***, enter my one-year subscription to the ***G2 Compliance Report (GCR)*** at the rate of $487/yr. Subscription includes the ***GCR*** newsletter, and electronic access to the current and all back issues. Subscribers outside the U.S. add $100 postal.*

❑ I would like to save $292 with a 2-year subscription to ***GCR*** for $682*

❑ ***YES!*** Please send me ___ copies of ***CLIA Compliance: The Essential Reference for the Clinical Laboratory, 3rd Edition*** for just $549 and your state's sales tax. The price includes shipping/handling. (Report Code # 4213NL)

Please Choose One:

❑ Check Enclosed (payable to G2 Intelligence)

❑ American Express ❑ VISA ❑ MasterCard

Card # _____ Exp. Date_____

Cardholder's Signature_____

Name As Appears On Card_____

Ordered by:

Name_____

Title _____

Company/Institution _____

Address _____

City _____ State _____ Zip_____

Phone _____ Fax_____

E-mail address _____

Mail to: G2 Intelligence, 1 Phoenix Mill Lane, Fl. 3, Peterborough, NH 03458-1467 USA. Or call 800-401-5937 and order via credit card or fax order to 603-924-4034

*By purchasing an individual subscription, you expressly agree not to reproduce or redistribute our content without permission, including by making the content available to non-subscribers within your company or elsewhere. For multi-user and firm-wide distribution programs or for copyright permission to republish articles, please contact our licensing department at 973-718-4703 or by email at: jping@g2intelligence.com.

GCR 4/11

 G2 Compliance Report (ISSN 1524-0304) is published by G2 Intelligence, 1 Phoenix Mill Lane, Fl. 3 , Peterborough, NH 03458-1467 USA. Tel: 800-401-5937 or 973-718-4700. Fax: 603-924-4034. Web site: www.G2Intelligence.com.

Kimberly Scott, Managing Editor; Dennis Weissman, Executive Editor; Heather Lancey, Designer; Beth Butler, Marketing Director; Dan Houder, Chief Marketing Officer; Doug Anderson, VP & Publisher; Joe Bremner, President

Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 800-401-5937.