G2 Compliance Report

For Hospitals, Laboratories and Physician Practices

Kimberly Scott, Managing Editor, kscott@G2Intelligence.com Issue 12-07 • July-August 2012

Inside this issue

www.G2Intelligence.com

The End of the Pathology Grandfather: Strategies for Negotiating TC Payments With Hospitals

With the June 30 expiration of the pathology grandfather protection just a few weeks away, some laboratories are scrambling to negotiate payment rates for the technical component (TC) of pathology services they provide to hospitals.

Experts say there are several ways to set payment for the TC, ranging from a fixed monthly payment to cost-plus pricing to a fixed fee schedule payment based on CPT code. Speaking during a May 31 webinar held by G2 Intelligence, Jane Pine Wood, Esq., an attorney with McDonald Hopkins (Dennis, Mass.), notes that she has clients who have negotiated a percentage of the Medicare physician fee schedule or the outpatient prospective payment system (OPPS) ambulatory payment classification (APC). "Each case is different," says Wood.

On Feb. 17, 2012, Congress voted to discontinue direct Medicare payment for the TC of pathology services provided to inpatients and outpatients for grandfathered hospitals after June 30, 2012. Since 1999, labs that provided services to grandfathered hospitals could

Continued on page 8

Lawmakers Prepare Bill to Give CMS Enforcement Discretion in PT Referrals

Lawmakers in both the House and Senate are preparing to introduce legislation that would give the Centers for Medicare and Medicaid Services (CMS) more discretion in enforcing a law that bars clinical laboratories from referring proficiency testing (PT) samples to another laboratory.

All laboratories certified under the Clinical Laboratory Improvement Amendments (CLIA)—except those performing waived tests—must participate in PT. Most sets of PT samples are sent to participating laboratories three times per year. After testing the samples in the same manner as its patient specimens, the laboratory reports its sample results back to their PT program.

Labs must test PT samples in the same manner as patient specimens, and the specimens must be tested by the same personnel who routinely test patient specimens. The lab director or designee and testing personnel must sign an attestation sheet, and each step in testing must be documented, with records retained for two years.

Continued on page 2

PT Referral, *from page 1*

Labs may not send PT samples to another laboratory with a different CLIA number for testing even if it typically sends patient specimens out for confirmation or identification testing. Sending PT samples to another laboratory for testing may be considered PT referral and will result in the loss of the lab's CLIA certificate for at least one year. In addition, the lab director cannot direct a laboratory for two years, and the lab owner may not own or operate a lab for two years.

Even though CMS has cautioned labs not to send out PT samples, not even for a reflex or confirmatory test, there are a certain number of referrals that occur each year. Under the current law, CMS does not have discretion in enforcement. A lab will lose its CLIA certificate, even if the lab can prove that the referral was inadvertent, or in cases where a lab sends a PT sample to a sister lab with a different certificate number.

According to an article published in 2009 in the *Archives of Pathology and Laboratory Medicine,* between 1993 and 2006, 78 laboratories received a principal sanction for a PT violation involving sample referral or result communication out of about 45,000 labs subject to PT testing. While violations are relatively rare when compared to the total number of labs being tested, the consequences of violations are severe, noted the author, Anthony Killeen, M.D., Ph.D., who offered suggestions on policies and practices to minimize the risk of a PT sample referral or result communication.

'Shall' to 'May'

The legislation being drafted would change the wording in the statute from "shall be suspended for the period the laboratory is so excluded" and replace it with "may be suspended for the period the laboratory is so excluded." The Senate version of the bill also calls for a study on improper referrals and would require that CMS issue guidance on how it defines "improper and intentional referrals."

Judy Yost, director of the division of laboratory services at CMS, says she recognizes that there are instances when referrals are made by accident and supports legislation that would give her division more enforcement discretion.

While CMS has prevailed in almost all administrative appeals involving PT referrals, a lab in September 2011 actually won its appeal. In *J.B. and Greeta B. Arthur Comprehensive Cancer Center v. CMS*, a Health and Human Services Departmental Appeals Board administrative law judge decided that CMS could not revoke the CLIA certificate of the cancer center laboratory based on it having sent unused portions of the PT samples to a lab operated by Audrain Medical Center of Mexico, Mo., with which the cancer center is affiliated.

According to the January 2012 issue of *CAP Today*, the medical center's laboratory tested the samples, which had been sent to it for storage, before the cancer center lab reported its PT results. The cancer center's position was that testing of the PT samples by another laboratory was not in and of itself a basis on which to find that a sample had been referred to another lab for analysis.

The ALJ agreed, finding it significant that the cancer center laboratory did not direct the medical center to test its PT samples and did not require or suggest that the medical center advise it of its own test results. The ALJ said it was clear that "the prohibition is against the sending of the proficiency samples to another laboratory for analysis. The intent requirement is not met by the simple act of sending PT samples to another laboratory." G2

Court Dismisses Whistleblower's Lawsuit On False Claims, Anti-Kickback Violations

A federal trial court in Louisiana May 21 dismissed a whistleblower's False Claims Act (FCA) lawsuit against West Calcasieu Cameron Hospital (WCCH), finding that the relator failed to plead a single specific false claim or a single specific referral in violation of the anti-kickback statute (*United States ex. rel. Nunnally v. West Calcasieu Cameron Hospital*, W.D. La., No. 2:08-cv-00371-PM-KK).

According to the U.S. District Court for the Western District of Louisiana, the qui tam complaint alleged that WCCH submitted false claims to the government by billing for laboratory services at a higher price than that charged to certain referred patients not covered by Medicare and billing for lab services rendered to patients referred to WCCH by physicians in violation of the anti-kickback statute (AKS).

The district court relied on *United States ex rel. Thompson v. Columbia/HCA Healthcare*, 938 F.Supp 399 (1997), in which the U.S. Court of Appeals for the Fifth Circuit held that a relator may not maintain an FCA case based on violations of the AKS unless the provider was required to file certification in connection with the claim, the filed certification was false, and the relator identifies specific claims and/or certifications that were fraudulent.

The qui tam complaint alleged that WCCH submitted false claims to the government by billing for laboratory services at a higher price than that charged to certain referred patients not covered by Medicare and billing for lab services rendered to patients referred to WCCH by physicians in violation of the anti-kickback statute (AKS).

The court, finding that relator Dent T. Nunnally failed to allege that WCCH made a knowingly false certification of compliance with a statute or regulation, or that WCCH impliedly certified compliance by participating in Medicare, or made an express certification, concluded that the complaint did not state a claim for which relief can be granted under the AKS.

The district court also found the complaint deficient under the Fifth Circuit's ruling in *Grubbs v. Kanneganti*, 565 F.3d 180 (2009) because it did not identify any specific physicians, patients, services, or claims involved in the alleged scheme.

House Approves Legislation Reauthorizing FDA User Fees

In a 387-5 vote, the House May 30 approved legislation (H.R. 5651) that renews the fees that drug and device companies pay to support the Food and Drug Administration (FDA).

The bill reauthorizes the Prescription Drug User Fee Act (PDUFA) and the Medical Device User Fee Act (MDUFA) and creates new user fee programs for generic drugs and biosimilar (or follow-on biologic) drugs. The user fees supplement congressional appropriations for FDA. The current PDUFA and MDUFA programs will expire Sept. 30, unless Congress reauthorizes them.

Significant for clinical laboratories, the legislation gives the Department of Health and Human Services a discretionary waiver authority. FDA officials have said that they would use the authority to ensure that lab-developed tests (LDTs) would not

be subject to user fees due to regulatory changes in policy on LDTs. The waiver would sunset on Oct. 1, 2017.

Industry groups worried that user fees might come into play for labs if the FDA issues guidance requiring LDTs to go through FDA clearance. They negotiated with FDA and other groups to ensure the agency had the waiver authority. The FDA says it plans to regulate LDTs and believes it has the authority to do so. However, legislation pending in Congress would assign LDT oversight to the Clinical Laboratory Improvement Amendments program at the Centers for Medicare and Medicaid Services.

The bill also has numerous provisions affecting FDA's regulation of drugs and devices, such as new incentives for the development of antibiotics and a provision to address drug shortages.

Significant for clinical laboratories, the legislation gives the Department of Health and Human Services a discretionary waiver authority. FDA officials have said that they would use the authority to ensure that lab-developed tests (LDTs) would not be subject to user fees due to regulatory changes in policy on LDTs. The waiver would sunset on Oct. 1, 2017.

The Senate approved its version of the bill (S. 3187) on May 24. The bills next will go to a conference.

In a summary of the legislation, the House Energy and Commerce Committee said the user fees bill "will ensure continuation of various FDA programs and the creation of new ones to facilitate the review and approval of life-saving and life-improving drugs and medical devices." As part of the agreement with industry to renew the fees, "FDA will commit to certain performance goals, fostering more interaction, predictability, and certainty between industry and FDA," the House summary said.

Although both bills have moved easily through the House and Senate, consumer groups have continued to criticize the measures for not doing enough to protect the public from unsafe medical devices. In addition, one group said the House bill is weaker than the Senate bill, while another consumer group cited concerns with a provision in the House bill that allows FDA to keep certain drug-related information confidential.

User Fees

The House bill would reauthorize PDUFA for fiscal years 2013 through 2017. It would set total PDUFA fee revenue for FY 2013 at $713 million and a higher amount in the remaining four years, according to the summary of the bill. The Senate version of the bill would set PDUFA fees for FY 2013 at $693 million.

The House bill also would reauthorize MDUFA, allowing a total of $595 million in fees to be collected from industry over the five-year period of FY 2013 through FY 2017, according to the summary. This is same amount as in the Senate bill.

The House bill, like the Senate bill, would authorize a new generic drug user fee program. Under the House bill, a total of $1.5 billion could be collected from industry over the five-year period, the summary said. Additionally, the House bill would authorize a new biosimilars user fee program. Both the Senate and House bills base the fee amounts on inflation-adjusted PDUFA fee amounts for each fiscal year and both set the initial product development fee at 10 percent of the human drug application fee under PDUFA.

G2 INTELLIGENCE

COMPLIANCE PERSPECTIVES

James J. Giszczak and Dominic A. Paluzzi are attorneys with McDonald Hopkins PLC (Bloomfield Hills, Mich.).

Data Breach at Your Laboratory? Immediate Action Items! How to Deal with a PHI Violation

Dr. Jill, one of your partners, and Mary, the head of human resources (HR), at a prominent lab (our hypothetical "XYZ Co.") pack up from a long day at work and put their laptops and hard copy files in the backseat of their respective cars. Both plan on catching up on work over the long holiday weekend. They decide to meet and have a drink on the way home to discuss workflow and personnel issues. When Dr. Jill and Mary leave the restaurant to head home, they walk to the parking lot to find their cars have been broken into. Although upset about the damage to their cars, and their missing personal effects, that is not their biggest problem. Rather, the loss of the HR files containing personal information (PI) and protected health information (PHI) will be the source of sleepless nights for Dr. Jill, Mary, and XYZ's senior management. Mary's computer and the hard copy files contained PI such as Social Security numbers, driver's license numbers, banking records, passport numbers, credit reporting histories, and PHI including medical information, treatment, diagnosis, and medical insurance information. Dr. Jill also had patient information on her computer, as well as in hard copy.

You may be thinking, "This will never happen to me or our organization." Well, according to the Privacy Rights Clearinghouse, over 544,664,595 data breaches have been reported since 2005. As you might imagine, many have gone unreported. It is estimated that the number of data breaches is more likely three times greater, or *1,633,993,785!*

There are lots of moving pieces, so what should Dr. Jill, Mary, and XYZ Co. do next?

1 Gather the Incident Response Team.

If you just read the above and are asking yourself, "What is an incident response team?" you are not alone. The incident response team is a group of decisionmakers in legal, information technology (IT), risk management, HR, marketing, and public relations. The composition of the incident response team is critical as a data breach affects almost every component of the organization. The incident response team should be predetermined and set forth in the incident response plan, which is the "go to" document that identifies the appropriate internal and external resources to properly deal with a data breach.

2 Call Insurance Agent.

Cyber liability insurance is the newest coverage being offered by top brokers and agents around the world. Cyber liability coverage can be complicated and may cover losses and expenses related to event management, cyber extortion, business interruption loss, fines and penalties, computer forensics, notices, network security liability, privacy liability, and electronic media liability coverage. The insurance agent must be put on notice at the very outset of the breach so that he or she is included in all relevant communications to ensure appropriate notice.

3 Call Experienced Data Privacy Attorneys.

The incident response team, Dr. Jill, Mary, and others should not be e-mailing each other regarding the cause of the breach or potential exposure. All of these e-mails could be discoverable in litigation or an investigation. It is critical that an attorney with data security experience is brought on board immediately to preserve the privilege of communications. This is not the time to call your corporate or estate planning attorney. Having the wrong professional or inaccurate advice as to whether notice is required, who to notify, what to include in the notification, and when to send it can result in substantial (six- or seven-figure) penalties, fines, or judgments, both as a result of private rights of action or enforcement actions brought by the Department of Health and Human Services and state attorneys general.

4 Determine and Assign Breach Coordinator.

One individual from the incident response team must be selected to coordinate the breach response efforts both internally and externally. This individual will be responsible for communicating with legal, HR, public relations, and outside vendors. It is critical that the organization has a consistent message with regard to the incident and the steps the company is taking to notify the affected individuals and ensure that PI and PHI in the company's possession is safeguarded in the future.

5 Preserve Evidence of Breach and Secure IT Systems.

When a breach is discovered, it is important that a forensic expert, either located within the company or an external vendor, is retained to contain the breach. In Dr. Jill and Mary's example, it's important to determine whether the computers were encrypted, what may have been on the laptop, whose PI or PHI may be threatened, and what was contained in the hard copy files. Most importantly, IT needs to secure the systems to make certain that a subsequent hacking incident does not take place, especially given the chance the thieves have the ability either to access the system themselves or sell the laptop and hard copy PI on the black market to an expert that knows how to steal identities. It is critical to contain the damage.

6 Contact Law Enforcement.

Dr. Jill and Mary probably contacted the local police and filed a police report related to the break-in of their vehicles and the theft of their laptops. (Counsel will most likely also be in touch with the FBI regarding the incident.) Dr. Jill and Mary most likely did not mention, however, that the laptops and folders contained PI and PHI of many individuals. Most of the data breach notification statutes (which 46 of the states and Washington D.C., have enacted various different versions of) allow for a delay in notification to affected individuals pending law enforcement investigation.

7 Breach Notification Letters: Do They Need to Be Sent? Who Gets Them? When Are They Sent? What Should They Say? What Should They Not Say?

One of the most complicated components of the data breach process is the breach notification letters to affected individuals. This is most confusing due to the fact that 46 states and Washington, D.C., have each enacted their own breach notification statutes that require notification based on different triggering events, such as when reasonable likelihood of harm to an individual exists, when the incident could result in identity theft, whether PI is subject to further unauthorized disclosure, when misuse of PI has occurred, or when the incident is likely to cause loss or injury or economic loss or financial harm. This is further complicated by federal statutes governing the loss of PHI.

The state of residence of the affected individual determines the applicable state notification law. (However, XYZ Co. must also consider the federal statutory requirements.) So a company that experiences a large data breach will most likely have to be compliant with almost every one of the 47 breach notification laws, in addition to foreign notification laws and federal statutes!

Moreover, each of the statutes requires different elements in the breach notification letter. Some states require the entity disclose the breach incident with specific detail, while other states, such as Massachusetts, prohibit any details of the breach be disclosed to affected individuals. Many of the laws also require notifications be sent by certain time periods (i.e., within 45 days of discovery of the breach). Depending on the amount of notices, companies can either send the letters directly or work with a mail house to do so.

If the laptop was encrypted, XYZ Co. may have dodged a huge bullet and may not have to provide notice, unless, of course, the encryption key is on a sticky note attached to the top of the laptop! It happens, more often than you think.

8 Offer Credit Monitoring.

Each of the three credit reporting agencies offers a credit monitoring service wherein they will monitor any suspicious behavior of a credit file and report same to the individual. Companies that experience data breaches will often provide, at no charge to the individual, a 12-month three (or one) bureau credit monitoring subscription to the affected individuals. This serves at least two purposes: (1) it eases the individuals' minds that their identity will be monitored and not compromised without their knowledge, and (2) it mitigates the entities' damages should a negligence lawsuit be filed in the future against it.

9 Draft Press Release.

Depending on the number of individuals that must be notified and the type of information that was compromised, XYZ Co. may be required to publish a press release or media statement with information about the breach. The press release may also appear on the company's Web site and, you must assume, that it will end up on other sites that track data breaches, such as *www.datalossdb.org*. As such, it is critical that experienced counsel is involved in this process as well.

10 Draft FAQs.

To assist with call center operations and for consistent messaging, organizations should draft a frequently asked questions document with answers to questions that the organization will most likely receive from affected individuals, state agencies, and the press. FAQs are often posted to the company's Web site in an effort to streamline communication.

11 Notify Appropriate State Agencies.

Many of the state breach notification statutes require that entities notify state agencies, such as attorneys general, offices of cybersecurity, and state police. The state agencies require full disclosure of the breach incident, the number of state residents affected, and a redacted copy of the notification letter in many instances.

If PHI was compromised, the Department of Health and Human Services must also be notified under the Health Information Technology for Economic and Clinical Health (HITECH) Act. Notification to major state media outlets is also necessary under HITECH if more than 500 people from one state were affected.

12 Report Incident to Credit Card Companies and Credit Reporting Agencies.

If credit card numbers were compromised in the incident, XYZ Co. will most likely, by contract with Visa, MasterCard, or American Express, have the obligation to notify the credit reporting companies. In addition, if the threshold number of affected individuals is met in any one state (i.e., 1,000 for most states), the organization is required to notify the credit reporting agencies of the breach incident.

Conclusion

It is not the case of *if* a data breach will occur to an organization, but *when*. It is critical that organizations engage now in proactive measures to minimize the risk of a data breach and be prepared to take appropriate and immediate actions when a data breach does occur.

The above action items are just a starting point. It's critical that organizations work with experts in the data privacy arena when preparing for and responding to a data breach.

James J. Giszczak and Dominic A. Paluzzi can be reached at McDonald Hopkins PLC, 39533 Woodward Ave., Suite 318, Bloomfield Hills, MI 48304, 248-220-1354. E-mail: jgiszczak@mcdonaldhopkins.com *and* dpaluzzi@mcdonaldhopkins.com.

The End of the Pathology Grandfather, *from page 1*

bill separately for the TC of pathology services. Effective July 1, 2012, pathologists' practices that provide TC services to a hospital's patients will need to negotiate hospital reimbursement for their TC services.

The grandfather exemption was only available to patients covered by traditional fee-for-service Medicare and not patients covered under Medicare Advantage plans, Medicaid, Medicaid health maintenance organizations, or any other third-party payer. Thus, Medicare Advantage and Medicaid never were required to recognize the exemption (although some plans did).

For clinical laboratory services—as opposed to anatomic pathology services—the rules remain unchanged. The laboratory must bill the hospital for Medicare inpatient work but can bill Medicare directly for outpatient work (for services covered under the clinical lab fee schedule). Labs participating in a Medicare demonstration project for highly complex tests can bill Medicare directly for those tests, notes Wood.

State Medicaid programs must be checked on a case-by-case basis, she advises. Because the grandfather protection never applies to Medicaid, labs will need to consider Medicaid billing separate from Medicare billing. "I am aware of some Medicaid programs that have informally recognized grandfathered hospitals and presumably that will go away come July 1," says Wood. "Every state Medicaid program sets its own rules, but most of them do not permit the independent lab to bill for inpatient TC services. However, most of them will allow labs to bill Medicaid directly for outpatient services."

Private payers have handled TC pathology payment in different ways, and there is great variation by region, notes Wood. Blue Cross and Blue Shield of Florida, for example, has maintained for years that it pays the hospital for the TC of pathology services provided to inpatients and will not pay the lab directly for those services. However, the health plan has in some contracts with labs recognized the grandfather exception, but that is expected to end as of June 30.

Because critical-access hospitals (CAHs) are not paid on a diagnosis-related group (DRG) basis but are paid on a cost basis, the requirement to bill the hospital does not apply. However, Wood recommends that labs negotiate TC payment with CAHs and let the hospitals collect payment directly from Medicare. Given the recent tightening of Medicare billing requirements and the increase in Recovery Audit Contractor (RAC) audits, Wood argues labs should avoid being put in the position where they have to prove they were allowed to bill Medicare directly especially since the grandfather exception language does not mention CAHs specifically.

Because the grandfather exception applies to "covered" hospitals and there is no master list of which hospitals are covered and which aren't, Wood also advises that labs get an attestation statement from each hospital that it was, in fact, covered by the grandfather exception prior to the June 30 expiration. The attestation statement is important if a lab were to undergo a RAC audit, she says, noting that it may be required to prove that the direct billings to Medicare prior to July 1 were appropriate.

Hospital Reimbursement

The College of American Pathologists (CAP), which has published a guidance document on options for negotiating the TC with hospitals, notes that labs should be aware of how hospitals are reimbursed for TC services from Medicare. This will help the practice in its negotiations.

Resources

The College of American Pathologists has a number of resources available to help labs and pathologists in their TC negotiations with hospitals.

- Background on TC grandfather and options for negotiations: *www.cap.org/apps/docs/advocacy/tc_alternatives.pdf*
- Hospital TC Sample Contract: *www.cap.org/apps/docs/advocacy/tc_sample_hospital_contract.pdf*
- Addendum B—Final OPPS Payment by HCPCS Code for CY2012: *www.cap.org/apps/docs/advocacy/apc_by_cpt_code_for_pathology.pdf*

"When attempting to understand what the hospital will receive for TC services, the practice may also want to consider the hospital's billing cost," says CAP. "Billing costs will affect the net revenue the hospital has available to pay the practice from their reimbursement for TC services."

For hospital inpatients, the hospital typically does not receive additional reimbursement for TC services since Medicare maintains that amount is already included in DRG payment.

For outpatients, the hospital generally receives additional reimbursement for TC services under OPPS. The payment rate is then adjusted by economic area and other factors. The APC rate varies by state and region, but in general hospitals receive 55 percent to 60 percent of the Medicare physician fee schedule amount for outpatient services, says Wood, who advises labs to keep this in mind as they conduct their negotiations.

Know Your Costs

Before beginning negotiations with the hospital, labs need to know their cost of providing the TC service by billing unit (CPT codes, case counts, and block and slide counts). When considering using CPT codes, the practice will need to decide whether to use all CPT codes or just those associated with TC services, notes CAP.

For example, CPT 85097 does not have a separate TC payment listed in the Centers for Medicare and Medicaid Services physician fee schedule as it is considered a professional-only service. However, 85097 does receive a reduced reimbursement when provided in a facility and it does translate to APC 0343. The net result is the practice will receive lower reimbursement for 85097 and the hospital can receive TC service reimbursement.

When determining the cost of providing TC services, the practice may want to consider not only the operational costs of services but also its overhead cost and capital requirements, notes CAP.

"The purpose of knowing the practice's costs is not to rack up accounting fees but to enable the practice to understand at what point it needs to walk away from the negotiations," says CAP. "A hospital-practice relationship where the practice is losing money cannot endure indefinitely and presents compliance concerns for both parties (providing services below cost is generally considered inducement or a kickback). A practice that knows its cost will know where it can be flexible and where it must be rigid in the negotiation process."

Payment Options

There are several options for how labs can structure their TC payment with the hospital, according to CAP.

- **CPT-based billing**. This is typically the first and easiest billing unit practices and hospitals consider. Payment usually is set as a certain percentage of the Medicare fee schedule. The advantage of this method is it is easily understood and relatively easy to implement. One disadvantage is the wide variety of costs that can be associated with a single CPT code like 88305, says CAP. "Depending on the case mix, CPT dependent billing can either be lucrative or provide a death knell to the pathologists' practice. A practice that knows its cost for each CPT will be in the best position to negotiate a customized fee schedule or exceptions to a percent of Medicare fee schedule pricing."

- **Cost-plus-based billing**. This approach commonly uses either a case count or block/slide count billing unit. The advantage of this system is it provides a way for the pathologists' practice and the hospital to predict and manage their cost and revenue. It also provides the basis for fact-based negotiations when there are changes in the costs of delivering TC services. Whether this approach is set up as cost-plus or at-cost depends on the goals of the hospital-practice relationship and a practice's margin requirements. This approach does require more initial work in establishing the reliability of the billing unit and associated costs.

For case-based calculations, compute the cost of providing TC services over a specific period of time (preferably a year) and the number of cases for the same period and divide the number of cases into the total costs. For each billing period, the practice would create a count and listing of cases to bill the hospital. This method can be more refined by systems by breaking down case counts and associated cost by type of case.

For block- or slide-based calculations, the practice must separate out the total cost for blocks and the total cost on slides. The appropriate total cost is then divided by the total number of blocks and slides respectively.

Recordings of the May 31 webinar are available for purchase at www.G2Intelligence.com/tcpayments.

CAP notes that a practice can make the above cost-based methods more robust by separating out the counting of and associated costs for high-cost or special tests and charging them by an appropriate billing unit. For example, if flow cytometry were to be billed separately, its cost would be removed

Case Study: Puget Sound Institute of Pathology

Pugent Sound Institute of Pathology (PSIP) recently completed TC negotiations with all eight hospitals for which it provides anatomic pathology services. Stewart Adelman, CEO, described the process during G2 Intelligence's May 31 webinar on the expiration of the pathology grandfather.

PSIP began by calculating the total collections by hospital for all payers and then determining annual collections for Medicare, Medicaid, and Tricare by hospital. Next, PSIP calculated the percentage of government collections at risk from the expiration of the grandfather provision and determined test volumes by CPT code by hospital.

PSIP then calculated its costs, factoring in materials, processing, embedding, cutting, staining, and tech time. Once it had all this information, it was ready to begin negotiation with its hospitals. Adelman said he provided hospital administration with materials explaining the end of the grandfather protection and why the hospital would now be responsible for paying the lab for the TC of pathology services. For his negotiations, Adelman discussed several options for payment with hospitals, including the APC fee schedule, a flat fee (with or without the medical director fee), and government-only testing versus all testing.

Adelman also advises softening the financial impact of the grandfather expiration by identifying cost savings opportunities within the lab, looking into technology investments to gain efficiencies (document scanning, bar coding, voice transcription), and considering adding new service lines, such as FISH, flow cytometry, and molecular testing. Labs should also look at additional hospital opportunities, including professional billing for clinical lab testing, additional medical directorships, and reviewing current discounts for direct billing.

Finally, Adelman advises being creative and flexible, noting that of the agreements reached with PSIP's hospitals, no two are exactly alike.

PSIP Agreements With Hospitals

Hospital A

- *80% APC fee schedule*
- *ClinPath billing*
- *Reduced direct billing costs*
- *Additional medical directorship*

Hospital B

- *100% APC*

Hospital C

- *80% APC fee schedule*
- *ClinPath billing*

Hospital D

- *Monthly flat fee includes medical director fee*

from the total cost and perhaps billed at cost based on CPT or billed by flow cytometry case by just using CPT 88185 as the billing unit. Setting up an approach that provides for special testing can allow for the addition of new tests as a separate, more manageable issue from routine services.

According to Barry Portugal, president of Health Care Development Services Inc., the mean payment for TC processing to independent labs and multihospital systems based on a survey he conducted several years ago was about 67 percent of the physician fee schedule although some of those surveyed reported receiving much more. Results of the survey were broken down into percentiles, with the 25th percentile at 50 percent of the PFS, the 50th percentile at 67 percent, and the 75th percentile at 89 percent.

Portugal says he is advising his clients to consider the entire spectrum of economic, service, and logistical issues before finalizing fee arrangements. He also notes that the amount of Medicare reimbursement hospitals will receive needs to be considered so they may calculate how much net unbudgeted expense they will incur as a result of being billed for outsourced services.

News-At-A-Glance

OIG FRAUD RECOVERIES: The Department of Health and Human Services Office of Inspector General May 29 announced expected recoveries of roughly $1.2 billion for the first six months of fiscal year 2012, due in part to an increased focus on technology solutions, according to the agency's Semiannual Report to Congress. "We are using advanced data analytics to help us conduct risk assessments; more effectively pinpoint our oversight efforts; and significantly reduce the time and resources required for audits, investigations, evaluations, and other program integrity activities," OIG Inspector General Daniel R. Levinson said in the report's introduction. During the first half of fiscal 2012, Medicare Fraud Strike Force operations recovered $51 million and led to the filing of charges against 101 individual or entities. In addition to the expected recoveries, the OIG also reported excluding 1,264 individuals and entities from participating in federal health care programs over the first half of FY 2012, as well as initiating 388 criminal actions and 164 civil actions against individuals and entities.

PRIVACY LAW VIOLATION: A Massachusetts hospital has agreed to pay $750,000 to resolve allegations of privacy law violations arising from a 2010 data breach involving personal data on as many as 800,000 people. Under the consent agreement filed in Massachusetts Superior Court, South Shore Hospital in South Weymouth, Mass., will pay a civil penalty of $250,000 and a contribution of $225,000 into the attorney general's education fund to promote protection of personal information. To satisfy the remainder of the judgment, the hospital will receive a credit of $275,000 to reflect security measures it has taken subsequent to the breach. South Shore Hospital reported in July 2010 that it had not received destruction verification certificates from a firm it hired in February of that year to destroy unencrypted backup computer tapes. The files contained personal data on patients, workers, doctors, volunteers, donors, vendors, and other business partners covering the period from Jan. 1, 1996, to Jan. 6, 2010. The attorney general alleged that South Shore violated the Massachusetts Consumer Protection Act and the Health Insurance Portability and Accountability Act by failing to implement appropriate safeguards, to protect consumer information and failing to execute a business associate agreement with the data destruction contractor, Archive Data Solutions.

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, kscott@G2Intelligence.com; Heather Lancey, Designer; Beth Butler, Marketing Director; Dan Houder, COO and Publisher

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.