Report on
Medicare Compliance

Volume 26, Number 7 • February 27, 2017

Weekly News and Compliance Strategies on CMS/OIG Regulations, Enforcement Actions and Audits

Contents

After OCR Probe of Stolen Flash Drive, Hospital Is Not Fined; Upgrade Was Under Way

If someone had stolen the flash drive from Lawrence General Hospital days or weeks later, there would have been no breach investigation by the HHS Office for Civil Rights (OCR), no site visit and no agonizing wait for an outcome. The hospital had completed an exhaustive risk assessment and was in the process of reconfiguring its computers so their USB ports could only accept hospital-issued, encrypted flash drives when the unencrypted flash drive disappeared. The security upgrades, however, had not yet come to the lower-risk departments, including the lab.

Because there would be no story to tell if it happened any other way, the flash drive was stolen from the lab at the Massachusetts hospital. But the fact the flash-drive replacement was under way at the time helps explain why, on Feb. 17, Compliance Officer Brian Kozik opened a letter from OCR saying it had closed the case "with no findings." That means there was no fine for this breach and no corrective action.

"We were jumping up and down," he tells *RMC*. Notwithstanding the relief, there had been a tremendous amount of activity in the intervening two years, between investigating the incident internally, notifying patients and the public of the breach,

continued on page 7

Outsourced Providers Are a Growing Risk for Hospitals; More Oversight is Needed

Many hospitals have turned over one or more clinical units to management companies, but if they're used as a way to take a compliance breather, things could get messy. Without hospitals independently monitoring their outsourced service providers, they could miss potential problems with billing or quality of care—and there's always the risk that some hospitals will turn a blind eye because they are promised greater revenue. In addition to the risk of reputational harm, hospitals might land in a false claims lawsuit. Five hundred hospitals were already named in a big wound-care management case before they were dropped.

"You could have a great partner who lives up to everything they promised and that's the way it should be, but it won't be the case all the time," says Atlanta attorney Sara Kay Wheeler, with King & Spalding. "You always have to be showing the government that you are mindful of your risks. It's a good item to put on your risk assessment."

Hospitals use outsourced service providers—also known as managed units—when they may not have the expertise for a niched operation, such as wound care, inpatient rehabilitation, behavioral health, bariatric surgery and emergency rooms. Hospitals may outsource management of the department or enter into a joint venture with a vendor, Wheeler says. Either way, hospitals are not supposed to offload the oversight of billing, documentation, medical necessity and quality of care, says

continued

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Managing Editor
Nina Youngstrom
Nina.Youngstrom@hcca-info.org

Margaret Hambleton, vice president and chief compliance officer of Dignity Health in California, which has managed units throughout its system. "Because hospitals are buying the expertise, you rely on their expertise, but it can give you a false sense of security," Hambleton says. "Hospitals may forget they still have the obligation to evaluate whether they are truly providing the services they are contracted to provide."

Sometimes that's what happens, and it could open the door to overpayment or false claims liability for the outsourced service provider and/or the hospital or other health care organization. "I think this is a vulnerability because of the mindset," Wheeler says. "In many cases, there is a sense of relief when an experienced partner is engaged and that can lead to a relaxation in fastidious oversight of their performance."

Cases Are Out There

It's not a hypothetical risk, Wheeler says. There have been cases in this vein, including, most recently, the RehabCare false claims settlement. And now the Healogics wound-care case is working its way through the courts.

RehabCare, a rehabilitation therapy contractor, agreed in January 2016 to pay $125 million to settle false claims allegations that it allegedly caused skilled nursing facilities to overcharge Medicare (*RMC 1/18/16, p. 3*).

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by the Health Care Compliance Association, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. 888.580.8373, www.hcca-info.org.

Subscriptions to *RMC* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.hcca-info.org that include a searchable database of *RMC* content and archives of past issues.

To order an annual subscription to **Report on Medicare Compliance** ($764 bill me; $664 prepaid), call 888.580.8373 (major credit cards accepted) or order online at www.hcca-info.org.

Subscribers to *RMC* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

Some of RehabCare's SNF clients also resolved false claims allegations in connection with the false claims lawsuit, which alleged the rehab contractor (and its parent, Kindred Healthcare Inc.) played games with physical, occupational and speech therapy to increase SNF reimbursement, which resulted in claims for services that weren't reasonable or necessary or didn't happen. The SNFs that were supposedly enriched by the alleged scheme also settled million-dollar or multi-million dollar cases, including Wingate Healthcare Inc. and 16 of its facilities in Massachusetts and New York.

And now a false claims case is pending against Healogics, a Jacksonville, Fla.-based company that contracts with hospitals to run their wound-care centers. Three whistleblowers filed the lawsuit against the wound-care company, which alleged Medicare, Medicaid and TRICARE were overcharged for wound care. One is a former Healogics physician, another is a physician who had worked at a hospital with a Healogics contract and the third a former Healogics wound-care program director. While the whistleblowers originally named 500 partner hospitals in the complaint, the whistleblowers dropped the hospitals in subsequent amendments to the complaint.

According to the third amended complaint, Healogics allegedly "educated, trained, directed and otherwise ensured that its employees and contracted panel physicians did things the 'Healogics Way.'" That took three forms:

◆ Physicians employed in its wound-care centers allegedly were instructed to upcode more minor selective debridements to surgical/excisional debridement. "The more expensive procedure was billed regardless of the type of procedure that was actually performed," the complaint alleges.

◆ Eligibility for hyperbaric oxygen therapy (HBOT) allegedly was falsified to allow billing for the expensive treatment, which treats certain chronic, non-healing wounds. According to the complaint, Healogics allegedly "targeted each and every patient for conversion to HBOT. Healogics and its Partner Hospitals forced their staff to meet these HBO benchmarks, and thereby increase revenue and profits. In order to do so, Defendant had its employees or contractors manipulate patients' actual diagnoses or wound classifications in order to create false support for providing the expensive therapy."

◆ All patients allegedly were required to have a test called transcutaneous oxygen measurement (TCOM), which measures oxygen saturation in capillaries along extremities. "While there is increased revenue associated with the widespread unnecessary testing, Healogics' true objective was to use the TCOM tests to identify and

justify the more expensive HBO therapies," the complaint alleges.

Although the hospitals have been dropped from this lawsuit, they may surface in the next false claims case where the vendor is the hub and the government also pursues the spokes of the wheel. Wheeler figures that the Healogics case is a roadmap for lawsuits against hospitals based on alleged management-company misadventures. "You will see another wave of hospitals being pursued," she says. It's somewhat of a wake-up call for hospitals to scrutinize their vendors, Hambleton says, and it extends past wound care.

Marketing Can Be a Minefield

Sometimes hospitals get in trouble by allowing the management company to market the service line, Hambleton says. "That's a dangerous proposition," she notes. The management company may try to sell the hospital community outreach services and other vehicles to drum up patients. "Those incentives don't align very well with the purpose of the unit, which is increasing efficiency and quality of care," Hambleton says. "If the agreement suggests it will increase business on the unit, you will need to have significant oversight. I would say you shouldn't be doing that at all."

Contractors should be required to routinely audit their documentation, billing and quality of care, but independently eyeballing their performance is necessary, she says. Because the point of hiring them in the first place is filling an expertise gap, the hospital probably has to hire an external auditor "to validate what they're telling me from a clinical perspective," Hambleton says. The contract should also specify the "expectations and metrics" so they are "observable and measurable," she says. They should reflect the guidelines of medical societies in the clinical areas of the outsourced service lines.

The reason this is so important is that hospitals are using outsourced service providers in more areas, including telehealth, biomedical equipment and 340B drugs, says Shannon Sumner, consulting principal with Pershing Yoakley & Associates in Nashville. "You have to be cognizant if your organization is outsourcing more services to third parties because you may not have the resources in house," she says. "It's imperative the right people are on the bus before you enter these relationships." They include compliance, legal, nursing and risk management.

Consider a 'Basic Diagnostic'

With the use of so many outsourced service providers, it's a good idea for hospitals to put one or two arrangements on their work plan, Wheeler says. "Do a basic diagnostic," she suggests. Here are a few things to consider:

- How is the relationship structured? Is it a joint venture or a contract where the hospital pays the vendor a fee for managing? "There you are figuring out what percent of the liability you own," Wheeler says. "If you're just bringing in a manager, you own it all. If it's a joint venture, the hospital may be a majority owner or a minority owner and still have some type of liability."
- Structure won't matter if their patients are harmed in the managed unit, Wheeler says. Reputational harm hurts everyone when there's poor patient care. "If it's cobranded and the thing goes south and you only own 49%, it doesn't matter," she notes.
- Find out the obligations of your outsourced service providers. Are they required to audit and educate? Does the contract indemnify the hospital against losses in the event of fines and penalties? What happens if a compliance issue surfaces? If it's a joint venture, will the outsourced service provider inform the hospital about a subpoena? "You are trying to make sure you max out on communication and collaboration," Wheeler says.

The point is to demonstrate that outsourced service providers are in your risk assessment, Wheeler says. "If you are able to show you are thinking about outsourced service providers, it goes a long way on cutting down on intent and reckless disregard."

Contact Wheeler at skwheeler@kslaw.com, Hambleton at Margaret.Hambleton@DignityHealth.org and Sumner at ssumner@pyapc.com. ✧

Outpatient Billing Is Allowed for 'Separate' Inpatient-Only Procedures

It seems to be a well-kept secret that hospitals may collect some Medicare reimbursement for inpatient-only procedures even when they are performed on an outpatient basis. But hospitals have to get out of the mindset that they're doomed when patients aren't admitted for inpatient-only procedures, which leads them to write off the charges, one expert says.

Also, effective Jan. 1, CMS has provided hospitals with another way to bill Medicare for outpatient services when it's best to transfer a patient having an inpatient-only procedure.

Medicare pays for certain surgeries only when they are performed on inpatients. These procedures are on the inpatient-only list, which is updated annually in Addendum E of the outpatient prospective payment system (OPPS) regulation. When inpatient-only procedures pop up on outpatient claims, they are detected by hospital claim scrubbers. Here's where hospital poli-

cies may not serve their own self-interest, says Valerie Rinkle, president of Valorize Consulting. Instead of submitting the claims for what they believe will be a denial, hospitals write off the charges, figuring there's no point in billing for services that aren't covered, she says. There's no claim denial because Medicare never receives the claims. It's like the services were never performed, which deprives CMS of the data for future payment adjustments.

Even worse for hospitals, they are losing out on reimbursement, Rinkle says. There's an invitation for it embedded in the integrated outpatient code editor (IOCE), which is the software logic that CMS uses for OPPS claims. The IOCE says there are inpatient-only procedures designated as "separate procedures" that can be billed, and claims can be paid. "When done by itself, the procedure is denied as inpatient-only. But it also can be done as a separate procedure in support of another procedure that's not on the inpatient-only list and is payable under OPPS," Rinkle says. "You get the line item denied for the inpatient-only procedure because it was [performed] as outpatient, but you get a separate payment for other surgery that was outpatient."

How to Find the Special Codes

Unless hospitals read the fine print of the IOCE logic, "they won't know this exists," she says. It will take some detective work to find the inpatient-only procedures that qualify for reimbursement when they're performed on an outpatient basis but are payable under these circumstances, Rinkle says. Addendum E has the inpatient-only procedure list with 1,746 procedure codes and the status indicator for these procedures is C, and then a subset of 55 procedures on the inpatient-only list has the special definition of "separate procedure," she says. The only way to identify them is to look at the specifications that are spelled out as part of the IOCE logic and the associated Excel spreadsheet file that contains the subset of codes with this designation. They tie back to the definition of the codes in the CPT manual, Rinkle says. "These codes represent a procedure that can be done by itself," she explains. The Excel file has the file name Q_CD_HcpcsMap in the quarterly IOCE files found on the CMS website at http://tinyurl.com/gotcray (see box, p. 4, for a sample of the procedures with this designation).

For example, a patient undergoes a cystourethroscopy; with treatment of ureteral stricture (e.g., balloon

Example of Codes that Qualify as 'Separate Procedures'

Here are some of the inpatient-only procedure codes that may be separately payable under certain circumstances when the procedures are performed on an outpatient basis (see story, p. 3).

HCPCS	Description	Separate Procedure
21750	Repair of sternum separation	1
27005	Incision of hip tendon	1
27090	Removal of hip prosthesis	1
27140	Transplant femur ridge	1
27161	Incision of neck of femur	1
31725	Clearance of airways	1
32220	Release of lung	1
32225	Partial release of lung	1
32310	Removal of chest lining	1
33140	Heart revascularize (tmr)	1
33496	Repair prosth valve clot	1
33800	Aortic suspension	1
38100	Removal of spleen total	1
38101	Removal of spleen partial	1

Source: CMS

dilation, laser, electrocautery and incision), which is CPT 52341. The patient later has to return to the operating room for suture of a bleeding ureter, ureterorrhaphy, suture of ureter, which is CPT 50900. Although CPT 50900 is on the list of inpatient-only procedures, it's flagged as a separate procedure (i.e., the CPT description includes "separate procedure"), Rinkle says.

"Both codes would be on the claim," she explains. CPT 52341 is payable as an outpatient procedure, has a J1 status indicator and is assigned to comprehensive APC (C-APC) 5373. The national unadjusted payment rate is $1,644.60. The IOCE logic calls for denying only the line item with CPT code 50900, but Medicare will process the rest of the claim and the hospital will receive payment for C-APC 5373.

"If a provider writes off the claim before billing Medicare because CPT 50900 is on the inpatient-only list, then the provider will never receive the C-APC payment for CPT 52341," Rinkle says.

This isn't brand new. Hospitals, however, don't seem to know about the special category or fail to capitalize on it, she notes.

CA Modifier is Expanded

There is something new this year that also opens the door to more reimbursement related to inpatient-only procedures, Rinkle says. In the 2017 IOCE specification, CMS expanded the "special capture rule" and made it retroactive to Jan. 1, 2016. The special capture rule allows hospitals to bill Medicare for patients who received services in advance of an inpatient-only procedure but died before their admission, as long as hospitals append the modifier CA to the line item on the claim with the inpatient-only procedure code. Medicare will pay for the outpatient services reported on the claim under a C-APC, she says. Now the outpatient code editor says Medicare also will pay for the outpatient services if the patient is transferred before admission and received the inpatient-only procedure as long as hospitals put the CA modifier on the claim.

Hospitals Can Reopen Claims

One glitch: the definition of the CA modifier has not been updated elsewhere in Medicare guidance, Rinkle says. "No hospital will think to put modifier CA on patients who got transferred because they haven't changed the definition of the modifier," she says. Probably the software will accept the modifier on claims for patients who are transferred before admission for an inpatient-only procedure (e.g., the emergency room stabilized them and they are being transferred to another facility for higher-level care) and pay the claim, Rinkle says. Because the expansion to transferred patients is retroactive to last year, hospitals can reopen or file claims within the timely filing limit and say they have good cause on the grounds that they have new and material information, she says. For example, "three accounts where we did three inpatient-only procedures in the emergency room to stabilize the patients and transferred them to a hospital for a higher level of care" could be reopened.

The fact that there are potential revenue gains in changes to the IOCE language is often eye-opening to hospitals. "It illustrates Medicare is making significant policy changes in this very obscure technical document," she says.

Contact Valerie at valerie.rinkle@valorizeconsulting.com. Visit the CMS outpatient code editor page at http://tinyurl.com/gotcray. ✧

Finding by Auditor is Always 'Credible Information' Under 60-Day Rule

When providers receive a letter from a Medicare auditor or zone program integrity contractor (ZPIC) saying they owe money for a billing error, providers have to do more than write a check. The letter is "credible information" of an overpayment, setting in motion the Medicare 60-day overpayment refund rule, said attorney Scott Grubman.

"It's your responsibility to do your own internal investigation and report and refund, so the responsibility

CMS Transmittals and *Federal Register* Regulations
Feb. 17 - 23

Live links to the following documents are included on *RMC*'s subscriber-only webpage at www.hcca-info.org. Please click on "CMS Transmittals and Regulations."

Transmittals

(R) indicates a replacement transmittal.

Pub. 100-19, Demonstrations

- Episode Payment Model Operations, Trans. 169 (Feb. 17, 2017)

Pub. 100-20, One-Time Notification

- Preventing Hospice Notices of Election with Future Dates, Trans. 1799 (Feb. 17, 2017)
- ICD-10 Coding Revisions to National Coverage Determinations (NCDs), Trans. 1798 (Feb. 17, 2017)

Federal Register

Final Regulation

- Medicare Program; Advancing Care Coordination Through Episode Payment Models (EPMs); Cardiac Rehabilitation Incentive Payment Model; and Changes to the Comprehensive Care for Joint Replacement Model; Delay of Effective Date, 82 Fed. Reg. 10961 (Feb. 17, 2017)

shifts from CMS to the provider to do the heavy lifting after one of the audits is conducted," said Grubman, who is with Chilivis Cochran Larkins & Bever.

As soon as the audit letter comes in, the countdown starts on the time that providers have to investigate the purported billing mistakes. "Once providers receive credible information of possible overpayments, they must make a reasonable inquiry into the potential overpayment," according to CMS's February 2016 final regulation interpreting the 60-day rule (*RMC 2/15/16, p. 1*), which was mandated by the Affordable Care Act, he said. They also are required to look back six years, if the error dates back that far. That can take a while, but CMS gave providers up to six months from the day they receive the credible information to conduct an investigation. When the overpayment is confirmed and quantified, providers have an additional 60 days to report and refund the overpayment.

Appeals Give You a Break

Grubman noted, however, that providers can pursue appeals if they disagree with the findings, and that it's reasonable to hold off on the internal investigation under the 60-day rule until the appeal is resolved. According to the regulation, "If the provider appeals the contractor-identified overpayment, the provider may reasonably assess that it is premature to initiate a reasonably diligent investigation into the nearly identical conduct in an additional time period until such time as the contractor-identified overpayment has worked its way through the administrative appeals process."

External auditors, including recovery audit contractors, Medicare administrative contractors and ZPICs, are a clear source of credible information, Grubman said at a recent webinar sponsored by the Health Care Compliance Association. He said that credible information "is information that supports a reasonable belief that an overpayment may have been received."

There are other sources of credible information, but some of them are a judgment call. However, Grubman said, "there is never a time when [contractor audits] are not credible sources of information." There's a good chance, however, that the audit won't go back six years, as required by the regulation.

Suppose a physician practice receives a letter from a ZPIC that says it concluded that 75% of evaluation and management (E/M) services billed at level four in 2014 and 2015 should have been billed at level three. The physician practice may hire a consultant to analyze the coding using RAT-STATS, which is publicly available sampling and extrapolation software, Grubman said. Providers will look at claims before 2014 because the rule requires providers to look back six years, farther than the auditors may go, he said.

"You often have to [use sampling and extrapolation] because it's not feasible to audit every claim," he said. He emphasized it's necessary to document every step of the way because the overpayment reporting form requires providers to describe their statistical and extrapolation methodology. They can submit one form and attach a spreadsheet.

Here are other examples of credible information:

- Complaints come in to the hotline, subject to a "fact-based determination";
- An internal review turns up incorrect coding that led to additional reimbursement;
- Providers find out that a patient died before the date of service;
- Providers discover that services were performed by excluded or unlicensed people;
- Providers find overpayments after an internal audit;
- Providers learn of Stark and/or anti-kickback violations; and/or
- There's a substantial increase in Medicare revenue for no apparent reason.

Whatever the source of the credible information, providers are obliged to confirm or deny it. "The cornerstone of an internal investigation is reasonable diligence," Grubman said. Reasonable diligence includes both "proactive compliance activities conducted in good faith by qualified individuals to monitor for the receipt of overpayments and investigations conducted in good faith and in a timely manner by qualified individuals in response to obtaining credible information of a potential overpayment."

Deadline May Be Extended

After providers quantify overpayments, they should report and return them to Medicare contractors. The overpayment return package should include a cover letter that explains the reason for the overpayment and the check with the repayment amount. Providers may be able to extend the overpayment deadline past six months plus 60 days if there are extraordinary circumstances. According to the final regulation, if the HHS Office of Inspector General or CMS acknowledges receipt of your submission to their respective self-disclosure protocols, the 60-day countdown is on hold. It becomes moot if providers settle cases through the OIG Self-Disclosure Protocol or CMS's Self-Referral Disclosure Protocol, Grubman said. However, if they withdraw or are terminated from the protocol, providers then have 60 days to report and return overpayments.

Contact Grubman at sgrubman@cclblaw.com. ✧

OCR Closes Case of Stolen Flash Drive

continued from p. 1

conducting a risk assessment of the breach, submitting detailed information to OCR, discussing the event with senior leaders and the board, meeting with three OCR investigators and awaiting their conclusions.

The incident happened on a weekend in October 2015. A vendor's unencrypted flash drive went missing from a computer that was part of the vendor system in the lab. The flash drive contained about 2,000 patient names and codes that correspond to the test (not diagnosis codes). While the hospital used security tapes to try to figure out the fate of the flash drive—could they spot someone slipping it into their pocket? (no)—and interviewed employees and checked lab coat pockets, the privacy and security officers started the analysis of whether the theft rose to the level of a reportable breach, Kozik says.

The HIPAA Breach Notification Rule sets out a four-factor analysis. It states that "an impermissible use or disclosure of protected health information is presumed to be a breach" unless the covered entity or business associate determines there is a low probability the PHI has been compromised according to these factors: (1) "The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) The unauthorized person who used the protected health information or to whom the disclosure was made; (3) Whether the protected health information was actually acquired or viewed; and (4) The extent to which the risk to the protected health information has been mitigated."

It was a close call, says Alex Laham, information security manager. Nothing on the flash drive identified it as coming from Lawrence General Hospital. "There was no way to tie it back to the hospital and this is a hospital-rich state," Laham says. Also, the data was limited, with no diagnostic information. Still, the people in on the decision—including the compliance, privacy and security officers—"were on the fence," so they erred on the side of caution and reported it. After the internal investigation, the hospital sent OCR 110 pages of information in late fall 2015 and informed the affected patients, who were offered free credit-report monitoring.

Preliminary Checklist for Evaluation of Vendor Security Compliance

Here's a list of "third-party security considerations," says Alex Laham, information security manager at Lawrence General Hospital in Massachusetts. The questions can be considered when developing a HIPAA security vendor assessment. "Another useful tool is the SANS ISO 17799 Audit Checklist, which provides a framework for non-vendor specific security considerations. Depending on the vendor, your organization will need to tailor specific questions to ensure a complete understanding of risks and responsibilities," he says. Contact Laham at Alexander.Laham@lawrencegeneral.org.

- Is this vendor critical to your organization's function?
- What is the nature of the data the vendor, and its staff, will have access to? (i.e. No data, discrete or financial data, PHI/PII/SSN)
- If sensitive data is being exchanged, what is the vendor's information security program?
- Does the vendor have a HIPAA compliance program?
- Does the vendor have dedicated roles for Information Security, Privacy and Compliance?
- Does the vendor have the appropriate information security and HIPAA policies in place?
- Has a HIPAA security risk assessment been completed by the vendor?
- Does the vendor have compliance certificates such as SSAE-16?
- What data security practices does the vendor follow?
- What is the incident response/management process?
- Will vendor equipment be installed within your organization's environment?
- Who is responsible for servicing the equipment and patching software and how often is that done?
- Is anti-virus allowed or installed on the vendor equipment and who applies updates?
- Will the vendor's employees be accessing your network remotely?
- What are the access provision and termination standards for remote accounts?
- Do you monitor/log vendor access to systems?
- What is the process to address security concerns that may arise during the vendor's contract period?
- Will the vendor allow external party assessments such as penetrations tests and vulnerability scans?

The whole thing drove Laham a little crazy. "It was terrible timing," he says. "We were doing everything we were supposed to be doing." The hospital finished its risk assessment earlier that year. "It is probably one of the most daunting pieces an organization has to go through. It is an assessment of the threats, vulnerabilities and weaknesses and what we need to defend ourselves against and who is at the highest risk," he says. The hospital had identified unencrypted flash drives and was implementing a "lockdown policy where our ports could only use our flash drives," he says. An exchange program was set up so employees could switch out their flash drives for the encrypted version. That was being phased in, with higher risk areas taking priority over lower risk areas like the lab, which isn't high volume and doesn't have multiple users of guest stations. "We didn't do this indiscriminately," he says. "It was terribly frustrating" the presumed theft occurred as improvements were under way.

Site Visit Came as a Surprise

But there was a payoff. "With the volume of documentation we sent them and the onsite discussions, we were clear in identifying that we followed the appropriate process and this was on our radar we were actively addressing it," Laham says. "OCR did acknowledge that."

After sending OCR the packet of information, it was quiet for more than six months. Then, in July 2016, Kozik got a call from someone new at OCR who was taking over the case, and was surprised to hear a site visit was planned.

"We were baffled as to where this was heading," Laham says. "This didn't seem like an event that would require an onsite and where an onsite would typically happen." It seemed like OCR could have gotten the picture from the paperwork.

OCR said it wanted two days. Kozik pushed back a bit because that seemed excessive. They settled on parts of two days. Kozik found a place for the three OCR investigators to work and set up a phone. They walked through the lab, checking the physical security. Was the office and desk locked? Was the sign on the door that said "no re-entry" for real? The OCR investigators also privately interviewed seven employees, asked questions about policies and procedures and learned about the additional cameras the hospital had installed and the increased security guard rotations throughout the hospital.

Then the OCR investigators left and the waiting game began, as 2016 turned into 2017 without a word. Finally, seven months after the onsite visit, OCR's letter arrived.

Hospital Increased Vendor Auditing

No one knows what happened to the flash drive. It never surfaced, and there have been no reports of anyone abusing the information on it. Kozik speculates that, assuming the flash drive was stolen, the thief was unable to turn the PHI into cash. But the experience had some valuable lessons for the hospital. "We have to be way more vigilant about what comes in and what goes out through vendors," Laham says. "Managing our vendors and how they engage with us is the new focus for all the contracts we have."

The hospital has increased its auditing of vendor practices and employee practices vis-à-vis vendors. Policies may say one thing, but what are the vendors actually doing? Do employees follow vendor directions even if they conflict with hospital procedures? The lab theft "forced us to be more critical during our internal audits," Laham says.

Contact Kozik at Brian.Kozik@lawrencegeneral.org and Laham at Alexander.Laham@lawrencegeneral.org. ✧

NEWS BRIEFS

◆ **A New Jersey physician, his oncology practice and his practice manager (who also is his wife) agreed to pay $1.7 million to settle allegations they illegally imported and used unapproved chemotherapy drugs and billed Medicare for them,** the U.S. Attorney's Office for the District of New Jersey said Feb. 16. The Oncology Practice of Dr. Kenneth D. Nahum, Nahum, and Ann Walsh, of Colts Neck, allegedly violated the False Claims Act. Between April 1, 2010, and January 31, 2011, Walsh allegedly ordered chemotherapy drugs from a foreign distributor to use at Nahum's practice in Howell, N.J., and Wall, N.J., the U.S. attorney's office says. The drugs were not approved by the FDA for sale in the United States. "Doctors at the practice allegedly injected the drugs into their patients, and the practice then submitted claims to Medicare for reimbursement for the drugs and infusion services," the U.S. attorney's office says. Visit http://tinyurl.com/h45n3gj.

◆ **CORRECTION:** Skilled nursing facilities don't have to complete the certification within three days of admission, as was stated in the Feb. 20 issue of *RMC*. The regulation states that "Certifications must be obtained at the time of admission or as soon thereafter as is reasonable and practical" (42 CFR 424.20).