Report on
Medicare Compliance

Volume 26, Number 31 • September 4, 2017

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

Contents

Disaster Recovery Is Top of Mind After Harvey; Emergency Preparation Rule Looms

As Hurricane Harvey engulfed Houston and other parts of Texas and with hospitals facing a Nov. 16 compliance deadline for Medicare-Medicaid regulations on emergency preparedness, they are reminded that the stakes are high for their disaster recovery plans, although the perfect should not be the enemy of the good, compliance experts say. Hospitals may want to concentrate on backup plans for their mission-critical services, while accepting they may not be able to recover everything in the event of a flood, ransomware attack or other catastrophe.

"Disaster recovery planning is like an insurance policy," says Brian Kozik, chief compliance officer at Lawrence General Hospital in Massachusetts. "You hope you never need it." But without disaster recovery and business continuity plans, organizations may not be able to get on their feet after a man-made or natural disaster.

The hospital is developing and implementing a disaster recovery plan following the 3-2-1 model—"You need three copies of your data in two different formats and one of them should be offsite or, better yet, offline," says Alex Laham, information security manager. There are always limitations, however. If the hospital's backup storage location is walking distance from the hospital, it would be just as hard-hit in a natural disaster, Kozik says. And there will never be enough funding for disaster planning because it's expensive, and money is not necessarily a panacea.

continued on p. 5

OIG 'Early Alert': Abuse of SNF Patients Is Not Always Reported, Suggests CMS Fine Violators

Worried about abuse and neglect of Medicare beneficiaries at skilled nursing facilities (SNFs), the HHS Office of Inspector General on Aug. 28 released an "early alert" on new audit findings. The preliminary results of OIG's review of potential abuse or neglect indicate that hospitals and SNFs may not always report potential incidents of abuse or neglect, and that CMS lacks sufficient procedures to determine whether SNFs have reported them.

OIG suggested that CMS start enforcing civil monetary penalties against SNFs under Sec. 1150B of the Affordable Care Act, also known as the Elder Justice Act, which requires immediate reporting of potential abuse or neglect (in certain cases) to state survey agencies and law enforcement.

OIG audited the emergency room records of 134 Medicare beneficiaries with any of 12 diagnosis codes that explicitly indicate potential abuse or neglect, such as encounter for examination and observation following alleged adult rape (diagnosis code Z0441); adult physical abuse (99581); and adult sexual abuse, suspected, initial encounter (T7621XA). OIG also looked at surveyor reports for the SNFs where the potential abuse or neglect occurred. The findings: 74% of the medical records—100 of them—"contained indications, such as victim or witness statements and photographs, that the Medicare beneficiaries' injuries may have been caused by potential abuse or neglect at

continued

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

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

Copy Editor/Designer
Bill Anholzer
Bill.Anholzer@hcca-info.org

the SNFs," OIG said. However, there was no evidence in the hospital records that 38 incidents were reported to local law enforcement, even though the hospital medical staff is obligated to report under laws in all 50 states.

Potential criminal conduct, including neglect and abuse, must be reported to law enforcement under Sec. 1150B of the Elder Justice Act. The "covered individual"—an owner, operator, employee, manager, agent, or contractor of a long-term care facility that got at least $10,000 in federal funds during the prior year—is responsible for reporting.

The report suggested that CMS enforce 1150B, which includes penalties for violations, work with the HHS Secretary to get the authority to impose civil monetary penalties delegated to CMS, and adopt procedures to compare Medicare claims for ER treatment with claims for SNF services to flag potential abuse or neglect of Medicare beneficiaries in SNFs and share the details periodically with survey agencies.

The report is a good opportunity for hospitals and SNFs to improve training on their reporting obligations, says former federal prosecutor David Hoffman, president of David Hoffman & Associates in Philadelphia. "Compliance officers should focus on the training of abuse and neglect and what it means, and timely reporting of abuse and neglect to the appropriate entities under the Elder Justice Act and state statutes," he says.

An Oct. 4, 2016, Medicare-Medicaid regulation from CMS reforming requirements for long-term care facilities, which are required to "investigate and report all allegations of abusive conduct," refined what constitutes neglect, Hoffman says. For example, outside service providers have been added to the definition of people and entities that will be held responsible for "neglect" if they fail to do their job. It's no longer delegated away, Hoffman says.

Why isn't reporting up to snuff? According to the OIG report, there are holes in CMS's oversight. "CMS officials informed us that they do not match Medicare claims for reimbursement of emergency room services with claims for reimbursement of SNF services to identify instances of potential abuse or neglect," OIG said. And there haven't been any consequences for SNFs that don't report potential abuse or neglect. "CMS has not taken any enforcement actions using section 1150B of the Act or used the penalties it contains since its effective date of March 23, 2011, to ensure SNF employees report incidents of potential abuse or neglect," OIG said. The reason: the HHS Secretary hasn't delegated enforcement to CMS, and it has not found any cases where covered individuals didn't report potential abuse or neglect. CMS also said the State Operations Manual wasn't updated to reflect Sec. 1150B until March 8, 2017, with an effective date of November 28, 2017. However, CMS said it issued a State Survey Agency Directors' Letter (S&C-11-30-NH) on June 17, 2011, with 1150B reporting requirements and sanctions and instructions consistent with CMS and state policies and procedures.

OIG: 'Findings Are So Significant'

"CMS officials stated that they have taken additional actions to protect residents in nursing homes by adding section 1150B requirements to training courses and issuing supporting interpretive guidance and training to surveyors," OIG said.

OIG's final report will come out in the fall of 2018, OIG spokeswoman Katherine Harris says. The reason OIG released the "early alert" is because "the findings are so significant regarding the beneficiaries' well-being" that OIG wanted to communicate them to CMS and raise general awareness as soon as possible, she says. Meanwhile, the incidents of possible patient abuse or neglect identified in the audit have been referred to OIG's Office of Investigations and state Medicaid fraud control units, Harris says.

Hoffman also thinks more attention should be paid to what happens after reports are filed. "We need to ensure that those receiving the reports on the law enforce-

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.

ment end are trained appropriately to ensure a thorough investigation," he says. For example, sexual assault is "underreported and explained away." While long-term care facilities shouldn't ban sexual contact between residents, "they need to evaluate consent and make it clear who can and can't consent," Hoffman says.

Contact Hoffman at dhoffman@dhoffmanassoc.com. View the early alert at https://go.usa.gov/xR79T and the Medicare-Medicaid regulation at http://tinyurl.com/zeub972. ✧

With First Diagnosis the Easy Path, Drop-Down Menus Invite Error

If a physician documents a patient's diabetes retinopathy in the chart but then chooses the first diagnosis in the drop-down menu of the electronic medical records—diabetes mellitus with peripheral neuropathy—there's a good chance the code will be wrong.

But that's happening in some physician offices and hospitals, says Michele Bohley, a specialist leader with Deloitte Advisory, and Dee DiMauro, a specialist senior.

Drop-down menus are a documentation shortcut in electronic medical records. They help physicians pick the most appropriate diagnosis for their patients, and like other documentation shortcuts, such as copy/paste *(RMC 9/7/15, p. 1)*, they are inviting coding errors, Bohley and DiMauro say. "Physicians are usually picking the first diagnosis on the drop-down menu," DiMauro says. "The first one listed may not be what the doctor is diagnosing. It's a coding error and may not meet medical necessity depending on what the doctor is treating the patient for."

Drop-down menus have a list of diagnoses that correspond to the ICD-10 code. It's designed to be efficient, but some compliance problems have emerged.

The major risk: physicians select an inaccurate or nonspecific diagnosis, Bohley and DiMauro say. Some physicians take the path of least resistance: picking the first diagnosis or the closest related diagnosis if they're unable to find the diagnostic statement they would like to document because the dropdown or scroll list may be long, hard to read or decipher due to abbreviations, or lack a complete list of diagnoses. Add to that the need to complete the documentation quickly in order to see the next patient, and the risk of coding errors increases.

The text box in the drop-down menu may not be long enough to accommodate the description of the diagnosis code, Bohley and DiMauro say. If the electronic medical record system was set up to accommodate 30 characters, diagnoses with long descriptions will be shortened or abbreviated. That may lead to the physician misinterpreting the description and selecting the incorrect code.

"The limited number of characters allowed in the descriptions hinder the physician from picking the correct diagnosis because the descriptions may not be specific enough to the individual codes," DiMauro says.

Space runs out quickly with the specificity demanded by ICD-10. For example, a compound fracture of your wrist bone on the right side has to be described in a fair amount of detail, including laterality (i.e., right or left sides)—"fracture, radius, greenstick, right side," DiMauro says. "You could see where we run out of characters, so characters drop off the menus." As a result, some electronic medical record systems have abbreviations that are now clinically accepted. For example, instead of spelling out fracture or laterality, they put "fx" for fracture or "rt" for right. But not all descriptions have been shortened.

Bohley and DiMauro suggest hospitals look at clinical descriptions approved by the American Medical Association and determine whether to adopt them.

Contact Bohley at mbohley@deloitte.com and DiMauro at ddimauro@deloitte.com. ✧

Hospitals Face Meaningful-Use Cost Report Audits, New OIG Reviews

Whether or not hospitals have escaped a meaningful-use audit from CMS's outside contractor, Figliozzi and Co., it probably won't be long before their cost reports are audited for the accuracy of payments from the electronic health record (EHR) incentive-payment program. Medicare administrative contractors (MACs) are required under the HITECH Act to audit cost reports and adjust meaningful-use payments based on the payment variables reported. That's on top of the audits hospitals are facing from the HHS Office of Inspector General, which added EHR incentive payments in July to its 2017 Work Plan.

"MACs are a couple years behind," says Mike Orr, a director at BKD LLP in Waco, Texas. But audits delayed are not necessarily audits denied. The good news for hospitals, however, is they might wind up receiving a check from Medicare after a HITECH cost-report audit, says Travis Skinner, a senior managing consultant at BKD. It's possible they are not getting credit on their cost reports for days associated with Medicare Advantage patients and charity care, and audit findings could be in their favor. But how the audits go depends, as always, on the quality of hospitals' documentation and the search for potential missing Medicare Advantage days, Orr and Skinner say.

The EHR incentive program—created by the HITECH Act in the 2009 stimulus law—used carrots and sticks to get providers on board with the technology. Hospitals and physicians started receiving Medicare and Medicaid bonuses for becoming meaningful users of certified EHR technology in 2011 and paying penalties if they weren't. To get incentive payments, hospitals and physicians have to answer some yes/no questions about their use of EHRs to satisfy meaningful-use objectives, enter some data on the objectives, agree to keep all required documentation and sign an attestation that it's all true. Compliance is evaluated after the fact—by audits. So far, hospitals and "eligible professionals" (e.g., physicians) have received almost $36 billion in meaningful-use money (see http://tinyurl.com/ycjtdtlk). Although payments are winding down and eligible-professional objectives are being absorbed into the Merit-Based Incentive Payment System (MIPS) of the Medicare Access and CHIP Reauthorization Act (MACRA), hospitals and physicians "have to continue moving forward with Stage 3 of meaningful use," Skinner says, and audits will continue.

The HHS Office of Inspector General has been auditing meaningful-use compliance and in June reported that "eligible professionals" were overpaid $729 million between May 2011 and June 2014 *(RMC 6/19/17, p. 5)*. OIG is turning next to hospitals, which also are audited by Figliozzi and Co. (*RMC 2/15/16, p. 1; 4/18/16, p. 1*). The Work Plan states that OIG will audit the $14.6 billion paid to hospitals in Medicare EHR incentives between 2011 and 2016.

MACs Reopen Cost Reports for Meaningful Use

And then there are the HITECH cost-report audits. Every EHR incentive payment received by a hospital will face a desk review, in-house audit or on-site audit, Orr says. The MACs aren't interested in attestations or the percentage of patients who received prescriptions electronically, for example. MACs look at the nine variables that drive payment, including inpatient days, total managed care days and charity care charges, and whether they're consistent with the amount of the EHR incentive payment received by the hospital during the reporting period, Orr and Skinner say.

But a lot of cost-report settlements are out there that have not gone through HITECH audits, Orr says. Because there's no way CMS is going to leave money on the table, hospitals should brace for these audits. In fact, "MACs have reopened cost reports just to do HITECH audits," Orr says. That means hospitals are not in the clear just because they have received a notice of program reimbursement from the MAC.

HITECH audits might have been delayed because MACs have been waiting for CMS's final instructions on the S10 worksheet, which they were hoping would clarify reporting of presumptive charity care. The more charity care that's provided by a hospital, the higher its incentive payment, Orr and Skinner say. As it turned out, the S1 guidance shed light on bad debt but not on charity care, they say.

Hospitals may find themselves receiving a check from MACs after a HITECH audit if they're not including all their Medicare Advantage (Part C) patient days on their cost reports, Orr and Skinner say. Hospitals are supposed to "shadow bill" Part C stays (also known as Medicare HMO days or information-only claims). That ensures they get credit on cost reports for inpatient days of Medicare Advantage patients, even though they don't submit Part A/B claims to MACs for them because hospitals are paid directly by the Medicare Advantage plans. Because the claims don't show on the standard inpatient report for the Provider Statistical & Reimbursement (PS&R) report, hospitals have to specifically bill these claims to their MAC to capture the claims for cost-report purposes and EHR and graduate medical education reimbursement purposes.

"When EHRs came along, the Part C days were added to the meaningful-use formula and they have the exact same value as a Part A day," Orr says. But he has found both small and large hospitals aren't shadow billing all or many of their Part C days, and as a result they lose out on meaningful-use money. However, that can be rectified during cost-report audits and is an opportunity for more incentive payment.

Contact Skinner at tskinner@bkd.com and Orr at morr@bkd.com. ✧

CMS Transmittals

Aug. 25 - 31

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

Transmittals

(R) indicates a replacement transmittal.

Pub. 100-04, Medicare Claims Processing Manual

- Inpatient Rehabilitation Facility (IRF) Annual Update: Prospective Payment System (PPS) Pricer Changes for FY 2018, Trans. 3849 (Aug. 25, 2017)
- Quarterly Healthcare Common Procedure Coding System (HCPCS) Drug/Biological Code Changes — October 2017 Update, Trans. 3850 (Aug. 25, 2017)
- October 2017 Integrated Outpatient Code Editor (I/OCE) Specifications Version 18.3, Trans. 3852 (Aug. 25, 2017)
- October 2017 Update of the Hospital Outpatient Prospective Payment System (OPPS), Trans. 3853 (Aug. 25, 2017)

Developing a Disaster Recovery Plan

Here are things to consider when developing a disaster recovery plan, according to Alex Laham, information security manager at Lawrence General Hospital in Massachusetts. Contact him at alexander.laham@lawrencegeneral.org.

Disaster Recovery Planning Outline

	Tasks	Rationale
1) Analysis and Data Gathering	• Business Impact Analysis • Risk Assessment • Application and Data Stratification	Analysis helps to identify the threats to your IT environment; what data is most critical to business function and which systems must be restored in a timely manner to support data requirements.
2) Recovery Strategies	• Methods of Storage and Recovery • Recovery Time Objective • Recovery Point Objective	Utilizing the 3-2-1 Backup rule and analysis data to determine how many copies of data should be stored, on what types of media and in what storage locations. *Disconnected/offline storage is also recommended for ransomware defense.
3) Policies, Standards, Communication	• Disaster Recovery Policy • Disaster Recovery Procedure • Disaster Recovery Plan • Communicate with involved parties	Once the technical backup processes have been established, the detailed policy, procedure and plan can be developed to outline the who, what, when, where and how disaster recovery will be enacted.
4) Plan Testing	• Develop testing plan • Test recovery process • Train required staff	To determine that the backup process has been setup appropriately to fulfill its intended purpose, testing plans are to be developed and backup tests performed.
5) Update Plan	• Track changes in volume requirements, threats and technologies.	As businesses (networks) expand, threat models change and data sources/volumes fluctuate; backup plans will need to be adjusted to meet those changing demands.

Stakes Are High for Disaster Recovery

continued from p. 1

Money only went so far when it came to the torrential rains that hit southeast Texas in late August. Texas Medical Center, which calls itself "the largest medical complex in the world," invested $50 million in infrastructure improvements, including a submarine door, after its hospitals were devastated by Tropical Storm Allison in 2001, according to news reports. But the hospitals were not immune to Harvey. Ben Taub Hospital's basement flooded, and it had to abort a plan to evacuate most patients; MD Anderson Cancer Center and Memorial Hermann had to cancel treatments.

Two hours from Houston, Baptist Hospital Beaumont was forced to evacuate about 200 patients after the city water supply went down, according to news reports.

Meanwhile, because of Harvey, on Aug. 30, HHS Secretary Tom Price waived sanctions and penalties against hospitals in Texas and Louisiana if they don't comply with certain requirements of the HIPAA Privacy Rule, including getting the patient's permission to speak to family members or friends involved in the patient's care and giving out a notice of privacy practices (see http://tinyurl.com/ya7oraej). CMS has waived certain administrative requirements in the two states, including the three-day inpatient hospital stay mandated before Medicare coverage kicks in for skilled nursing facility admissions.

90,000 Phishing Emails Were Filtered in a Week

The urgency of disaster recovery planning has been growing in the past two years as dependence on electronic health records dovetails with the exponential growth of ransomware, which is hostage-taking of electronic health records (EHRs) by cybercriminals in exchange for payment *(RMC 6/5/17, p. 3)*. "Disaster recovery was always an important part of IT and corporate strategy, but with the destructive nature of ransomware, disaster recovery has pushed its way to the forefront," Laham says. There were two ransomware attacks—WannaCry and NotPetya—that spread to 150 countries, "and we had over 90,000 spam and phishing emails filtered over the past week, so the impact of a storm, while devastating to certain locations, does not necessarily rise to everyone's minds as the primary threat"—unless it's a natural disaster of the magnitude of Harvey, Hurricane Katrina in New Orleans, or Hurricane Sandy in New York and New Jersey. There are also potential internal threats from

continued on p. 7

CMS Emergency Preparedness Requirements by Provider Type

This is an excerpt of a chart CMS prepared of some of the requirements in its emergency preparedness regulation for 17 provider types. It takes effect Nov. 16. View the chart at http://tinyurl.com/zolagv3. View the regulation at http://tinyurl.com/ydfeh8ue. View an emergency preparedness checklist at http://tinyurl.com/yb2twygk.

Inpatient					
Provider Type	**Emergency Plan**	**Policies and Procedures**	**Communication Plan**	**Training and Testing**	**Additional Requirements**
Hospital	Develop a plan based on a risk assessment using an "all hazards" approach, which is an integrated approach focusing on capacities and capabilities critical to preparedness for a full spectrum of emergencies and disasters. The plan must be updated annually.	Develop and implement policies and procedures based on the emergency plan, risk assessment, and communication plan which must be reviewed and updated at least annually. System to track on-duty staff and sheltered patients during the emergency.	Develop and maintain an emergency preparedness communication plan that complies with both federal and state laws. Patient care must be well-coordinated within the facility, across health care providers and with state and local public health departments and emergency systems. The plan must include contact information for other hospitals and CAHs; method for sharing information and medical documentation for patients.	Develop and maintain training and testing programs, including initial training in policies and procedures and demonstrate knowledge of emergency procedures and provide training at least annually. Also annually participate in: • A full-scale exercise that is community- or facility-based; • An additional exercise of the facility's choice.	Generators—Develop policies and procedures that address the provision of alternate sources of energy to maintain: (1) Temperatures to protect patient health and safety and for the safe and sanitary storage of provisions; (2) Emergency lighting; and (3) Fire detection, extinguishing, and alarm systems.
Critical Access Hospital	*	*	*	*	Generators
Long-Term Care Facility	Must account for missing residents (existing requirement).	Tracking during and after the emergency applies to on-duty staff and sheltered residents.	In the event of an evacuation, method to release patient information consistent with the HIPAA Privacy Rule.	*	Generators Share with resident/family/representative appropriate information from emergency plan.

*Indicates that the requirements are the same as those for hospitals. Exceptions are noted for individual provider/suppliers.

NOTE: This table is an overview of the regulation with key differences summarized. This is not meant to be an exhaustive list of the requirements nor should it serve as substitute for the regulatory text.

employees, who may delete data (accidentally or not) or corrupt or steal it.

"Every day we are defending the organization from multiple attacks," he says. "Had we not had some sort of defense in place, the organization would be compromised."

Because disaster recovery planning is expensive, Laham says it's not something organizations do "in one fell swoop. You attack what you can and have money for, and defend against the biggest threats you have."

For example, Laham is prioritizing the mission-critical departments in the event the electronic health record system fails. That means determining which services need to come back online the fastest—and how much time each of these departments think they can be offline without posing a risk to patient safety. He has been focusing on pharmacy, lab, radiology and the nursing units. They list all the services they provide and the software they use and "rate them on how long they could be without the services until you reach critical mass," Laham says. For example, how long could nurses run on paper documentation before it becomes too hard to manage patient care? Four hours? One day? "We are used to electronic medical records, and communication among departments breaks down without them," he explains.

Then you roll up the responses of individual departments into a larger impact analysis. If most departments in a hospital are using the same EMR system and they all list it as critical, "that's how you start stratifying and weed out what is most critical and less critical for the organization as a whole," he says.

It's challenging because "you have to be willing to not recover some things," Laham says. "You want to recover everything, but you can't. What is not essential to survivability" may have to be set aside.

Hospital Communicates in More Ways Than One

Preparing employees for a disaster that takes out their computers or worse is essential. Lawrence General Hospital learned employees often don't get the message about IT disruptions even when they are warned repeatedly. "Even if we send out 15,000 emails saying we will have downtime, there always seem to be some people who say, 'I didn't know this was happening,'" Laham says. "When IT goes down, everything grinds to a halt and people freak out." So the hospital has multiple communication channels to ensure employees are informed. They include text messaging through a third-party service, an overhead call system, department leaders giving updates as part of the standard emergency department plan and computer alerts that come up in a banner.

Lawrence General Hospital went with a multipronged approach to disaster recovery planning. It uses cloud storage for some EMR databases. "We have an offsite contracted disaster-recovery site that provides us with a separate location for the storage of data. They have generators, backup batteries, water cooling and a connection back to that data if we need to pull it off from here or we need to go to the facility and pull it there," Laham says.

The 3-2-1 recovery process applies regardless of the reason for the loss of data. "You need three copies of your data in two different formats and one of them should be offline," Laham says. One copy of data should be in a primary location, one in a secondary location and one in a cloud. The two different formats could be actual tape and an electronic version. Preferably, one set of data isn't connected to the Internet. The reason for the 3-2-1 methodology is to give organizations flexibility in responding to all types of threats. If the hospital is the victim of ransomware, it would wipe all data. If the threat were internal, maybe they can just replace a drive.

Even when hospitals can bring back their data after a flood or other disaster, it has to be turned into useable data, Laham says. "Logistically, it's very messy. It's a large process because you have a lot of what-ifs: if the computers are functional, if you have power, if you are able to pull data from the cloud to a host system, then you can generally get your information back," he says. "Part of the disaster recovery process is planning pathways to get the data back and access it."

The hospital also used a vendor for its IT HIPAA security risk assessment. The vendor looked at the information security program components, including disaster recovery, and made recommendations on how to improve security posture in relation to industry standards. Laham asked for sufficient funds to mitigate the risks and is hoping to get at least half the amount requested. The full amount would have been better, "but with half, he can do a decent job," Kozik said.

A corollary of disaster recovery was mandated by CMS, which published a final regulation Sept. 16, 2016, on emergency preparedness for 17 types of Medicare and Medicaid providers and suppliers. The purpose of the regulation is to "establish national emergency preparedness requirements to ensure adequate planning for both natural and man-made disasters, and coordination with federal, state, tribal, regional and local emergency preparedness systems," CMS said. It requires policies and procedures, risk assessment, a communications plan, training and testing, and will be embedded in the conditions of participation (see box, p. 6).

Contact Kozik at brian.kozik@lawrencegeneral.org and Laham at alexander.laham@lawrencegeneral.org. View the emergency preparedness regulation at http://tinyurl.com/ydfeh8ue. ✧

NEWS BRIEFS

◆ **Christus St. Vincent Regional Medical Center in Sante Fe, N.M., and its partner, Christus Health, agreed to pay $12.24 million to settle false claims allegations over donations to county governments, the Department of Justice said Sept. 1.** The donations were used to pay for the state share of Medicaid payments to the hospital, DOJ alleged. Under New Mexico's Sole Community Provider (SCP) program, which ended in 2014, supplemental Medicaid funds were provided to hospitals in mostly rural communities. The federal government paid back the state for about 75% of its health care spending under the SCP program, DOJ says. According to federal law, New Mexico's 25% matching share of SCP payments had to come from state or county funds and not "donations" from private hospitals, DOJ explained. "This restriction on the use of private hospital funds to satisfy state Medicaid obligations was enacted by Congress to curb possible abuses and ensure that states have sufficient incentive to curb rising Medicaid costs," according to DOJ. "Between 2001 and 2009, St. Vincent and CHRISTUS allegedly made non-bona fide donations and thus caused the presentment of false claims by the state of New Mexico to the federal government under the Medicaid program." The lawsuit originated with a whistleblower. Visit www.justice.gov.

◆ **CMS has developed a home health review tool that it says may help home health agencies avoid the common reasons for claim denials.** Visit http://tinyurl.com/y7dksv57.

◆ **Fox Rehabilitation in New Jersey, one of the largest outpatient therapy providers in the country, was overpaid more than $29 million between July 1, 2013, and June 30, 2015, the HHS Office of Inspector General said in a new report.** OIG selected a random sample of 100 Medicare claims submitted by Fox Rehabilitation and hired an independent medical review contractor to audit the medical records for compliance with medical necessity, documentation and coding requirements. The findings: 85 claims had therapy services that weren't medically necessary, one claim didn't comply with documentation requirements, and another claim didn't meet coding rules. "On the basis of our sample results, we estimated that Fox improperly received at least $29,902,452 in Medicare reimbursement for outpatient therapy services that did not comply with certain Medicare requirements," OIG asserted. In a written response, Fox said it doesn't agree with OIG's recommendation that it refund the $29.2 million, and that Fox's outside statistical expert, Frank Cohen, found the method of extrapolation "critically flawed." Read the report at https://go.usa.gov/xRA3g.

◆ **The HHS Office of Inspector General gave the green light to a plan for a preferred hospital network to give $100 premium credits to patients who are Medigap policyholders even though co-insurance waivers could run afoul of the anti-kickback statute.** The requestors of the advisory opinion offer Medigap policies, which supplement Medicare. They have an agreement with a preferred hospital organization (PHO) to discount up to 100% of the inpatient deductibles incurred by the Medigap policyholders. "Requestors return a portion of the savings resulting from the Arrangement directly to any Policyholder who has an inpatient stay at a Network Hospital in the form of a $100 credit toward a future renewal premium," the opinion explained. Although OIG noted that waivers of beneficiary coinsurance and deductibles violate the anti-kickback law and this arrangement doesn't earn the protection of a safe-harbor, OIG won't impose sanctions on the requestors because "it poses no more than minimal risk of fraud and abuse." The discounts and premium credits won't affect per-service Medicare payments, and the arrangement probably won't increase utilization or "unfairly affect" hospital competition or influence medical judgment. Visit https://go.usa.gov/xRsa7.

◆ **Most accountable care organizations (ACOs) in the Medicare Shared Savings Program reduced Medicare spending during the first three years of the program, the HHS Office of Inspector General said in a report posted Aug. 29.** "The net reduction in spending across all ACOs was about $1 billion," the report states. OIG said 428 ACOs served 9.7 million Medicare beneficiaries the initial three years, although they operate in some states more than others. OIG noted, however, that it didn't independently confirm the data it got from CMS on spending, utilization, shared savings and the quality scores. Read the report at https://go.usa.gov/xRA3D.