G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

January 2017

INSIDE THIS ISSUE

Forget 2014: New Discussion Paper Outlines FDA's Current Thinking on LDT Regulation 1

Enforcement Firsts: Presence Health Fined $475,000 for Taking Too Long to Report HIPAA Breach 1

By the Numbers: DOJ Touts 2016 as Bumper Year for False Claim Act Recoveries 2

COMPLIANCE PERSPECTIVES:
How to Create a HIPAA Breach Notification Policy 5

Quiz: Is Offering Free Labelling Services to Dialysis Facilities a Kickback? 11

www.G2Intelligence.com

Upcoming Events

Conference:
Lab Institute 2017
October 25-27
Hyatt Regency Washington on Capitol Hill, Washington, DC
www.labinstitute.com

Forget 2014: New Discussion Paper Outlines FDA's Current Thinking on LDT Regulation

In December, the U.S. Food and Drug Administration ended two years of anticipation or dread, depending on your point of view, by announcing that it would not finalize the guidance on agency oversight of laboratory developed tests (LDTs) that it proposed back in 2014—at least not yet. Instead, the FDA said it would work with the new administration and Congress "to get our approach right."

With that in mind, on Jan. 13, 2017, the agency issued a discussion paper summarizing the public feedback it has received on the 2014 draft guidance and outlining the key features of a possible alternative approach to FDA regulation of LDTs. Here is an overview of the key points from the new discussion paper.

Continued on page 10

Enforcement Firsts: Presence Health Fined $475,000 for Taking Too Long to Report HIPAA Breach

Patient health information breaches—whether from hacking, glitches or just plain old carelessness—remain an all too common occurrence in labs and other health care institutions. A new HIPAA rule took effect in 2013, requiring providers to furnish timely notification of such breaches. And on Jan. 3, a large Illinois health system named Presence Health became the first provider penalized for failing to meet those notification requirements.

The Rule

Under the HIPAA rule, providers must furnish notification of breaches to three sets of recipients:

1. The HHS Office for Civil Rights (OCR);
2. The individuals affected by the breach; and
3. The media (if the breach affects 500 or more individuals).

The deadline for notification: within 60 days of discovering the breach.

Continued on page 2

Enforcement Firsts: Presence Health Fined $475,000, *from page 1*

What Happened

On Oct. 22, 2013, Presence discovered that paper-based OR schedules for one of its surgery centers had been removed from the files. The missing records listed personal health information of 836 individuals, including names, birth dates, medical record numbers, dates and types of procedures received and anesthesia administered.

It was a breach requiring notification under the HIPAA rule. The good news is that Presence did send out all of the required notices. The bad news is that it do so only well after the 60-day deadline had expired:

Notice Recipient	Notice Due Date	Actual Notice Date	Days Late
OCR	Dec. 22, 2013	Jan. 31, 2014	41
836 individual patients	Dec. 22, 2013	Feb. 3, 2014	44
Media outlets	Dec. 22, 2013	Feb. 5, 2014	46

The Case

The OCR charged Presence with a separate HIPAA violation for each one of the notices that was late (as well as additional violations committed later on that were discovered during the investigation). Faced with potential liability in the millions, Presence decided to settle the claims. The price tag: $475,000 and the promise to adopt a Corrective Action Plan (CAP) implementing measures to prevent future violations.

Takeaway: Based on the settlement agreement, it appears that Presence understood and made earnest efforts to comply with its breach notification obligations. Unfortunately, it took too long to do so. Although it is not clear why the notices were late, what can be said with confidence is that implementing clear and specific rules and timetables for responding to and reporting data breaches is crucial to ensure compliance with HIPAA breach notification requirements.

G2CA

Kelly A. Hardy, JD, Editorial Director

Glenn S. Demby, Editor

Catherine Jones, Contributing Editor and Social Media Manager

Barbara Manning Grimm, Managing Editor

David van der Gulik, Designer

Randy Cochran, Corporate Licensing Manager

Myra Langsam, Business Development

Michael Sherman, Director of Marketing

Jim Pearmain, General Manager

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

G2 Compliance Advisor (ISSN 2332-1474) is published by G2 Intelligence, Plain Language Media, LLLP, 15 Shaw Street, New London, CT, 06320.
Phone: 1-888-729-2315
Fax: 1-855-649-1623
Web site: www.G2Intelligence.com.

BY THE NUMBERS

DOJ Touts 2016 as Bumper Year for False Claim Act Recoveries

The False Claims Act (FCA) remains the federal government's most potent fraud enforcement tool. After sagging a tad in recent years, FCA recoveries bounced back in fiscal year 2016. As usual, the health care industry was responsible for the lion's share of the money. Here are the key numbers from the year in FCA recoveries as reported by the U.S. Department of Justice (DOJ) on Dec. 14.

- **$4.7 billion:** Total FCA recoveries in FY 2016, the third highest in history;
- **$2.5 billion:** Total recoveries against health care providers in FY 2016 (not including state Medicaid);

The False Claims Act remains the federal government's most potent fraud enforcement tool.

- **$31.3 billion:** Total FCA recoveries between 2009-2016;
- **$4 billion:** Average annual FCA recoveries between 2009-2016;
- **$19.3 billion:** Total FCA recoveries from health care providers between 2009-2016;
- **$2.4 billion:** Average annual FCA recoveries from health care providers between 2009-2016;
- **702:** Total *qui tam* (whistleblower) lawsuits filed in FY 2016, an average of 13.5 cases per week;
- **$2.9 billion:** Total recoveries in *qui tam* lawsuits in FY 2016;
- **$519 million:** Total recoveries paid to whistleblowers in FY 2016.

Top 5 FCA Health Care Recoveries

The biggest FCA recovery against a lab for the year was the $260 million paid by Millennium Health (formerly Millennium Laboratories) to settle charges of billing unnecessary urine and genetic tests and giving free items to physicians to induce referrals of costly tests. The complete Top 5:

1. **Wyeth and Pfizer:** $1.2 billion for allegedly reporting false and fraudulent prices on drugs used to treat acid reflux;
2. **Novartis Pharmaceuticals Corp.:** $390 million for allegedly paying kickbacks to specialty pharmacies in exchange for recommending the drugs Exjade and Myfortic;
3. **Tenet Healthcare Corp.:** $244.2 million for allegedly paying kickbacks to physicians in return for referral to four Tenet hospitals;
4. **Millennium Health:** $260 million for alleged false billing of urine and genetic tests and paying kickbacks to physicians;
5. **RehabCare Group Inc., RehabCare Group East Inc. and parent company Kindred Healthcare Inc.:** $125 million for allegedly inducing skilled nursing homes to falsely bill Medicare for rehab services that were not medically necessary or provided at all.

Beyond the Numbers

The DOJ FY 2016 FCA report is noteworthy not just for the numbers but the enforcement trends it cites, including:

Voluntary Compliance: U.S. Health and Human Services Inspector General Daniel R. Levinson emphasized that the big dollar values belie the "collateral benefits" achieved via "voluntary observance of federal laws through corporate integrity agreements addressing compliance weaknesses and self-disclosures that encourage health care providers and other entities to voluntarily report suspected violations."

Executive & Individual Accountability: The DOJ also continued its determination to go after not just entities but the individuals running them in pursuit of the policy announced in the September 2015 Yates memorandum. Of the 11 individuals the DOJ cites as being held personally liable for alleged false claims in 2016, nearly half were connected with laboratory testing, including:

- Dr. Jonathan Oppenheimer, a former executive with a Nashville drug testing laboratory who agreed to a $9.35 million settlement;
- Gottfried and Mieke Kellerman, founders of Pharmasan Labs, Inc. and NeuroScience, Inc., who settled for $8.5 million;
- Dr. David G. Bostwick founder and former owner and CEO of Bostwick Laboratories, who entered into a $3.75 million settlement; and
- Dr. David Spellberg and Robert A. Scappa, urologists who settled allegations of billing Medicare for medically unnecessary fluorescence in situ hybridization, (FISH) testing.

False Claims Act Recoveries in *Qui Tam* Cases against Health Care Providers Since 2009 (In billions of dollars)

Year	*Qui Tam* Recovery against Health Care Providers	Total Recovery against Health Care Providers
2009	$1.394	$1.632
2010	$1.969	$2.508
2011	$2.271	$2.449
2012	$2.541	$3.098
2013	$2.642	$2.703
2014	$2.313	$2.401
2015	$1.831	$1.965
2016	$2.499	$2.597
Total	**$17.460**	**$19.353**

Source: U.S. Department of Justice

Takeaway: The DOJ's reporting of FY 2016 fraud recoveries indicates large scale and individual enforcement efforts continue unabated and that laboratory testing is a fruitful target for enforcement agencies.

Congress to CMS: Catch Medicare Fraud *Before* It Happens

Despite the enforcement successes reflected in the Department of Justice's announcement of $4.7 billion in recoveries in fiscal year 2016, there is concern that more needs to be done *before* false claims are paid. In September 2016, Members of Congress sent a letter to Andrew Slavitt, Acting Administrator of the Centers for Medicare and Medicaid Services, stating that "the billions of dollars lost to Medicare fraud each year underscore the importance of stopping potentially fraudulent payments before they are made." The letter eschews the so called "pay and chase" efforts to recover improper payments after the fact and supported increased use of methods such as the Fraud Prevention System (FPS) to use predictive analytics to "identify claims and providers that present a high fraud risk to the Medicare program."

The Congressional members expressed a concern that despite the use of FPS, CMS was still relying "too heavily" on efforts to identify and recover improperly paid claims rather than preventing them from happening. The letter requested information regarding the types of schemes FPS has identified and total investigations for the past three years.

How to Create a HIPAA Breach Notification Policy

Privacy lapses can occur despite your best efforts to prevent them. If prevention does fail, the imperative switches to incident response and damage control. One of the key response challenges is furnishing timely notification under the HIPAA Breach Notification Rule. Here is how to implement a breach notification policy enabling you to meet that challenge.

What the Notification Rule Requires

The Notification Rule, which took effect nearly four years ago, requires providers to notify affected parties of breaches that compromise the privacy of protected health information. And you must act fast. Notification must be provided "without unreasonable delay" and no later than 60 days of discovering the breach.

Breach notification has become a compliance imperative. The recent $475,000 settlement with Illinois health system Presence Health (see related article on page 1) sends a clear signal that the HHS Office for Civil Rights (OCR) is dead serious about enforcing the 60-day deadline.

The Importance of a Breach Notification Policy

Breach notification is not something you can do on the spur of the moment. You must plan ahead and implement a policy enabling you to do three things:

- Investigate incidents in which PHI is or may have been compromised;
- Determine whether the incident constitutes a HIPAA breach for which notification is required; and
- If so, process and transmit the appropriate notifications.

The 10 Things to Include in Your Breach Notification Policy

Although breach notification policies cannot be one-size-fits-all, there are 10 things they should include.

1. Policy Statement

Start with a broad statement expressing your lab's commitment to privacy and HIPAA compliance.

MODEL LANGUAGE

Policy: Fictional Laboratories (Labs) is committed to protecting the privacy and security of Protected Health Information (PHI) with which it is entrusted in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), including but not limited to the HIPAA Breach Notification Rule, as well as state privacy laws, other applicable laws and regulations and Labs' own internal HIPAA privacy and security policies.

2. Explanation of Purpose

Explain that the purpose of the policy is to ensure appropriate and timely breach response and notification.

MODEL LANGUAGE

Purpose: The purpose of this policy is to establish rules and procedures for responding to data incidents that compromise or have the potential to compromise the privacy of PHI and which may constitute "breaches" requiring written notification under the Breach Notification Rule.

3. Incident Investigation & Breach Determination

Moving from principle to action, require designated personnel, e.g., a privacy officer or incident response team, to investigate incidents involving the actual or potential compromising of PHI to determine whether they constitute "breaches" for which notification must be provided. Explain what a "breach" is and list a few illustrative examples so that investigators know what incidents to investigate and how to determine if they are notifiable breaches.

MODEL LANGUAGE

Incident Investigation & Breach Determination: Any incidents in which the privacy of PHI is or may have been compromised must be investigated to determine if they constitute a "breach" requiring notification under the Breach Notification Rule. For purposes of this policy, "breach" means a use or disclosure of unsecured PHI that is not allowed under the HIPAA Privacy Rule and that compromises the PHI's privacy or security. Examples of incidents that must be investigated for potential breach notification purposes include where:

- An unauthorized person has or may have gained access to PHI, e.g., by accessing Labs' private patient data bases;
- PHI has or may have been used for an unauthorized purpose;
- A business associate to which Labs entrusts PHI has or may have had a security incident;
- PHI is missing.

Also tell investigators what information to collect so they can determine whether the incident constitutes a breach, including:

- The data involved;
- How the information was accessed, used or disclosed;
- Whether the access, use or disclosure was authorized by your lab's HIPAA policies;
- The incident date(s);
- The date the incident was discovered;
- The number of individual patients whose PHI was or may have been compromised.

4. Determination of Whether PHI Was "Secured"

Require investigators to determine if the data compromised was secured or unsecured and explain how. *Explanation:* A breach occurs when the compromised data was *unsecured*; if the data was properly secured, the incident is not deemed a breach and no notification is required.

MODEL LANGUAGE

Determine If Compromised Data Was Properly Secured: Assess whether the PHI compromised or potentially compromised in the incident was properly secured in accordance with HIPAA. For purposes of making this determination:

- Data is unsecured if it is not encrypted and rendered unusable, unreadable or indecipherable to unauthorized individuals via use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).
- Electronic data is secured only if both of the following things are true:
  1. The data is properly encrypted according to HHS guidance; and
  2. The individual or entity with improper access to the information does not have access to the confidential decryption key or process.

If you determine that the data is secured, you may conclude that the incident is not a breach requiring HIPAA notification. You must create a written record to document your conclusion and the specific facts on which you based it.

If you determine that the data is unsecured, its unauthorized access, use or disclosure may constitute a breach under HIPAA and you should proceed to Section X immediately below.

5. Determine If an Exception Applies

General rule: A breach occurs when the compromised PHI is unsecured. *Exception:* There are two kinds of PHI lapses for which notification is not required. Require investigators to determine whether either of these exceptions applies and explain how.

MODEL LANGUAGE

Determine If a Notification Exception Applies: If you conclude that the data compromised is unsecured, notification is generally required. However, notification is not required if the incident falls within one of two exceptions. Here is an explanation of each exception and how to determine if it applies to the incident under investigation:

- **The unintentional acquisition, access or use of PHI exception** applies if ALL of the following are true:
  1. The unauthorized acquisition, access or use of the PHI was unintentional;
  2. The individual who acquired, accessed or used the PHI was one of the following:
     i. A member of Labs' workforce;
     ii. A member of the workforce of a Labs business associate; or
     iii. A person acting under the authority of Labs or its business associate.
  3. The individual who acquired, accessed or used the PHI did so in good faith; and
  4. The unauthorized acquisition, access or use of the PHI did not result in a further use or disclosure not permitted under HIPAA.
- **The inadvertent internal disclosure of PHI exception** applies if ALL of the following are true:
  1. The disclosure was made by an individual who is authorized to access PHI;
  2. The disclosure was made to an individual who is authorized to access PHI;
  3. Both individuals work for the same organization, which may include:
     i. Labs;
     ii. A business associate of Labs; or
     iii. An organized health care arrangement in which Labs participates;
  4. The unauthorized disclosure of the PHI did not result in a further use or disclosure not permitted under HIPAA.

If you determine that an exception applies, you may conclude that the incident is not a breach requiring HIPAA notification. You must create a written record to document your conclusion and the specific facts on which you based it. If you conclude an exception does not apply, proceed to Subsection X immediately below.

6. Conduct a Risk Assessment

If the PHI is unsecured and neither exception applies, the impermissible use or disclosure is presumed to be a breach *unless* a risk assessment concludes that there is a low probability that PHI was compromised. Make sure your policy requires investigators to conduct a risk assessment.

MODEL LANGUAGE

Risk Assessment to Determine If Breach Occurred: If the PHI was unsecured and neither exception applies, the impermissible use or disclosure is presumed to constitute a breach requiring notification unless a risk assessment concludes that there is a low probability that PHI was compromised. Accordingly, the final stage in breach determination is to conduct the risk assessment to determine the probability that PHI has been compromised. In so doing, consider the following factors:

- The nature and extent of the PHI involved, including identifier types and likelihood of re-identification;
- The unauthorized person(s) who used or received the PHI;
- Whether the unauthorized recipient is a covered entity or business associate with a legal obligation to keep the PHI confidential;
- Whether the PHI was actually acquired, viewed or used; and
- The extent to which the risk to the PHI could have been minimized.

7. Require Patient Notification

Having determined that a HIPPA breach has occurred, you must provide appropriate notification within the 60-day deadline. Make sure your policy provides for such notification, starting with the individual patients whose PHI was or may have been compromised as a result of the breach. The Model Language below incorporates the basic requirements for patient notification. In a future issue of *G2 Compliance Advisor*, we'll provide a model letter you can use to notify patients.

Pointer: The notification deadline starts running when you first learn of the incident—not the date your investigation concludes that the incident constitutes a reportable breach.

MODEL LANGUAGE

Patient Notification: Upon completion of the investigation in which a breach is determined to have occurred and no later than 60 days from the date of discovery of the incident prompting the investigations, Labs will provide written notification to patients whose PHI was or may have been involved in the breach.

1. Notification will be provided to the patient, or where the patient is:
   i. Deceased, the next of kin or personal representative;
   ii. Incapacitated, the personal representative;
   iii. A minor, the parent or guardian.
2. Notification will be sent to the last known address of the patient or next of kin, unless the patient specifically requests that notice be sent via unsecured email.
3. If Labs' contact information is insufficient or out-of-date, notification will be provided via alternative methods, depending on the number of individuals affected:
   i. Fewer than 10: a phone call or other substitute form of notice;
   ii. 10 or more, either:
   - Posting a conspicuous notice including a toll-free number for 90 days on the homepage of Labs' website; or
   - Providing notice in major print or broadcast media in the geographic area where the patient can learn whether his/her PHI may have been involved in the breach, including a toll-free number.
4. Notification will be provided in plain language and clearly syntaxed and written in a manner that an individual of the recipient's reading level can understand without use of external materials or assistance.

8. Require HHS Notification

You must also notify the OCR of breaches. Unlike patient notices, the 60-day deadline for OCR notice varies depending on the number of individuals affected.

MODEL LANGUAGE

HHS Notification: Labs will provide written notification to the HHS Office of Civil Rights using the appropriate electronic breach report form available on the HHS website.

1. Where the breach involves 500 or more individuals, Labs will furnish the OCR notice upon completion of the investigation and no later than 60 days from the date of discovery of the incident prompting it;
2. Where the breach involves fewer than 500 individuals, Labs will furnish the OCR notice no later than 60 days after the end of the calendar year in which the breach was discovered as part of an annual report disclosing all such breaches that occurred during that calendar year.

9. Require Media Notification

Breaches affecting 500 or more individuals in a state must also be reported to "prominent media outlets" serving the state within the 60-day deadline, typically in the form of a press release.

10. List Required Content of Notification

Content requirements for all three forms of notice are the same and should be incorporated at the end of your notification policy.

MODEL LANGUAGE

What Information Breach Notification Must List: Regardless of delivery method and intended recipient, notification of HIPAA breaches will list, at a minimum, the following information:

- A brief description of the breach;
- The date the breach occurred;
- The date the breach was discovered;
- The types of PHI that the breach involved;
- Steps affected individuals should take to protect themselves from potential harm caused by the breach;
- Measures taken by Labs to investigate the breach, mitigate its potential harm and prevent further breaches;
- Contact information and procedures—including a toll-free number, email address, website or postal address—that individuals can use to ask questions or get further information.

Takeaway: While prevention is the primary objective, HIPAA also requires you to take action to mitigate data breaches you fail to prevent, which may include providing notification of the breach. When incidents occur, you must figure out what went wrong, which medical records were involved and, above all, whether the incident constitutes a breach for which breach notification is required. If so, you must prepare and deliver all of the required notifications. And you must do all of these things within 60 days!

The key to compliance: Implementing a breach notification policy at your lab.

New Discussion Paper Outlines FDA's Current Thinking on LDT Regulation, *from page 1*

Analysis of the Feedback

As part of the feedback process, the FDA asked stakeholders to suggest how they think the agency should regulate LDTs. According to the discussion paper, the various proposals shared some similar features, including:

"Based on the feedback received, a *prospective* oversight framework that focuses on new and significantly modified high and moderate risk LDTs would best serve the public health and advance laboratory medicine."

- Risk-based approach;
- Premarket review for some tests, with exemptions for certain categories;
- Test approval based on analytical and clinical validity;
- Adverse event reporting;
- Quality systems;
- "Grandfathering" for certain existing tests; and
- Transparency regarding test performance information.

"Based on the feedback received, a *prospective* oversight framework that focuses on new and significantly modified high and moderate risk LDTs would best serve the public health and advance laboratory medicine," the new discussion paper concludes.

The FDA Alternative Model

The FDA also sets out how its own thinking on LDT regulation has developed since 2014. Over the two years of "engagement," "positions of many groups, including the FDA, have evolved." The paper sets out key features that may be incorporated in an alternative to the framework the FDA proposed back in 2014, including:

- Phased-in oversight program over four years rather than the originally proposed nine years;
- Grandfathering for many LDTs already on the market;
- Broader definition of LDTs for unmet needs;
- Collaboration between FDA and third parties to use existing review standards and certification programs—such as the National Glycohemoglobin Standardization Program or the Cholesterol Reference Method Laboratory Network—for evidence standards;
- Potential use of existing review programs for third-party review, such as New York State's Clinical Laboratory Evaluation Program and independent CLIA accreditation programs;
- Clinical collaboration with stakeholders and health care professional organizations on standards for analytical and clinical validity;
- Public availability of evidence of analytical and clinical validity;
- Reliance on CLIA certification requirements plus three FDA quality systems requirements regarding test development processes—design controls, acceptance activities, and procedures for corrective and preventive action (CAPA); and

- Postmarket surveillance requiring labs report serious adverse events for tests except for traditional LDTs, LDTs for public health surveillance, specific transplantation related LDTs, and forensic-use LDTs.

What It Means

The FDA expressly states that its discussion paper and the proposal it outlines is not a final version of the 2014 guidance and "does not represent the formal position of the FDA, nor is it enforceable. We hope to simply advance the public discussion by providing a possible approach to spur further dialogue."

Takeaway: LDTs remain very much a work in progress, one that has evolved since 2014, and you need to stay tuned for further developments.

QUIZ

Is Offering Free Labelling Services to Dialysis Facilities a Kickback?

SITUATION

XYZ Labs wants to offer dialysis facilities free labeling of test tubes and specimen collection containers. But rather than offering it to all dialysis facilities, XYZ Labs would provide it only to selected facilities based on whether it thinks the freebie is necessary to attract or retain that particular facility's business.

QUESTION

Does the arrangement violate the Anti-Kickback Statute (AKS)?

A. Yes, because the free labelling is designed to induce referrals

B. Yes, because free services of any kind are automatically kickbacks

C. No, because the arrangement meets the personal services and management contracts safe harbor

D. No, because free labelling provides no benefit to dialysis facilities

ANSWER

A. The arrangement is problematic because it looks like the lab is using it to buy the dialysis facilities' referrals.

EXPLANATION

This scenario, which is based on a recent Advisory Opinion (16-12), illustrates how the Office of Inspector General (OIG) determines whether free lab services run afoul of the AKS.

Free or below-market services are problematic because they raise the inference that the lab is trying to influence the referral source to select the lab. In this case, the inference is enforced by XYZ Labs' admission that it would offer free labelling only to particular dialysis facilities when it thought the inducement was necessary to attract or retain their business. *Result:* The OIG said it would treat the proposed arrangement as an AKS violation. So A is the right answer.

Continued on page 12

The free labelling offered by XYZ Labs covers services the dialysis facility would otherwise have to perform at its own expense.

WHY WRONG ANSWERS ARE WRONG

B is wrong because while they raise red flags, free or below-market lab services are not *automatically* treated as kickback violations and may be justified in certain circumstances, e.g., if an AKS safe harbor applies.

C is wrong because the personal services and management contracts safe harbor applies only when compensation payments are consistent with fair market value. The dialysis facilities in this case would not pay *any* compensation to XYZ Labs for labelling.

D is wrong because free labelling *would* provide dialysis facilities a tangible benefit. *Explanation:* The Medicare end stage renal disease (ESRD) bundled payment that dialysis facilities receive includes ESRD-related lab tests. Labelling and other services related to those tests are not broken out from the ESRD bundled payment. *Result:* The free labelling offered by XYZ Labs covers services the dialysis facility would otherwise have to perform at its own expense.

Takeaway: The OIG's recent Advisory Opinion continues to emphasize the government's concern that free items or services can influence provider selection or induce referrals. The OIG's conclusion reiterates a nearly identical opinion issued in 2008.