G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

April 2016

Inside this issue

Survey Reveals Cybersecurity and Social Media as Top Compliance Concerns 1

AACC Adds to List of Alternative LDT Oversight Proposals 1

Federal Agencies Prepare to Battle Zika Virus in the U.S. 3

COMPLIANCE PERSPECTIVES

Avoid False Claims Liability: CMS Clarifies How to Comply with 60-Day Deadline for Returning Medicare Overpayments 5

FDA's LDT Oversight Framework Could Impact 60,000+ Tests 9

COMPLIANCE CORNER

Make Sure Existing Compliance Policies Match Current Operations 9

NEWS AT A GLANCE 12

www.G2Intelligence.com

Survey Reveals Cybersecurity and Social Media as Top Compliance Concerns

Cybersecurity is a top compliance concern according to a survey of compliance professionals conducted by Health Care Compliance Association (HCCA) and the Society of Corporate Compliance and Ethics (SCCE). In January 2016, HCCA and SCCE surveyed 900 individuals, suggesting 38 potential compliance issues and asking them to pick no more than 10 in answer to the question: "What are the hot topics in compliance you will be focusing on in 2016?" Those surveyed included compliance professionals from many different sectors, including health care.

The results revealed that cybersecurity and cybercrime were the top concern from survey respondents overall. For health care respondents cybersecurity and cybercrime ranked second, behind another internet-related issue—social media compliance risks. The SCCE and HCCA report on the survey reveals the top five responses identified

Continued on page 11

AACC Adds to List of Alternative LDT Oversight Proposals

Another industry trade group has chimed in on the issue of the U.S. Food and Drug Administration (FDA) regarding its intent to regulate laboratory developed tests (LDTs).

The American Association of Clinical Chemistry (AACC) issued a position paper urging the FDA to give up its effort to regulate LDTs and instead strengthen the existing CLIA regulations.

The FDA has proposed regulating LDTs in recent years, raising concerns that the complexity of the tests could put patients in danger if they are not properly interpreted. It has issued proposed guidelines for regulation over the objection of virtually all the laboratory sector. In its position paper, the AACC made the following recommendations:

- LDTs should be defined as new or significantly modified tests for which the modification alters the clinical claims
- CLIA should be updated to require laboratories to demonstrate that LDTs are clinically valid for use in medical decisions
- The Centers for Medicare & Medicaid Services (CMS) should credential third-party organizations to review a laboratory's clinical validation data for LDTs

Continued on page 2

AACC Adds to List of Alternative LDT Oversight Proposals, *from page 1*

- CMS and deemed accrediting organizations should include on inspection teams individuals with expertise to evaluate LDTs amount of the overpayment.

The AACC's position is similar to that of other trade groups in the laboratory space, including the American Clinical Laboratory Association. However, the AACC has gone the farthest in terms of articulating a specific alternative to the FDA regulating LDTs. (See box below for comparison of some proposed alternatives to the FDA framework).

"Clinical labs have one of the lowest error rates in healthcare, showing that CLIA has done an excellent job of regulating labs so that clinicians get the quality test results they need to make critical decisions about patient treatment," said AACC Chief Executive Officer Janet B. Kreizman in a statement. "AACC urges Congress and CMS to update the already rigorous CLIA framework, as we firmly believe this is the most effective way to improve oversight of laboratory-developed tests while still fostering innovation and enabling labs to meet the changing needs of patients."

Takeaway: The AACC is joining the chorus of laboratory groups objecting to the regulation of laboratory developed tests by the FDA, but has issued an extensive alternative. G2

Alternatives to FDA LDT Oversight Framework Proposed

To contrast AACC's proposal here are brief summaries of four other proposals put forth by other organizations in the laboratory industry.

Organization	Proposal
AMP	Update CLIA provisions with tiered, risk-based structure. Uses term Laboratory Developed Procedure defined as a professional service. Relies on CLIA, lab accreditation and professional certification for oversight. Expanded CLIA regulation should include verification of LDP clinical validity with clinical consultant reviewing appropriateness of test ordered and interpretation of results; public CLIA registry of labs and test offerings and public information about adverse events in labs; third party review for moderate and high risk LDPs. Multianalyte assays with algorithmic analyses with proprietary algorithms submitted to FDA
ACMG and AMA Coalition (includes AMP, American Association of Bioanalysts, American Society for Clinical Pathology, Bioreference Laboratory, Infectious Diseases Society of America and National Independent Laboratory Association)	Suggest modernizing CLIA by setting standards for clinical validity and strengthening existing standards for quality control, quality assurance, personnel standards and regular proficiency testing. Limited role for FDA.
ACMG	Position statement on genetic testing and LDTs claims LDTs used for genetic testing should be treated differently than routine diagnostic tests. Such tests involve the practice of medicine. Espouses approach closer to radiologic imaging oversight model rather than that based on devices. Proposes enhanced CLIA regulations with tiered and risk based approach, third party review system, public reporting of test performance, CMS and FDA coordinate oversight. Third party genetic testing laboratory accreditors assess analytical and clinical validity of new tests. Precertification of clinical validity under CLIA by third party accreditors for low and moderate risk genetic tests. High risk tests subject to CLIA/FDA/third-party review. NIH support for common data sharing regarding clinical significance of variants facilitating test validation and post market surveillance.
CAP Accreditation checklist	Opposes FDA framework and proposed alternative in 2009 with tiered, risk-based approach focused on analytic and clinical validity. Differed from FDA on defining LDTs and risk classifications and the role of CLIA and CMS. Also recently updated accreditation requirements address LDTs and impose requirements for "a minimum number of samples to ensure analytic accuracy."

Federal Agencies Prepare to Battle Zika Virus in the U.S.

As spring arrives and the threat of Zika virus grows in the U.S., the Centers for Disease Control and Prevention (CDC) and the U.S. Food and Drug Administration (FDA) are taking action to address the virus threat.

April 1, 2016, the Centers for Disease Control and Prevention (CDC) hosted 300 federal, state and local government representatives, health care professionals and private stakeholders at a national summit to discuss how to prepare to battle the Zika virus here in the U.S. "The mosquitoes that carry Zika virus are already active in U.S. territories, hundreds of travelers with Zika have already returned to the continental U.S., and we could well see clusters of Zika virus in the continental U.S. in the coming months. Urgent action is needed, especially to minimize the risk of exposure during pregnancy," said CDC Director Tom Frieden, M.D., M.P.H. in the CDC's release announcing the summit. The CDC also released a report that includes maps of the U.S. indicating the agency's estimate of where the mosquitoes that carry Zika virus can be found.

> ***"In the future, should Zika virus transmission occur in other areas, blood collection establishments will be able to continue to collect blood and use the investigational screening test, minimizing disruption to the blood supply."***
>
> **— Peter Marks, M.D., Ph.D.**

Amy Pope, J.D., White House Deputy Homeland Security Advisor and Deputy Assistant to the President also noted in the CDC statement the President's $1.9 million funding request to "prepare for, detect, and respond to any potential Zika outbreaks" in the U.S.

The FDA has also issued several guidances and approved some tests for detecting the virus, while questioning the developers of other tests.

FDA Guidance and Testing Approved for Donated Blood

Days before the summit, the FDA announced that a screening test to detect Zika virus in blood donations was available for use under an investigational new drug application. Noting the importance of protecting the nation's blood supply and screening blood in U.S. territories already affected by Zika transmissions, Peter Marks, M.D., Ph.D., director of the FDA's Center for Biologics Evaluation and Research, said in a statement: "In the future, should Zika virus transmission occur in other areas, blood collection establishments will be able to continue to collect blood and use the investigational screening test, minimizing disruption to the blood supply."

Roche, whose cobas® Zika test was authorized for use to screen blood donations, says the "first stage" will be to use the test in Puerto Rico to reduce the need to import blood and the "second stage of deployment" for the test will be use "in the southern United States, which will most likely be impacted by any spread in the virus." "All Testing Laboratories will need to be enrolled in and contracted into the clinical trial as specified and agreed with the FDA Center for Biologics Evaluation and Research."

Previously, in February 2016, the FDA issued recommendations on how to reduce risk of transmission via blood transfusion. Blood establishments, in areas with active Zika virus transmission, need to obtain whole blood and blood components for transfusion from areas of the U.S. without active transmission. Collection and preparation of platelets and plasmas can continue as long as FDA-approved pathogen-reduction device is used. For those blood facilities in areas without Zika virus transmission, FDA noted importance of deferral of donors at risk of Zika virus for four weeks.

FDA Urges Caution in Donations of Human Cells and Tissues

FDA is intent on reducing risk of transmitting the Zika virus from human cell, tissues and cellular and tissue-based products (HCT/Ps). The agency released March 1 recommendations for handling these donations from living and deceased donors.

> ***"It is particularly important for the FDA to review information related to your Zika Virus RNA by RT-PCR Assay's design, validation and performance characteristics."***
>
> **— U.S. Food and Drug Administration**

The FDA said people should be considered ineligible of donating HCT/Ps if they were: 1) diagnosed with the Zika virus infection; 2) were in an area with active Zika virus transmission; or 3) had sex with a male with either of those risk factors within the past six months. As to donations of HCT/Ps from deceased, the FDA advises they not be accepted when the donor had the Zika virus within six months of death.

The FDA points out in its guidance document that HCT/Ps with the highest potential for transmission of the Zika virus are those recovered from living donors.

FDA Takes Action Concerning New Zika Tests

The FDA granted approval for a diagnostic test for the Zika virus to be distributed to certified labs by the CDC. The test is the CDC Zika IgM Antibody Capture Enzyme-Linked Immunosorbent Assay (Zika MAC-ELISA).The CDC, which made an emergency use request for the test, is sharing it with labs in the Laboratory Response Network, a group of domestic and international labs that respond to public health emergencies. Hospitals and other providers seeking the tests for patients need to work through the CDC and CDC-certified labs.

But while this test got the green light by the FDA, the agency wrote other test-makers to challenge their Zika tests, seeking agency review of their design, validation and performance. MD Biosciences Clinical and Diagnostic Services Laboratory announced in March a rapid assay to detect the Zika virus in human blood and urine samples. The FDA issued a letter to MD Biosciences, Inc. indicating the test "appears to meet the definition of a device" under section 201(h) of the Federal Food, Drug, and Cosmetic Act and should be subject to premarket clearance, approval or Emergency Use Authorization. The letter added that "it is particularly important for the FDA to review information related to your Zika Virus RNA by RT-PCR Assay's design, validation and performance characteristics."

The company, after receiving a letter from the FDA, said it is "proceeding with the Zika test services following clarification with the FDA regarding any pre-market approval requirements pertaining to this assay. Testing services will not be offered pending this clarification."

The FDA has issued similar letters regarding other tests: to First Diagnostic Corporation for its ATFirst's One Step Zika Antibody Test and to Texas Children's Hospital and Houston Methodist Hospital for their Zika Direct Test intended as a rapid diagnostic test. The FDA also states in those letters the need for the agency to review the "design, validation, and performance characteristics of those tests." G2

Avoid False Claims Liability: CMS Clarifies How to Comply with 60-Day Deadline for Returning Medicare Overpayments

The Affordable Care Act requires labs, pathology groups and other providers to return overpayments to Medicare within 60 days of identifying the overpayment. Failing to comply with that deadline can mean False Claims liability and a fine ranging from $5,500 to $11,000 per claim. Until now, there was little clarity regarding what constitutes identification of an overpayment. This February, however, the Centers for Medicare and Medicaid Services (CMS) issued a final rule interpreting the 60-day repayment requirement (See *G2 Compliance Advisor*, March 2016, p. 1). It's not just the regulatory provisions that offer clarity, however. CMS responses to commenters, which are set forth in the preamble to the final rule, are insightful as well. Here's what you can learn from CMS' new rule.

CMS clearly emphasizes in the preamble to the rule that an overpayment is any amount which a lab receives to which it isn't entitled—whether the result of fraud, inadvertent error or mistake.

When the rule applies

Note the Feb. 12, 2016 final rule applies to Medicare providers and suppliers billing Medicare Parts A and B and any overpayments reported or returned on or after March 14, 2016, irrespective of the date on which the overpayment was received, says health care lawyer Robert E. Mazer of Ober Kaler. A claim any time in the last six years, that is discovered this year after March 14, 2016, must be returned in compliance with the final rule's interpretation of the 60-day deadline.

For providers already participating in a Stark law, self-referral disclosure protocol, instead of the six-year lookback a four-year lookback period applicable under Stark law applies. CMS is seeking OMB authorization, Mazer says, to require providers and suppliers reporting Stark Law violations under CMS' self-referral disclosure protocol to report financial information back six years.

Calculating the Overpayment

CMS clearly emphasizes in the preamble to the rule that an overpayment is any amount which a lab receives to which it isn't entitled—whether the result of fraud, inadvertent error or mistake. The amount that must be repaid is the difference between the amount received and the amount that should have been received, explains Mazer. In the case of an overpayment caused by violations of the Anti-Kickback Statute, Stark Law or goods or services provided by an excluded provider, the entire amount received is considered an overpayment, he adds.

But, Mazer indicates the "final rule includes certain exceptions or special rules for cost report claims, formal OIG and CMS self-disclosures, and requests for extended repayment schedules." Additionally, a change in law or regulation doesn't render a payment that was properly received suddenly an overpayment. "However, a so-called agency 'clarification' could result in an overpayment," says Mazer.

Note too that underpayments can't be used to offset overpayment amounts according to CMS which explains in the preamble that underpayments are "outside the scope of this rulemaking." Instead, providers can address underpayments by requesting reopenings.

Impact on Appeal Rights

Mazer advises "providers and suppliers review available appeal rights as part of the process of reporting and returning overpayments. Use of a statistical sample, for example, may preclude a Medicare claims appeal." He explains that CMS notes in the preamble that if a repayment of a "self-identified overpayment results in a revised initial determination of any specific claim or claims, a person would be afforded any appeal rights that currently exist."

An existing appeal of a contractor's determination of overpayment may render it premature to return any overpayment. "If a *contractor's* determination *is* appealed, the provider or supplier *may* reasonably determine that it is premature to investigate whether it received an overpayment during other periods until conclusion of the appeal process," says Mazer. But after having self-identified an overpayment, filing an appeal would not impact a provider's or supplier's duty to investigate potential overpayments or report and return any that are identified, Mazer adds.

> ***"If a contractor's determination is appealed, the provider or supplier may reasonably determine that it is premature to investigate whether it received an overpayment during other periods until conclusion of the appeal process."***
>
> **— Robert E. Mazer, Esq., Ober Kaler**

Beware: Effective Compliance Doesn't Merit Leniency

Mazer notes that CMS "encourages providers and suppliers to have 'effective compliance plans.'" CMS rejected, however, a commenter's request for a presumption that an overpayment is a simple mistake if the provider has a 'certified' or 'approved' compliance plan, stating: "Based on our experience, it is possible for providers or suppliers who have active compliance programs to commit fraud."

CMS further adds that "[a] provider or supplier with little if any compliance activities to monitor claims is exposed to liability 'based on the failure to exercise reasonable diligence if the provider or supplier received an overpayment.'"

"It is unclear what CMS means by this," says Mazer. "It may mean that a provider or supplier without an effective compliance program or the like will be deemed to have identified an overpayment on the date that it was received."

Additionally, unlike sentencing guidelines and the OIG compliance program guidance, CMS' final rule on overpayments doesn't accommodate different types or sizes of providers. "Providers and suppliers, large and small, have a duty to ensure their claims to Medicare are accurate and appropriate and to report and return overpayments they have received."

Guidelines for Reasonably Diligent Investigations

The final rule begs the question: What is reasonable diligence? Here are 6 lessons from CMS' rule that should guide labs seeking to be reasonably diligent.

#1. Be "active"

CMS defines reasonable diligence as be both proactive and reactive including "proactive compliance activities" that monitor receipts and look for overpayments *and* reactive investigations in response to "obtaining credible information of a potential overpayment."

Note too that the 60-days for returning overpayments starts when the reasonable diligence is completed. But, if a party fails to exercise reasonable diligence, the 60-day time frame

for returning an overpayment runs from the time the entity received credible information about a potential overpayment (that is, when it *should have* started exercising reasonable diligence to address the potential overpayment).

#2. Act on credible information within six months

The need for reasonable diligence can be triggered by receipt of credible information. "Credible information includes information that supports a reasonable belief that an overpayment may have been received," explains Mazer. He emphasizes that CMS' preamble indicates that reasonable diligence is "demonstrated through the timely, good faith investigation of credible information, which is at most 6 months from receipt of … credible information [of a possible overpayment], except in extraordinary circumstances." "This 6 month deadline is not included in the language of the actual regulation," says Mazer.

CMS explained that the six month estimate for timely investigation was chosen "because we believe that providers and suppliers should prioritize these investigations and also to recognize that completing these investigations may require the devotion of resources and time." CMS added that extraordinary circumstances may warrant extending the six months for investigation and 60 days for payment (so 8 months total) but said such extraordinary circumstances may include "unusually complex investigations" such as those involved in a physician self-referral law violation under the CMS voluntary self-referral disclosure protocol, natural disasters, or states of emergency.

#3. Treat contractor determinations as credible information

Mazer notes that CMS says Medicare contractor audit findings "are credible information of at least a potential overpayment." He adds that CMS also says a provider's confirmation of a Medicare contractor's audit findings, may constitute "credible information related to a potential overpayment for periods that were not audited, triggering a need to conduct reasonable diligence." Further, if a contractor determines that there has been an improper payment of a cost report claim, the provider is required to "conduct reasonable diligence on other cost reports."

Examples of Overpayments

CMS provided the following examples of situations in which an overpayment has been identified in its preamble to the February 2016 Final Rule:

- A provider finds incorrectly coded services in its review of billing or payment records.
- Patient death occurred prior to the date of service on a submitted claim
- Services were provided by unlicensed or excluded individual
- Overpayments are discovered during an internal audit
- A government agency informs a provider that an audit has revealed a potential overpayment and the provider doesn't make reasonable inquiry. If the provider does make a reasonable inquiry that confirms the government reported overpayment it has identified the overpayment and the 60 days begins to run.
- A provider "experiences a significant increase in Medicare revenue and there is no apparent reason" and the provider doesn't make a reasonable inquiry to determine if overpayment exists.
- A physician group finds that profits for the group or for a particular physician "were unusually high in relation to hours worked or the relative value units associated with the work" and fails to conduct a reasonable inquiry.

Notably, if a provider uncovers a kickback arrangement to which it wasn't a party but which affects its reimbursement, it may not be deemed to have identified an overpayment. That provider must report the information to the government which will investigate and "would most likely focus on holding accountable the perpetrators of that arrangement" and refer overpayment issues to the OIG. Generally an innocent provider benefiting from the arrangement won't be required to repay the overpayment "except in the most extraordinary circumstances," according to CMS' preamble to the new rule.

#4. Document efforts to comply with reasonable diligence

Health care providers should be conditioned by now to document everything relevant to demonstrating compliance with the law—but it bears repeating. CMS' preamble expressly cautions "it is certainly advisable for providers and suppliers to maintain records that accurately document their reasonable diligence efforts to be able to demonstrate their compliance with the rule."

"A provider or supplier cannot return those specific claims found to have been overpaid as part of an audit sample, but then choose not to extrapolate its findings and report and return total overpayments."

— Robert E. Mazer, Esq., Ober Kaler

#5. Medicare revenue and medical necessity are relevant

CMS addressed medical necessity in general and specifically with regard to labs in the preamble. Generally, CMS indicates "principles set forth in the final rule apply to 'medical necessity' determinations," Mazer points out. Commenters claimed that lack of medical necessity or insufficient documentation "are extremely difficult to define objectively" and alluded to application of the rule in those circumstances being unfair. CMS responded, however, that "[s]ufficient documentation and medical necessity are longstanding and fundamental prerequisites to Medicare coverage and payment."

Additionally, a significant increase in Medicare revenue should trigger the need for reasonable diligence, according to CMS. A commenter sought leniency for labs in this regard, pointing out that labs aren't "in a position to determine the medical necessity of the services they provide because they do not order the tests," and thus they shouldn't be expected to "proactively conduct an inquiry into whether an overpayment exists based on the volume of Medicare work it conducts." CMS responded: "All providers and suppliers have a duty to ensure that the claims they submit to Medicare are accurate and appropriate. There may be situations where a significant increase in Medicare revenue should lead a laboratory to conduct reasonable diligence."

#6. Extrapolate and find other similar overpayments

"A provider or supplier cannot return those specific claims found to have been overpaid as part of an audit sample, but then choose not to extrapolate its findings and report and return total overpayments," explains Mazer. CMS says it believes "it is appropriate to inquire further to determine whether there are more overpayments on the same issue before reporting and returning the single overpaid claim."

CMS further indicates it believes providers should be able to conduct a probe sample and incorporate it into a larger full sample to extrapolate overpayments "in a timely manner." "In the clinical laboratory setting it may well be that you have hundreds of claims that are virtually the same and don't require detailed analysis to determine if it's overpaid," Mazer told *G2 Compliance Advisor* when discussing the *Continuum Health* case (see *G2 Compliance Advisor*, August 2015, p. 1). Although this won't always be the case, when it is, you should be able to address the issue more quickly.

Editor's Note: Robert E. Mazer, together with his colleague Kelly J. Davidson, also a health care lawyer with Ober Kaler's Health Law Group, will be presenting a webinar addressing this final rule and what it means for labs and pathology groups April 13, 2016, 2-3pm EST. For more information, visit www.g2intelligence.com/web. G2

FDA's LDT Oversight Framework Could Impact 60,000+ Tests

The U.S. Food and Drug Administration's (FDA's) proposed regulation of laboratory developed tests (LDTs) could affect more than 60,000 genetic tests, according to analysis by Tenn.-based IT firm NextGxDx. Depending on the ultimate classifications of risk, nearly 8,000 genetic tests could face premarket review requirements with a high-risk device designation. Accurate estimates of the number of tests currently on the market are important as the FDA finalizes its oversight plan, designs implementation strategies, and allocates adequate resources towards operationalizing for the new regulatory scheme.

G2 Compliance Corner

Make Sure Existing Compliance Policies Match Current Operations

While labs may draft a comprehensive compliance plan and policies and procedures, those policies, procedures and plan can be a liability if they aren't being followed. There can often be "a lot of gaps between what the compliance plans say [labs] are doing and what they are actually doing," observes health care attorney David Gee, a partner with Davis Wright Tremaine. "People get ahead of themselves in terms of thinking they are doing all these great things putting in place policies and they aren't really syncing up the policy with what practice is." This can create a "house of cards," warns Gee.

Having a compliance plan or policies and procedures that you aren't actually following can create bigger problems than having no compliance program at all. "Gaps between policy and practice, if significant, can come back to bite you," says Gee. So labs need to be monitoring, auditing and training on a continuous basis, he advises. Train staff regularly on the details of your compliance plan and your policies and procedures. Then, monitor compliance activities and audit your policies and procedures to be sure they are being followed. Ensure that what your staff is doing in terms of compliance activities matches what they should be doing according to the compliance plan and policies you have developed. When you find gaps, make adjustments as needed to either the policies or practices. It may not always be that operations that do not align with a written policy issued previously are in violation of law. Sometimes, the guidance or protocol set forth in your written compliance program or policies may not be practical or necessary in light of your current operations and resources. So it may be prudent to revise or update your program and policies to reflect those realities, while still ensuring compliance with applicable law.

David Gee and his colleague Caitlyn Forsyth will be addressing tips for implementing and maintaining laboratory compliance best practices at G2 Intelligence's Lab Revolution, April 7, 2016, in Chandler, Arizona.

Many have been trying to estimate the number of currently marketed genetic tests. The FDA and industry sources have publicly quoted that 11,000 laboratories are offering as many as 100,000 molecular LDTs in the United States. GeneTests.org, a wholly owned business unit of BioReference Laboratories, maintains that as of Feb. 25, 2016 there are 55,574 genetic tests available from 678 laboratories internationally. The National Institute of Health's Genetic Testing Registry, which requires test providers to voluntarily input test information, has records for 32,000 genetic tests including prenatal, somatic, and pharmacogenetic tests.

Since the vast majority of new molecular diagnostics have come to market under CLIA, the proposed regulations represent a significant shift. With the FDA indicating it will utilize a risk-based approach to regulation and prioritization, laboratories are assessing where their tests will fall along the spectrum.

As of Jan. 11, 2016, NextGxDx estimates that there are 60,482 genetic testing products on the market, with an additional eight to 10 tests entering the market daily. In 18 months from July 2014 to January 2016, the company's databases show that 5,674 new testing products entered the market, with panel entrants growing 24 percent in that time period.

Using data from October 2015 (53,000 genetic testing products), NextGxDx analyzed tests under three different risk classification scenarios, recognizing the FDA's stated intention to use expert advisory panels to guide decisions about risk status. The company's bioinformatics specialists estimate that, de-

pending on the definition of risk, anywhere from 1.12 percent to 14.43 percent of tests could fall under high-risk regulation, which translates to between 587 and 7,568 tests. One major variable in the different risk scenarios is whether the FDA includes the American College of Medical Genetics and Genomics' 56 recommended genes to report incidental findings in its definition of high-risk tests. If the FDA does include these genes, NextGxDx says tests for these genes alone would involve: 121 laboratories, 331 clinical categories of tests, and 3,455 different testing products.

	Test Categories	Number of Tests	Percent of Genetic Testing Market
High Risk Test Scenario 1	Products similar in nature to those already regulated by the FDA: ■ Class III kits & devices ■ Companion Diagnostics	587	1.12%
High Risk Test Scenario 2	■ Companion Diagnostics ■ Class III kits & devices ■ Tests that target one of the ACMG 56 genes ■ Panels that include tests targeting one of the ACMG 56	3452	6.58%
High Risk Test Scenario 3	■ Companion Diagnostics ■ Class III kits & devices ■ Tests that target one of the ACMG 56 genes ■ Panels that include tests targeting one of the ACMG 56 ■ Pharmacogenomic Tests ■ Non Invasive Prenatal Tests (NIPTs) ■ All Oncology tests	7568	14.43%

Source: NextGxDx, October 2015.

NextGxDx provides an online genetic testing marketplace that offers health care providers and hospitals the ability to compare up-to-date listings of all genetic tests from CLIA-certified laboratories, order tests online, and manage results and utilization electronically within the HIPAA-compliant portal.

"We see great value in data-driven stakeholder dialog throughout the regulatory process," says Gillian Hooker, Ph.D., vice president of clinical development at NextGxDx. "We provide an innovative way to track parts of the market and bring transparency to everyone. We play a role in informing multiple stakeholders."

Once laboratories understand the risk profile of their tests, Hooker says laboratories are waiting to see what evidentiary standards the FDA requires.

"If there are high evidentiary standards, this could be the most costly part of getting a test approved," says Hooker. She adds that the next step in this analysis is incorporating cost data to estimate the potential financial impact of complying with the proposed regulations on laboratories.

Takeaway: As the industry awaits the FDA's finalization of LDT regulation criteria, NextGxDx is helping to inform estimates of how many LDTs could fall under the FDA's purview and in what risk category. G2

Survey Reveals Cybersecurity and Social Media as Top Compliance Concerns, *from page 1*

by respondents overall and grouped by employer type. For health care companies, other issues making the top five were: "More effective internal investigations," False claims enforcement, and "Creating/Maintaining an ethical culture." For small entities, nonprofits and privately held businesses, cybersecurity and social media compliance risks were most frequently cited issues. Respondents at larger and publicly traded companies, however, placed cybersecurity risks behind third party risks and leveraging compliance to increase efficiency and effectiveness.

The survey results correspond to many other reports highlighting cyber risks in health care. In 2014, the Federal Bureau of Investigation warned that the health care industry wasn't prepared for cyber risks. Cybersecurity was also named by health care attorneys interviewed by *G2 Compliance Advisor* about the top 10 compliance issues facing laboratories and pathology groups in 2016.

A May 2015 Ponemon Institute study that revealed health care-related criminal attacks on data increased 125 per cent since 2010 and were "the leading cause of data breach" in health care, yet most organizations still weren't prepared to respond to this threat to patient information. (See *G2 Compliance Advisor*, May 2015, p. 3) The authors of the Ponemon report also estimated that such breaches cost the health care industry $6 billion annually, with average costs per breach for individual health care organizations hitting about $2.1 million.

In February 2016, the Ponemon Institute released results of a new study, *The State of Cybersecurity in Healthcare Organizations in 2016*, which indicates 48 per cent of health care organizations surveyed have had a cyber incident in the past year that involved exposure or loss of patient information. The Ponemon Institute—a research firm focused on privacy and information management—worked with ESET, a security software developer, on the study which surveyed 535 IT and IT security professionals in small to medium sized health care organizations. "Based on our field research, healthcare organizations are struggling to deal with a variety of threats, but they are pessimistic about their ability to mitigate risks, vulnerabilities and attacks," reported Larry Ponemon, chairman and founder of the Ponemon Institute, in a statement announcing the organization's latest study.

In that study, 81 per cent of organizations surveyed identified patient medical records as the biggest target for hackers and others seeking unauthorized access. The top threats reported by surveyed entities were system failures, cyber attacks and unsecure medical devices. More than half of those surveyed reported that new technologies relevant to mobile health and big data and cloud storage increased risk to patient information. Other risks of concern included employee negligence and business associate relationships.

Takeaway: Cybersecurity continues to be a significant concern for both IT and health care compliance professionals. G2

HHS Task Force Members Named as $3.9 HIPAA Settlement Highlights Need for Better IT Security

A $3.9 million settlement arising from a potential HIPAA breach and an announcement regarding a U.S. Department of Health and Human Services Task Force emphasize the risks to the privacy and security of patients' health information.

Feinstein Institute for Medical Research, a biomedical research institute based in New York, agreed to the settlement which includes a corrective action plan after a laptop was stolen from an employee's car, according to an HHS Office for Civil Rights (OCR) March 17 press release. "This case demonstrates OCR's commitment to promoting the privacy and security protections so critical to build and maintain trust in health research," HHS said. The settlement is the result of an investigation following the organization's filing of a breach report concerning the 2012 theft of the laptop, which reportedly held about 13,000 patients' and research participants' health information. OCR asserted the organization failed to have adequate policies and procedures and safeguards with regard to laptops.

Just a day earlier, HHS had also announced membership of the Health Care Industry Cybersecurity Task Force which includes government and private sector leaders. The Task Force will seek "the best ways organizations of all types are keeping data and connected medical devices safe and secure" and report to Congress within the next year before the Task Force's term ends in March 2017. The Task Force arises out of the Cybersecurity Information Sharing Act of 2015 and will also develop materials to help organizations ensure security of health information.

News at a Glance

HHS Reports Medicare Spending Declined. After announcing that the goal of linking 30 percent of Medicare payments to quality was reached months earlier than anticipated, the U.S. Department of Health and Human Services (HHS) reported that Medicare spending between 2009 and 2014 was $473.1 billion lower than it would have been if average growth in the eight years prior to that period had continued. HHS also estimates that Medicare spending could be $648.6 billion less between 2009 and 2015 than it would have if 2000-2008 average growth rate had continued. "To put this in context, this reduction in spending is greater than all of Medicare's spending for personal health care expenditures in 2015," according to HHS' report. The prediction relies on per enrollee spending growth remaining as low as 1.1 percent. Crediting the Affordable Care Act for the success, the HHS press release announcing the release of the Medicare spending report said "[t]he health care law gives HHS new tools to pay providers for what works, better coordinate and integrate care, and make information more readily available to those who can use it to improve health. Initiatives to limit avoidable hospital readmissions and to promote new payment models that focus on value are contributing to the moderation in overall health spending, and particularly for Medicare." Despite the slowed growth in spending, the report does reveal that 2014 expenditures for national personal health care increased by 4.3 percent per person. Still even this increase is considered "modest" by HHS, compared to growth in prior years, and is attributed to the increase in health care insurance coverage under the ACA.

ACLA Seeks Better Medicare Coverage for Vitamin D Testing. The American Clinical Laboratory Association (ACLA) has asked regional fiscal intermediary Novitas—and by extension, much of the Medicare program—to reconsider its austere position on testing for some vitamin deficiencies. In particular, the ACLA has asked Novitas to reconsider its position regarding testing for vitamin D. Currently, Medicare does not reimburse for many forms of vitamin or micronutrient testing, considering such tests to be medically unnecessary. It makes a few exceptions for patients with specific diseases or medical conditions, but they are generally narrow. Although the draft LCD currently provides testing coverage for Medicare enrollees diagnosed with rickets, osteomalacia, osteoporosis, chronic kidney disease and some digestive disorders such as irritable bowel syndrome and Crohn's disease, the ACLA wants coverage to include other patients as well. The organization is asking for coverage of patients who have been diagnosed with cystic fibrosis, undergone bariatric surgery or suffered from radiation enteritis—an inflammation of the digestive system due to radiation treatments for cancer. It is also asking for coverage for patients diagnosed with several forms of lymphoma and histoplasmosis.

U.S. Lab Sector Globalizes with Foreign Deals. The U.S. lab industry has in recent decades begun to go global. Large multinational corporations that own laboratories in other nations are buying American companies and acquiring either their labs or opening new domestic facilities. Some examples of globalization are straightforward: Sonic Healthcare Laboratories, an affiliate of an Australian firm, has had significant operations in the U.S. for years, although it keeps testing within U.S. borders. Other deals involve foreign labs entering the U.S. market and publicly traded U.S. labs beginning commercialization initiatives outside the U.S. The Centers for Medicare & Medicaid Services (CMS) has also created an "International Laboratory CLIA Certification Process" that provides a blueprint for labs operating outside of the United States to legally accept and process samples from the U.S. The March 17, 2016 issue of *Laboratory Industry Report* provides an in-depth look at foreign lab deals and off shore CLIA certifications. G2

 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 or Fax: 1-855-649-1623. Web site: www.G2Intelligence.com.

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; Lori Solomon, Ron Shinkman & Donna Marie Pocius, Contributing Writers; Stephanie Murg, Managing Director, G2 Intelligence; Kim Punter, Director of Conferences & Events; Randy Cochran, Corporate Licensing Manager; Jim Pearmain, General Manager; Michael Sherman, Marketing Director; Pete Stowe, Managing Partner; Mark T. Ziebarth, Publisher.

Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 1-888-729-2315.

