G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

NATIONAL INTELLIGENCE REPORT™

Covering Government Policy For Diagnostic Testing & Related Medical Services

Celebrating Our 36th Year of Publication

Vol. 15, Iss. 21, November 26, 2015

INSIDE THIS ISSUE

www.G2Intelligence.com

FDA Report Asserts Case Studies Support Need for More Oversight of LDTs

The U.S. Food and Drug Administration (FDA) released a 30-plus page report detailing case studies it says demonstrate the need for the FDA to abandon its policy of enforcement discretion and exercise more robust oversight of laboratory developed tests (LDTs). Washington D.C. lawyer, Jeffrey N. Gibbs, of Hyman, Phelps & McNamara P.C., who works with medical device and in vitro diagnostic companies, explains the report is likely a response to a Congressional request last year that the FDA provide evidence of the harms associated with LDTs and "was obviously timed to coincide with [the] House hearing on LDTs."

An *FDA Voice* blog article announcing the release of the report describes the report as an illustration of "the real and potential harms to patients and to the public health from certain laboratory developed test (LDTs)." The report covers 20 case studies that the FDA asserts demonstrate the risks of false positives and false negatives from certain LDTs. FDA Voice blog author, Peter Lurie M.D., M.P.H., FDA's Associate Commissioner for Public Health Strategy and Analysis claims the lack of FDA oversight of LDTs has led to "staggering" costs and indicates the report estimates the "public health cost for five of the 20 cited tests."

Continued on page 2

HHS' Top Ten Management Problems Include Labs

Every year the Health and Human Services (HHS) Office of Inspector General (OIG) summarizes HHS' top management and performance challenges, which "reflect continuing vulnerabilities that the OIG has identified for HHS over recent years as well as new and emerging issues that HHS will face in the coming year."

The OIG's FY 2015 Top Management and Performance Challenges include clinical laboratories as a necessary focus of efforts to fight fraud, abuse and waste in Medicare. Specifically, the report notes that while "[f]raud schemes shift over time, … certain Medicare services have been consistent targets"—namely, clinical laboratories. Labs were included in a list of seven types of services ripe for fraud and abuse, including home health, ambulance transport, chiropractors and durable medical equipment suppli-

Continued on page 7

FDA Report Asserts Case Studies Support Need for More Oversight of LDTs, *from page 1*

The FDA report, titled *The Public Health Evidence for FDA Oversight of Laboratory Developed Tests: 20 Case Studies* is available on the FDA website. It categorizes the case studies according to the problems raised: false positives, false negatives, lack of relevance to the tested disease, tests linked to disproved scientific concepts, tests undermining drug approval or treatment selection, and unvalidated tests. The cases were gathered, according to the FDA, from "publicly available information in medical journals, media reports and FDA Warning letters."

Among the tests disputed by the FDA include assays to determine the risk for ovarian cancer; a test for whooping cough; tests to help guide treatment of patients with breast cancer, prostate cancer and melanoma; non-invasive prenatal testing; and vitamin D deficiency testing, among others.

The report detailed 20 different LDTs that while compliant with CLIA regulations, did not require approval of the FDA. A couple of the tests have been withdrawn or not brought to market, but most are currently available commercially. According to the FDA report, they "illustrate, in the absence of compliance with FDA requirements, that these products may have caused or have caused actual harm to patients. In some cases, due to false-positive tests, patients were told they have conditions they do not really have, causing unnecessary distress and resulting in unneeded treatment. In other cases, the LDTs were prone to false-negative results, in which patients' life-threatening diseases went undetected. As a result, patients failed to receive effective treatments."

Among the tests disputed by the FDA include assays to determine the risk for ovarian cancer; a test for whooping cough; tests to help guide treatment of patients with breast cancer, prostate cancer and melanoma; non-invasive prenatal testing; and vitamin D deficiency testing, among others. Gibbs notes that some of the tests mentioned in the report have been discontinued.

He also predicts the report is unlikely to "shift opinions substantially." While the report provides "ammunition for those pressing for FDA oversight," opponents of LDT regulation may assert the case studies "present a skewed view of the performance of LDTs, and disregard the benefit side of the ledger" and test companies will likely characterize the "FDA's very brief description and conclusions as incomplete and misleading," Gibbs explains. Indeed, the American Clinical Laboratory Association was immediately dismissive of the report. "These so-called case studies are not representative of the thousands of LDTs utilized on a daily basis by providers to positively impact patient care," the ACLA said in a statement.

Takeaway: The FDA backs up its claims that LDTs need more oversight with case studies addressing specific tests it asserts are problematic. G2

Precision Medicine Initiative Sets Privacy Principles

In mid-November the White House released the Privacy and Trust Principles for the Precision Medicine Initiative (PMI). The principles provide a framework for protecting the data of individuals participating in the initiative, while accelerating biomedical research and breaking new ground in providing participants data access.

"PMI includes aligned efforts by the Federal government and private sector collaborators to pioneer a new approach for health research and health care delivery that prioritizes patient empowerment through access to information," said Jo Handelsman,

associate director for science at the White House Office of Science and Technology Policy, in a blog post. "These principles are intended to establish a foundation for future PMI activities to ensure that privacy has been built into the core of the Initiative and that privacy is maintained as a central priority of PMI throughout all components."

Earlier in the year, President Obama asked for $215 million in funding for the initiative. The largest line item in the proposed budget—$130 million—was for the creation of a massive database containing the genetic data of at least one million volunteer participants. Given the increasing number of health care-related data breaches and the inherent sensitivity of genetic data, privacy must be ensured and trust must be built to ensure recruitment of the large cohort.

An interagency working group, initially convened in March, helped to provide guidance for the principles. The working group that was co-led by the White House Office of Science and Technology Policy, the Department of Health and Human Services Office for Civil Rights, and the National Institutes of Health. The principles were developed following expert roundtables, review of the bioethics literature, an analysis of privacy policies and frameworks used by existing biobanks and large research cohorts, and public comment this summer.

The principles provide broad guidance for future PMI activities regarding: building trust and accountability through transparency and involving participant representation in all stages of the initiative's development and implementation; respecting participant preferences; empowering participants through access to information; ensuring responsible data sharing, access, and use; and maintaining data quality and integrity.

Central to trust is transparent communication. The principles outline that information should be communicated to participants "clearly and conspicuously" regarding how their data will be used, accessed, and shared; types of studies for which the individual's data may be used; the goals, potential benefits, and risks of participation. Furthermore, the principles outline that data sharing expressly prohibits the sale or use of participant data for targeted advertising. Hand in hand with privacy principles is development of data security safeguards.

The PMI is taking steps to build sound security practices from the beginning of the initiative to ensure the confidentiality and integrity of all PMI participant data. The Security Policy Framework will draw on industry's best practices in identifying strong administrative, technical, and physical safeguards, but will require regular reevaluation as practices evolve.

Takeaway: The PMI offers a new model of patient empowerment throughout the research process. Given the scope of the PMI endeavor, that patients will have access to their own data, and the number of anticipated participants, elaboration of guiding trust and privacy principles is an important step.

FDA and CMS Address LDT Regulation Before Energy and Commerce Committee

Last week, the U.S. House of Representatives Energy and Commerce Committee heard testimony about oversight of laboratory developed tests (LDTs) from representatives of the U.S. Food and Drug Administration (FDA) and Centers for Medicare and Medicaid Services (CMS). The opportunity to speak at the hearing, titled "Examining the Regulation of Diagnostic Tests and Laboratory Operations," was invitation only. The agencies presented a united front in supporting FDA oversight of LDTs.

"In many cases, the only difference between many modern LDTs and other IVDs is where they are manufactured, and the accuracy and reliability are every bit as important for modern LDTs as for any other IVD."

— Jeffrey Shuren, FDA

Jeffrey Shuren, director of the Center for Devices and Radiological Health at the FDA, spoke about the agency's regulation of medical devices and in vitro diagnostic tests (IVD) and explained the history leading up to the framework released last year. He also noted current proposals from the lab community that "acknowledge that LDTs must demonstrate that they are analytically valid and clinically valid." He cited problematic LDTs like those referenced in the FDA's report released last week (see page 1), to demonstrate the need for oversight. For example, his written comments highlighted one test discussed in the report that is used to determine a patient's response to statin therapy. The FDA found there wasn't an adequate link between the genetic variant and statin response. But 150,000 patients received the test, and the FDA estimates the problematic results cost $2.4 billion due to under or overtreatment with statins.

Identifying LDTs as a type of IVD, Shuren explained "[m]odern LDTs are often complex, have a nationwide reach, and have high-risk uses, and without oversight could present risks for patients and health care providers who rely on the results of LDTs to make medical decisions." "In many cases, the only difference between many modern LDTs and other IVDs is where they are manufactured, and the accuracy and reliability are every bit as important for modern LDTs as for any other IVD." Citing examples of the complexities involved, the written testimony discusses high risk tests such as companion diagnostics and moderate risk tests such as a blood test to detect heart attack, suggesting they require FDA oversight because inaccurate test results could delay treatment. "In both cases, the Agency's premarket review and post-market controls are essential to ensuring patients don't experience grave consequences from inaccurate results."

Discussing test modifications, the FDA's written submission contrasted simple changes that likely don't require review: "such as modifying the salt used in a buffer solution, or making an increase in the number of samples that a laboratory analyzer can process at one time." On the other hand, review would be required for "highly complex modifications that affect a test's performance—such as changing the measuring range of a marker to detect lower levels or adding a new marker to a panel of markers—or a test's intended use, such as changing the intended use of a Hemoglobin A1c test from monitoring glucose control in someone who already has diabetes to using that test to diagnose diabetes." When such a change can increase the risks posed by the testing or affect test performance or intended use, the FDA argues it should be exercising oversight concerning such modifications.

FDA's Next Steps

Shuren's written statement reported that the FDA "has completed its review of the public comments on the draft guidance documents that it received through an open public docket and a two-day public meeting, as well as feedback received from several webinars FDA held with stakeholders to discuss concerns and address questions." He outlined the following steps that the FDA is now taking:

- Coordinating with CMS on laboratory oversight and FDA plans to develop draft guidance regarding quality system requirements for LDTs, "to provide clarity for laboratories on how they can leverage compliance with CLIA requirements to satisfy those applicable FDA guidelines";
- Working with CMS and accrediting bodies and CLIA-exempt state laboratory programs, "to identify any potential overlaps between CMS and FDA activities" and look for ways to increase efficiency; and
- "Ongoing meetings with stakeholders, including laboratories, patients, traditional IVD manufacturers, and medical practitioners."

In response to questioning from the committee, Shuren indicated that the FDA intends to finalize its regulatory framework in 2016.

"CMS does not have a scientific staff capable of determining whether a test is difficult to successfully carry out or likely to prove detrimental to a patient if carried out improperly."

— Patrick Conway, Deputy Administrator, CMS

CMS Backs Up FDA

Patrick Conway, CMS' deputy administrator for innovation and quality and chief medical officer, also provided testimony, explaining the roles of CMS, the FDA and the Centers for Disease Control and Prevention under CLIA. His written statement to the committee clarified that CLIA "merely regulates how and by whom the test is conducted and reported out, rather than the scientific principles behind or the clinical validity of the test system itself." He added that CMS defers to FDA to determine clinical validity of a test.

Conway explained that "CLIA does not regulate the scientific principles behind or the clinical validity of any test – that is, the ability of the test to identify, measure, or predict the presence or absence of a clinically relevant condition or predisposition in a patient."

Further he added: "CMS does not have a scientific staff capable of determining whether a test is difficult to successfully carry out or likely to prove detrimental to a patient if carried out improperly. This expertise resides within the FDA, which assesses clinical validity in the context of premarket reviews and other activities aligned with their regulatory efforts under the Food, Drug, and Cosmetic Act."

Takeaway: The FDA and CMS are presenting a united front concerning the need for FDA oversight of LDTs and 2016 promises to bring changes for laboratories offering LDTs. G2

FCC Names Spectrum Coordinator, Paving Way for Remote Patient Monitoring

In a decision with implications for remotely monitoring patients throughout the care continuum, the Federal Communications Commission (FCC) announced a frequency coordinator for medical body area network (MBAN) operations. The FCC named Enterprise Wireless Alliance (EWA) as coordinator for the 2360 to

2400 MHz frequency range. Health care organizations are required to register MBAN devices capable of operating in the spectrum with EWA.

This may be an important development for laboratory administrators and pathologists, who could eventually find opportunities to leverage diagnostics data captured by the technology. "MBAN technology will provide a flexible platform for the wireless networking of multiple body transmitters used for measuring and recording physiological parameters and other patient information or for performing diagnostic or therapeutic functions, primarily in healthcare facilities," the FCC said in its November announcement.

"MBAN technology will provide a flexible platform for the wireless networking of multiple body transmitters used for measuring and recording physiological parameters and other patient information or for performing diagnostic or therapeutic functions, primarily in healthcare facilities."

— Federal Communications Commission

For its part, EWA is charged with ensuring interference-free sharing of the band, which also serves the Aeronautical Mobile Telemetry (AMT) operations. "Our role is to ensure MBAN deployments are conducted pursuant to FCC rules governing those deployments, specifically securing operational concurrence from the Aerospace and Flight Test Radio Coordinating Council to ensure there is no risk of interference to Aeronautical Mobile Telemetry devices," Mark Crosby, EWA president, told *National Intelligence Report (NIR)*. EWA, a national association with members including communication device manufacturers and resellers, announced that it has begun developing an online system for MBAN registration in anticipation of facilitating use of the advanced technology by health care facilities.

MBAN devices may provide patient monitoring parameters including blood glucose and pressure, delivery of electrocardiogram readings, and neonatal monitoring, Dale Woodin, senior executive director of the American Society for Healthcare Engineering, told *NIR*.

GE Healthcare and Philips Electronics, developers of remote monitoring systems (pulse, respiration rate, blood pressure, arterial oxygen saturation, to name a few offered by Philips Electronics), provided a joint proposal to the FCC prior to the Commission's approval of a plan to allocate spectrum in May 2012. MBANs offer a variety of patient monitoring capabilities in acute care and critical care settings, as well as emergency vehicles, homes and beyond, the companies say.

How do they work? The MBANs, networks of devices worn on the body, use a wireless communication link to connect with a programmer or controller device outside the body, the FCC explains. In addition to enabling the monitoring of clinical measurements wherever a patient is located, MBAN devices have these additional benefits, developers say: 1) early intervention by allowing caregivers to see a condition before it becomes critical; 2) ease of patient transport since there is no need to disconnect and reconnect wires; 3) reduced risk of infection; and 4) flexibility in ease of removing sensors from the body.

Takeaway: With the FCC's naming of a coordinator to protect spectrum for wireless medical devices, providers intending to use the MBAN spectrum need to register with Enterprise Wireless Alliance. The decision suggests remote health monitoring is progressing—with implications for developers of the devices; labs that analyze and capture data; and patients, whose vital signs may be more conveniently assessed with the new technology. G2

HHS' Top Ten Management Problems Include Labs, *Continued from bottom of p.1*

ers. The OIG report notes "CMS is not realizing the full potential of contractors to proactively identify fraud and address other program integrity concerns."

Related challenges included reducing improper payments, which the report notes could be complicated by the recent transition to ICD-10 diagnosis coding. Additionally, "significant challenges in adjudicating provider appeals of Medicare overpayments … including a substantial backlog of appeals at the administrative law judge level" were also noted.

Specifically, the OIG advised *"[t]o make use of the benefits of the growing amounts of data in the health care context, data must be available, subject to appropriate privacy and security safeguards, where and when needed."*

The OIG does commend the Health Care Fraud and Abuse Control Program for its ability to return $7.70 for every $1 invested in fighting fraud and abuse, the Fraud Prevention System which achieved $133 million in adjusted actual and projected savings and a $2.84 return on each $1 invested, as well as the establishment of the ICD-10 Coordination Center and appointment of an ICD-10 ombudsman as successful efforts by HHS to address the above challenges. However, the report asserted "more needs to be done" and the Centers for Medicare and Medicaid Services needs to identify and recover improper Medicare payments "in a timely manner" and implement safeguards to prevent recurrence.

"[M]eaningful and secure exchange and use of electronic information and health information technology" was another top concern. The OIG noted that HHS faces significant challenges with regard to ensuring privacy and security of information and improving information flow. Specifically, the OIG advised "[t]o make use of the benefits of the growing amounts of data in the health care context, data must be available, subject to appropriate privacy and security safeguards, where and when needed." The hurdles impeding this information flow include lack of interoperability, complex federal and state privacy and security laws, cost of information technology, information blocking and consumer unwillingness to share information. The report indicates this lack of information sharing can have patient safety implications; for example, if a patient undergoes additional invasive testing because prior results from a different provider aren't shared.

Not surprisingly reforming payment programs was also included among the top ten challenges facing HHS—including implementation of the "new market-driven payment system for laboratory services beginning in 2017." The report warned that substantial investment is being made into developing new payment models (a 10-year, $10 billion budget has been allocated to the Center for Medicare and Medicaid Innovation) and CMS "must establish policy, infrastructure, data systems, and oversight mechanisms to successfully implement these substantial changes." Among the steps the OIG says need to be taken are providing "clear guidance for providers on program requirements" and developing systems to ensure models are successfully implemented and problems or inefficiencies are identified and addressed. Data is also a concern. Noting the new payment models rely heavily on electronic health records, data and technology, the OIG warns that data must be secured and yet also integrated and shared.

Other challenges rounding out the top ten include Medicaid fraud and abuse; administration of grants; appropriate use of prescription drugs; quality nursing home, hospice and home- and community-based care; implementing and overseeing health

insurance marketplaces; operating public health programs; and ensuring safety of food, drugs and medical devices (which included compound drugs, off-label promotion, kickbacks and dietary supplements, but notably didn't mention in vitro diagnostic devices or laboratory developed tests).

Takeaway: Once again laboratories are included as a top target for fraud and abuse enforcement; yet HHS and laboratories share common ground in facing significant challenges in the coming year while adapting to new payment models and making data work for the health care delivery system.

Healthcare Sector Fares Well in GAO Review of Cybersecurity Progress

Perhaps in part due to the fact that the healthcare sector has long been focused on information security thanks to the HIPAA privacy and security rules, the Department of Health and Human Services (HHS) fared well in a review by the U.S. Government Accountability Office (GAO) regarding how federal agencies are protecting critical infrastructure from cyber risks.

The GAO's report included a recent high profile attack on a health insurer that potentially compromised the information of 1.1 million customers as one example demonstrating the impact of cyber attacks, and evaluated the efforts of 15 critical infrastructure sectors including the health care and public health sector—which it defined to include providers such as laboratories, insurers, pharmaceuticals, blood and health information technology. The GAO found that HHS addressed eight of nine Call to Action steps identified by the National Infrastructure Protection Plan to improve cybersecurity and mitigate cyber risks. The only Call to Action step which the GAO found the health sector hadn't addressed was "advancing research and development solutions" to improve infrastructure security and resilience.

HHS was, however, one of only three sectors that "established performance metrics to monitor cybersecurity-related activities, incidents, and progress in their sectors." Those metrics included mandatory reporting of data breaches (under the HITECH requirements), HHS monitoring of such breach incidents and use of data breach information to identify "cybersecurity-related trends." HHS also monitors receipt of its security alerts. It is these performance metrics that GAO found lacking in the remaining sectors and the GAO made such metrics the main focus of its recommendations to the other sectors.

Takeaway: As many agencies warn that more needs to be done to address cybersecurity risks, the GAO finds that the healthcare sector is ahead of other sectors in terms of monitoring its cybersecurity performance.

National Intelligence Report (ISSN 2332-1466) 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.

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; Lori Solomon, Contributing Writer; Stephanie Murg, Managing Director;
Kim Punter, Director of Conferences & Events; Randy Cochran, Corporate Licensing Manager; Michael Sherman, Director of Marketing; Jim Pearmain, General Manager; 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.