G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

NATIONAL INTELLIGENCE REPORT™

Covering Government Policy For Diagnostic Testing & Related Medical Services

Celebrating Our 40th Year of Publication

Vol. 19, Iss. 8, August 2019

INSIDE THIS ISSUE

Surviving PAMA:
Keep an Eye on Industry Disruptors 3

Focus On:
State AGs Break New Ground by Teaming Up to Enforce HIPAA 4

Labs in Court:
A roundup of recent cases and enforcement actions involving the diagnostics industry 8

Enforcement Trends:
Investment Return on Fraud Fighting Continues to Decline 10

News:
New FDA Guidance Tells IVD Makers How to Test for Biotin Interference 11

PAMAgeddon: Congress Tables Bill to Delay Next Round of Price Reporting for One Year

The PAMA data collection process has been a lightning rod for criticism from almost the moment CMS unveiled it. And now Congress may be getting ready to intervene. A newly proposed bill called Laboratory Access for Beneficiaries (LAB) Act would delay the reporting of lab payment data required by PAMA by one year. Here's a rundown of what you should know about the LAB Act.

The PAMA Payment Data Reporting Controversy

Price data reporting is, of course, crucial to the lab industry because it serves as the basis of what are supposed to be the market-based rates for lab tests under Medicare Part B mandated by PAMA. Under the statute, CMS is responsible for collecting this data. The problem is that instead of assembling a database representative of private payor rates, CMS ended up collecting a sample representing less than 1% of the market. CMS price data reporting left out huge swaths of labs including hospital labs that command higher prices for lab tests.

In addition to overweighing data from large firms with cost structures lower than typical labs, such as Quest Diagnostics and LabCorp, the exclusion of higher-price labs artificially skewed rates by more than

Continued on page 2

Industry Buzz: Obamacare Appeal Set for Round 2

Seven months after a Texas U.S. District Court striking down Affordable Care Act, aka Obamacare, unconstitutional, the case is going back to court on appeal. The betting is that the Fifth Circuit, which opens the proceedings on July 16, will reverse the lower court's ruling that not just the individual mandate but the entire Obamacare law is unconstitutional. But that's no slam dunk. And if the Fifth Circuit does defy expectations, it will pave the way for a Supreme Court battle, not to mention a massive wave of disruption in health insurance markets. We'll keep you apprised as things develop. Meanwhile, for a complete analysis of the latest court challenge against Obamacare, see *National Intelligence Report (NIR), April 15, 2019*.

PAMAgeddon: Congress Tables Bill to Delay Next Round of Price Reporting for One Year, *from page*

30% across a broad range of diagnostic tests. In 2017, the American Clinical Lab Association (ACLA) filed a lawsuit challenging the legality of the rate setting process. A lower federal court dismissed the case in 2018 but ACLA maintained the pressure by filing an appeal. (For more about the ACLA PAMA lawsuit, see *National Intelligence Report (NIR)* Dec. 15, 2018.)

Last December, the CMS gave some ground by broadening reporting labs to include hospital outreach labs that submit Medicare claims using 14X billing. The agency also tweaked the formula labs must use to determine the percentage of revenue generated by the Clinical Laboratory Fee Schedule or Physician Fee Schedule in a way that will likely lead to more labs having to report payment data.

While the welcoming the changes, lab industry groups continue to insist that they don't go far enough. "Our most vulnerable seniors are at the whim of a flawed data collection and reporting process that is fundamentally at odds with the quality care they deserve," according to a press release from ACLA President **Julie Khani**. "They have seen the impact of PAMA's misguided implementation already—laboratory closures, reduced test menus and longer wait times for care."

The LAB Act Bill

In addition to litigating and seeking to negotiate with CMS, the lab industry has been working with Congress in hopes of securing much needed PAMA relief. And it now appears that those efforts have borne fruit. In late June, a bipartisan group of U.S. House members introduced the LAB Act bill to delay the next round of PAMA reporting for one year.

Congressmen Leading the Fight for PAMA Relief

The six Congressmen that proposed the LAB Act come from both parties and include Rep. Scott Peters (D-Calif.), Rep. Gus Bilirakis (R-Fla.), Rep. Bill Pascrell (D-N.J.), Rep. Kurt Schrader (D-Ore.), Rep. Richard Hudson (R-N.C.) and Rep. George Holding (R-N.C.).

Explanation: The most recent PAMA payment data collection period just ended, running from January 1, 2019 to June 30, 2019. Labs are slated to report this payment data between Jan. 1, 2020 and March 31, 2020, with rates based on that data to be implemented starting Jan. 1, 2021.

The LAB Act would delay that process by a year during which new payment data reporting requirements would be explored. The bill also calls for the National Academy of Medicine to provide recommendations to Congress on less burdensome data collection methods and representative reimbursement rate calculations that result in the reliable, sustainable, market-based system originally intended by Congress.

NIR

Glenn S. Demby, Executive Editor

Paula Santonocito, Contributing Editor

Elayne Demby, Contributing Editor

Lori Solomon, Contributing Editor

Paula Santonocito, Contributing Editor

Barbara Manning Grimm, Managing Editor

Myra Langsam, Business Development

Michael Sherman, Director of Marketing

Jim Pearmain, General Manager

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

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.

"The LAB Act is a meaningful step forward to achieving comprehensive PAMA reform for clinical laboratory services. We applaud Reps. Peters, Bilirakis, Pascrell, Schrader, Hudson and Holding for their leadership in protecting Medicare beneficiaries and urge Congress to prioritize the LAB Act before seniors face another round of cuts," said Khani in the press release.

Surviving PAMA: Keep an Eye on Industry Disruptors

A talking point of a G2 Lab Institute 2018 presentation deserves closer attention, especially given its implications for the lab industry.

"Advantages and Disadvantages Confronting Labs in a Post-PAMAgeddon World," was the title of the Lab Institute session led by **Lâle White**, executive chairman and CEO of XIFIN, a health information technology company that leverages diagnostic information to improve the quality and economics of healthcare.

Changing Landscape

As part of her presentation, White looked at industry disruptors, with a focus on how consumerism and data analytics shape the future of healthcare delivery.

She cited these partnerships as examples of macro trends, noting the following activity:

Amazon – Chase – Berkshire Hathaway Alliance

- Already obtained licenses for durable medical equipment (DME) distribution in 48 states
- Could partner with pharmacy benefit managers (PBMs)
- Amazon and Echo capabilities (schedule office visit; virtual house calls)
- AI based in-home healthcare and diagnostics

CVS – Aetna Merger and Cigna/Express Scripts

- Both mergers designed to control rising medical costs and provide data analytics
- CVS has 9,700 pharmacies and 1,100 walk-in clinics (Minute Clinic vs. ER option or physician visit)
- Three largest PBMs become vertically integrated with insurers (United Health Care/Catamaran)

Walmart – Humana

- Combining retail pharmacies with a PBM

Continued on page 4

Enforcement Trends: Investment Return on Fraud Fighting Continues to Decline, *from page 3*

- Data analytics building a 360 view of consumer
- Medicare Advantage growth – better care at lower cost
- Delivering care close to consumer

Pharma Invests in Labs (Novartis, Roche, Opko)

- Companion deals drive therapeutic drug sales
- Big Data (next-generation sequencing) identifies cancer related DNA
- Big Data helps physicians optimize test orders and treatment choices
- Big Data helps manage population health and control medical costs

Implications of Disruption

White discusses these partnerships in relation to the Protecting Access to Medicare Act (PAMA), but arguably this disruption will have far-reaching impacts on healthcare and diagnostic testing.

Going forward, the healthcare industry, including labs, will be driven by:

- consumer preference for convenience;
- solutions that allow for increased capture and sharing of data;
- solutions that streamline care;
- attention to cost control; and
- technology and alliances that enable all of the above.

This is not an "in the future" scenario – it's happening now.

Is your lab prepared?

FOCUS ON:

State AGs Break New Ground by Teaming Up to Enforce HIPAA

Lab managers and compliance officers take note: For the first time ever, state attorneys general (AGs) have banded together to go after a health care provider for HIPAA violations. Although the defendant was a medical software firm, the same enforcement strategy could very easily apply to labs as well. Here's a look at a groundbreaking new case and what it may portend. (See page 6 for a related story on new state HIPAA laws.)

The MIE Data Breach

The focal point of the case is a medical software provider named Medical Informatics Engineering (MIE) which licenses a web-based

FOCUS ON:

electronic health record application called WebChart and its subsidiary, NoMoreClipboard (NMC), which provides patient portal and personal health record services to healthcare providers allowing patients to access and manage their health information. MIE installed two generic accounts, one having a shared password of "tester" and the other having a shared password of "testing." Neither included a unique user identification name. These accounts were flagged as "high risk" by a formal penetration test conducted in January 2015. But MIE decided not to eliminate them because it didn't want to deny a client request for the capacity to login without using unique usernames and passwords.

Later that year, hackers used the generic accounts to launch an SQL injection attack and insert malware on MIE's system, compromising the electronic protected health information (ePHI) of approximately 3.5 million individuals.

The Legal Action against MIE

The federal Office of Civil Rights (OCR) cited MIE for HIPAA violations resulting in a $100,000 settlement. Although it's not unusual for states to file separate privacy law charges on behalf of state residents harmed by the breach, there had never been a multistate HIPAA data breach lawsuit before. So, it was pretty eye-opening when AGs from no fewer 16 different states (including Arizona, Arkansas, Connecticut, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Michigan, Minnesota, Nebraska, North Carolina, Tennessee, West Virginia and Wisconsin) banded together to go after MIE in Indiana federal court.

In addition to wielding their statutory authority to enforce HIPAA, the state AGs brought claims under their respective data breach and personal information protection statutes. Result: MIE was accused of 38 separate counts of state law violations stemming from the same breach. Outnumbered and out-resourced, MIE agreed to pay $900,000 to settle all the charges. It also agreed to implement an onerous corrective action plan.

Why Labs Are Also Vulnerable

As if HIPAA and security breaches weren't already damaging enough, the potential for multistate enforcement stemming from a single breach ups the ante exponentially. Labs are especially vulnerable given:

- Their reliance on web-based applications for ePHI management that hackers love to target; and
- The fact that they manage ePHI of residents from multiple states.

State Law Round-up: New Privacy Breach Notification Laws

As illustrated by the recent MIE settlement (see the story on page 4), security breaches involving patients' electronic protected health information (ePHI) exposes your lab to liability risks under not just HIPAA but also state medical privacy and even consumer protection laws. In 2019, no fewer than nine states have proposed, adopted or are about to adopt strict new breach notification laws and other privacy protection laws that could potentially be used to prosecute labs for violations involving the private information of residents of the state.

Illinois: Breach Notification (SB 1624)

New requirement under the Personal Information Protection Act that businesses notify the state Attorney General of privacy breaches involving at least 500 Illinois residents. Status: Passed the legislature and the Governor is expected to sign it.

Maine: Internet Consumer Data Protection (LD 946)

New Act to Protect the Privacy of Online Consumer Information bans internet service providers (ISPs) from using, selling or distributing consumer data without their consent or attempting to pressure customers into letting the ISPs selling their data, e.g., via a penalty or discount. Status: Takes effect July 1, 2020.

Maryland: Breach Notification (HB 1154)

New rules under the Personal Information Protection Act banning a business that's responsible for a data breach from charging the data owner or licensee for information needed for notification and using information about the breach for purposes other than providing notification of the breach, protecting or securing the personal information involved and taking measures to avoid future breaches. Status: Takes effect Oct. 1, 2019.

Massachusetts: Breach Notification (HB 4806)

New requirement that businesses:

Offer free credit monitoring for 18 months if a breach involves a resident's Social Security number;

Provide breach notifications on a rolling basis if necessary to avoid delay;

Identify the third party that owns the exposed data, if any; and

Notify state regulators if they maintain "a written information security program."

Status: Took effect April 11, 2019.

New Jersey: Scope of Protected Information & Breach Notification (S. 52)

Expands the definition of "personal information" protected by the privacy law to include usernames, email addresses, passwords, and security

questions and answers affiliated with an individual's online account. Also requires businesses to notify New Jersey residents affected by a breach and direct them to promptly change their log-in credentials associated with that business, and any other accounts in which they use the same username or email address, password or security questions/answers. Bans business from using email for notification if the victim's email account was the subject of the security breach. Status: Takes effect Sept. 1, 2019.

New York: Scope of Protected Information & Breach Notification (SB5575B)

Proposed amendments to Stop Hacks and Improve Electronic Data Security Act to:

Expand security breach protection to biometric data, account numbers and credit or debit card numbers without a security code, and usernames, email addresses, passwords, and security questions and answers;

Exempt businesses from issuing breach notifications when: (a) the breach results from an unauthorized person's inadvertent disclosure and the business reasonably finds that the breach doesn't pose any financial or emotional harm; or (2) the business has already sent out notifications under federal or other New York regulations;

Expand definition of "breach" to include unauthorized access, in addition to acquisition, of private information;

Require businesses to take "reasonable safeguards" to protect information through procedures such as: designating and training employees to implement and oversee security programs; regularly testing the effectiveness of security programs and making necessary modifications; and promptly deleting private information that's no longer used;

Extend the statute of limitation for the New York Attorney General to prosecute a business for a violation from two years to three.

Status: Proposed on May 9, 2019.

Oregon: Scope of Protected Information & Breach Notification (SB 684)

Stricter breach notification requirements of vendors under Oregon Consumer Information Protection Act including requiring them to notify any contracted "covered entity" within 10-days of discovering a breach of security; must also notify the Attorney General if the breach involves more than 250 consumers or the number of individuals effected is unknown. Expands definition of "personal information" to include "user names or other means of identifying a consumer for the purpose of permitting access to the consumer's account." Status: Effective Jan. 1, 2020.

Texas: Breach Notification (HB 4390)

Requires businesses to send Texas Identity Theft Enforcement and Protection Act law breach notifications to affected individuals without "unreasonable

Continued on page 8

State Law Round-up: New Privacy Breach Notification Laws, *from page 7*

delay" and no later than 60 days after identifying a breach. Must also notify Texas Attorney General within 60 days if the breach affects at least 250 Texas residents. Status: Effective Jan. 1, 2020.

Washington: Scope of Protected Information & Breach Notification (HB 1071)

Expands definition of "personal information" protected by privacy laws to include birthdate, unique private keys for signing electronic records, student, military or password identification numbers, medical information, biometric information, and online login credentials;

Allows businesses to send breach notifications by email unless the breach involves the credentials associated with that email account;

Requires notice to the Attorney General of breaches affecting more than 500 residents that identify the type of information exposed, the time frame of exposure, the steps taken to fix the breach, and a copy of the notice sent to affected individuals;

Cuts the notification deadline from 45 to 30 days.

Status: Takes effect March 1, 2020

Labs IN COURT

A roundup of recent cases and enforcement actions involving the diagnostics industry

Feds Salvage $2.5 Million from $90 Million Genetic Testing Scam

Case: The feds accused Nevada Heart & Vascular Center (NHVC) of taking kickbacks from a pair of now defunct genetic testing companies Natural Molecular Testing Corp. and Iverson Genetic Diagnostics, Inc., in exchange for referrals of Medicare patients over a roughly two-year period starting in September 2012. Rather than risk trial, NHVC shelled out $2.5 million to settle the case.

Significance: The $2.5 million recovered from NHVC is chump change compared to the $90 million in fraudulent payments ($71 million to Natural Molecular and $19 million to Iverson) allegedly made to the labs that declared bankruptcy before CMS could get any of that money back. Genetic test labs going bankrupt after being busted for Medicare fraud has become a pattern with other notable examples including Texas-based Companion Dx and Pharmacogenetics Diagnostic Laboratory LLC in Louisville.

Florida Marketer Convicted of Genetic Testing Kickbacks

Case: Speaking of genetic testing fraud, a federal jury found the owner of a Tampa medical marketing firm guilty of taking part in a $2.2 million scam involving payment of cash bribes to medical clinics in exchange for referral

of DNA swabs collected from Medicare patients. The owner allegedly instructed the clinics to collect DNA from all patients regardless of medical necessity.

Significance: In addition to the fact that it went to trial, the other notable thing about this case is the financial dimension. What began as a series of direct cash payments evolved in the course of one year to a sophisticated arrangement involving shell companies. During the trial, the prosecution contended that the defendant went from ATM to ATM across south Florida to make separate withdrawals of thousands of dollars in an effort to conceal the scam and stay under the $10,000 deposit threshold for filing federal currency transaction reports to the US Treasury Dept.

Lab Owner Gets 30 Months, $3 Million Fine for Masterminding Kickback Scheme

Case: The 62-year-old Illinois man paid "marketers" $150 to $200 (50% of the profits) per urine and saliva sample for referrals of Medicare and Medicaid patients to his labs operating in Missouri and other states under the name of AMS Medical Laboratory Inc. Some test orders listed doctors who never saw the patient and had no idea their names were being used for the scam.

Significance: In April, a federal jury in St. Louis convicted three of the marketers who were on the receiving end of the 50% profit payments. Altogether, 10 defendants have been charged in the case, including a doctor found guilty of conspiracy and four counts of health care fraud at trial last October.

IBM Shells Out $14.8 Million to Settle Claims of Overhyping ACA Software

Case: The DOJ contends that IBM and Cúram Software, the company it acquired in 2011, misrepresented the capabilities of its products to win a subcontract to develop an Affordable Care Act health insurance exchange website and information technology platform for the Maryland Health Benefit Exchange in February 2012. The alleged claims were made during a product presentation one month earlier demonstrating the software's capability to calculate tax credits and integrate with another subcontractor's health plan shopping software. The claims proved unfounded and, after a series of mishaps with the product, the Maryland Health Benefit Exchange terminated the contract in October 2013.

Significance: The Maryland health insurance exchange rollout proved a disaster and IBM, as the provider of the technology, is being blamed for the problems. Of course, several other states experienced significant health insurance exchange website failures, but the Maryland case was particularly high profile due in part to the parties involved including not only IBM but also then Governor Martin O'Malley and Lt. Governor Anthony Brown, who were running for President and Governor, respectively. Each man would go on to lose his election bid due in part to the negative publicity from the exchange fiasco.

Continued on page 10

Labs in Court, *from page 10*

CMS Finds Lab Safety Violations at Texas Hospital

Case: CMS has found the University of Texas MD Anderson Cancer Center out of compliance with Medicare conditions of participation with regard to lab services. The inquiry began in December 2018 after MD Anderson reported an adverse event related to a blood transfusion to the FDA, which then referred the case to CMS for a separate investigation. Although the details haven't yet been made public, CMS has apparently required the lab to submit a plan for remedying the problems by June 18.

Significance: Although the lab deficiencies were the only ones requiring a corrective action plan, CMS reportedly uncovered other conditions of participation violations involving MD Anderson's governing body, quality assessment and performance improvement program and patient rights. CMS hasn't threatened to revoke its Medicare status but MD Anderson will be subject to Texas health department investigation to ensure it complies with the conditions.

Enforcement Trends: Investment Return on Fraud Fighting Continues to Decline

Although it's still a profitable endeavor, enforcing federal health care fraud laws isn't providing the investment returns of yesteryears. That's the main takeaway of the new joint HHS and DOJ report on the financial performance of the Health Care Fraud and Abuse Control Program (Program) during fiscal year 2018.

ROI Keeps Trending Down

Arguably, the most significant metric in the report is the Program's return on investment (ROI). Continuing recent trends, ROI for FY 2018 dipped to $4.00 for every dollar spent, as compared to $4.20 in FY 2017. That's the sixth annual decline in a row since Program ROI peaked at $8.10 in FY 2013.

Annual Program ROI, FY 2013 to FY 2018

FY 2013	FY 2014	FY 2015	FY 2016	FY 2017	FY 2018
$8.10	$7.70	$6.10	$5.00	$4.20	$4.00

"Because the annual ROI can vary from year to year depending on the number and type of cases that are settled or adjudicated during that year, DOJ and HHS use a three-year rolling average ROI for results contained in the report," the agencies explain in their report. But while rolling averages may take off some of the edge for a particular year, they can't conceal the long-term trend. Simply put, the return on enforcement dollars is only about 50% of what it used to be just six years ago.

By The Numbers

Total recoveries from health care fraud judgements and settlements topped $2.3 billion in FY 2018, slightly down from the previous year. The chart below summarizes the key year-to-year findings.

Metric	FY 2018	FY 2017
Total recoveries	$2.3 billion	$2.4 billion
New DOJ criminal health care fraud investigations	1,139	967
New DOJ civil health care fraud investigations	918	948
New criminal cases filed	572	439
Convictions	872	639
Criminal actions resulting from OIG investigations	679	788
Exclusions issued by OIG	2,712	3,244

While these accomplishments are noteworthy, they come at a higher price than in recent years.

News: New FDA Guidance Tells IVD Makers How to Test for Biotin Interference

On June 13, the FDA issued a draft guidance explaining how makers of in vitro diagnostic devices (IVDs) should perform biotin interference testing and communicate testing results to labs, clinicians and other device end-users. Here are the key takeaways.

What Is Biotin Interference

Biotin, aka vitamin B7, is a common ingredient in multi-vitamins, prenatal vitamins and dietary supplements. Falsely high or falsely low test results have been known to occur in patients who consume high levels of biotin from such products. These results can lead to inappropriate patient management or misdiagnosis.

The FDA Response

The FDA first expressed concern about biotin interference on IVD performance in a November 2017. Since then the agency has worked with manufacturers of currently marketed devices to address the problem.

As the guidance points, devices using biotin/avidin technology have historically been assessed for biotin interference at the normal recommended daily doses of biotin of 30 µg per day, which results in plasma/serum biotin levels of < 1 ng/mL. Nevertheless, "unanticipated biotin interference with the performance of some IVDs due to consumer use of dietary supplements" have in some instances revealed much higher levels; extremely high biotin doses also have been observed of up to 300 mg per day, which results in plasma/serum biotin levels of > 1000 ng/mL.

Continued on page 12

New FDA Guidance Tells IVD Makers How to Test for Biotin Interference, *from page 11*

The FDA's 6 Recommendations

The first five of the six recommendations contained in the new draft guidance involve testing methods. Specifically, the FDA recommends that:

Sponsors contact the appropriate Center for Biologics Evaluation and Research (CBER) or Center for Devices and Radiological Health (CDRH) review division when biotin interference at clinically relevant analyte and biotin concentrations is demonstrated;

Designing studies to test for biotin interference in accordance with the designs set out in the most current version of Clinical Laboratory Standards Institute (CLSI) EP07, Interference Testing in Clinical Chemistry; Approved Guideline;

Concentrations of biotin be evaluated up to 3500 ng/mL to reflect current trends in biotin consumption;

Test samples include analyte levels near the medical decision point(s) of the device;

The concentration of biotin at which no interference is detected be determined for assays that are susceptible to biotin interference at concentrations less than 3500 ng/mL.

The draft guidance also recommends including information on biotin interference testing in the labeling of the device, including the percent difference or bias at each concentration tested for both qualitative and quantitative assays and the consequence of biotin interference, e.g., any falsely elevated or falsely depressed observed.

Takeaway

As with other FDA guidance documents, the new draft guidance doesn't carry the effect of law. The recommendations are just that—recommendations—not mandates (unless specific regulatory or statutory requirements are cited). Even so, because the guidance incorporates the FDA's expectations and standards, IVD makers are well advised to take it seriously.