G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

# NATIONAL LAB REPORTER™

Formerly: National Intelligence Report

Covering Government Policy For Diagnostic Testing & Related Medical Services

Celebrating Our 42nd Year of Publication

Vol. 21, Iss. 8, August 2021

## IN THIS ISSUE





## LDTs: VALID and VITAL Are Back in Play—and This Time One of Them Might Actually Pass

The COVID-19 pandemic exposed the truth of something the lab industry has known and publicly stated repeatedly for over a decade: The FDA is ill-equipped to regulate Laboratory Developed Tests (LDTs) and allowing it to continue to do so, at least under its current model, stifles innovation and keeps needed tests off the market. Of course, many members of Congress on both sides of the aisles have shared in this knowledge. And now an increasing number of their colleagues do, as well. Accordingly, the renewal of efforts to impose legislative order might actually come to fruition this time. The spearhead of those efforts, at least for now, is the reintroduction of a pair of bills that failed to take hold the last time they were on the table: the VALID and VITAL Acts. Here's a quick briefing on the 2021 version of each bill and how it proposes regulate LDTs.

### The FDA's Ham-Handed Regulation of LDTs

The original Food Drug & Cosmetics Act legislation doesn't provide for regulation of lab tests. The FDA claims that its authority to regulate LDTs, aka, *in vitro* clinical tests (IVCTs), is rooted in its

*Continued on page 2*

## Privacy: Health Care Data Breaches Hit a New High in First Half of 2021

While health care data breaches have become an all-too-common occurrence, the problem seems to be getting worse. According to the HHS' Office for Civil Rights (OCR), there have already been 360 federally reported data breaches involving health information in the first half of 2021, the highest total for the first six months of a year since the government began tracking this data over a decade ago. Protected health information of nearly 23 million patients have

*Continued on page 11*

LDTs: VALID and VITAL Are Back in Play—and This Time One of Them Might Actually Pass, *from page 1*

power to regulate medical devices. To fit this square peg into a round hole, the agency clears LDTs via the 510(k) premarket review pathway. Since there's no statutory or regulatory basis for any of this, the FDA makes up the rules as it goes along. Adding to the arbitrariness is that the agency exercises its oversight of LDTs by issuing informal guidance rather than following the strict notice of rulemaking process designed to ensure comment and review for federal regulation. In parallel, the FDA has also practiced what it calls "enforcement discretion" by deferring regulation of most LDTs to CMS under CLIA.

One of the earliest legislative efforts to clean up the mess was a bill called the Diagnostic Accuracy and Innovation Act (DAIA) that would have removed diagnostic tests from the definition of a medical device and thus placed it outside the scope of the 510(k) pathway. After getting input from the lab and diagnostics industry, legislators submitted the DAIA draft to FDA for technical assistance. Instead of the usual technical edits, however, the FDA proposed an entirely new framework to overhaul the 510(k) premarket review program while maintaining its own authority of IVCTs.

Although the FDA's proposed scheme didn't gain much traction, DAIA's sponsors incorporated some of the agency's ideas, including pre-certification, into a 2018 bill called the Verifying Accurate, Leading-edge IVCT Development (VALID). In March 2020, amid grumblings about the FDA's slow, haphazard and overall inadequate response to the pandemic-fueled need for new SARS-CoV-2 tests, VALID was reintroduced.

While the 2020 bill went nowhere, new impetus for reform came from a surprising source in August of that year when the U.S. Department of Health and Human Services (HHS) issued a determination that the FDA can't require premarket review of LDTs without notice and comment rulemaking. For the lab industry, the determination served as vindication; however, it didn't solve the larger problem of LDTs regulation.

## The VALID Act of 2021

Unlike DAIA, the VALID Act of 2021 recognizes FDA authority to regulate IVCTs, which would become a new product category consisting of LDTs and test kits. VALID would create a risk-based framework for IVCT regulation:

**High-Risk Tests:** High-risk tests, like novel assays, would be required to go through premarket review to verify analytical and clinical validity.

**Lower-Risk Tests:** VALID would establish a separate technological certification program for lower-risk tests, as well as a new system allowing hospitals and labs to submit their tests electronically.

**Emergency Use Tests:** To speed up the EUA bottleneck, validated tests would be authorized to use for emergency purposes pending review of their EUA clearance, analogous to the notification process FDA used

NLR

Glenn S. Demby, Executive Editor

Barbara Manning Grimm, Managing Editor

Andrea Stowe, Business Development

Jim Pearmain, General Manager

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher



***National Lab Reporter***
(ISSN 2332-1466) is published by G2 Intelligence, Plain Language Media, LLLP, 15 Shaw Street, New London, CT, 06320.
**Phone:** 888-729-2315
**Fax:** 855-649-1623
**Web site:** www.G2Intelligence.com.

for certain COVID-19 tests during the early days of the public health emergency.

**Grandfathered Tests:** Qualifying LDTs offered for clinical use before enactment of the legislation would receive "grandfathered" status and not require premarket review, provided that they:

- Carry a disclaimer on the label;
- Aren't modified; and
- Aren't flagged by the FDA as posing a special concern.

**Transitional Tests:** IVCTs first offered between the date VALID is enacted and 90 days after it takes effect would be allowed to remain on the market as "transitional" IVCTs, provided that the test maker submits a timely marketing application to the FDA.

Other key features of the 2021 version of VALID:

- Establishment of test design and quality requirements for IVCTs, equivalent to the current Quality Systems requirements for medical devices;
- Creation of a new process that the FDA can use to request information from an otherwise exempt IVCT, such as a transitional or grandfathered test, in certain situations;
- Authority of FDA to participate in collaborative communities for purposes of "facilitating community solutions and decision-making" for IVCTs;
- A requirement that FDA create and maintain an IVCTs database that's more extensive than the current device registration and listing database; and
- New IVCT adulteration, misbranding and postmarket surveillance requirements mirroring current rules that apply to medical devices.

## The VITAL Act

VALID isn't the only LDTs regulation bill on the table. First introduced by Senator Rand Paul (R-KY) in March 2020, the newly reintroduced Verified Innovative Testing in American Laboratories (VITAL) Act would transfer the FDA's regulatory powers over LDTs to HHS. Supporters of the bill believe that the FDA's slow response in expanding access to SARS-CoV-2 virus tests during the pandemic reaffirms the need for stripping the agency of power to regulate LDTs. "When we face a health emergency, government should trust academic, community and public health labs to do what they are already trained and certified to do," noted Senator Paul in a press release at the time. "With all of the debates about how government should respond, here's one thing it can stop doing: piling counter-productive bureaucratic hurdles in the way of our medical professionals."

*Continued on page 4*

LDTs: VALID and VITAL Are Back in Play—and This Time One of Them Might Actually Pass, *from page 3*

Subsequent FDA management of the EUA process seemed to vindicate and strengthen the drive to get the agency out of the business of regulating LDTs. In August 2020, HHS issued a determination stating that the FDA cannot require premarket review of LDTs without notice and comment rulemaking. While not eliminating FDA regulatory authority over LDTs, the HHS determination barred the agency from its traditional—and to most in the industry—infuriating practice of exercising that authority via website guidelines and other informal pronouncements serving as shortcuts around the burdensome notice and comment rulemaking protocols.

"In the earliest and most frightening days of the pandemic, CLIA-accredited academic clinical laboratories could have used their valuable expertise and resources to expand SARS-CoV-2 diagnostic testing in their communities, but were unable to do so due to inappropriate FDA restrictions," she continued. "Priceless weeks were lost, making the urgency to address these issues now even more clear."

### Takeaway

*The FDA's handling of COVID-19 tests in response to the pandemic exposed the truth of what the lab industry has been saying for over a decade: The agency's ham-handed and ad hoc regulation over LDTs thwarts innovation and keeps vitally needed new tests from reaching the market. While the VALID and VITAL Acts aren't new, the impetus and urgency to do something about FDA LDTs regulation most certainly are. This suggests that change is really going to happen this time.*

*What exactly that change will be, however, remains unclear. Maybe the FDA will be stripped of its LDTs regulatory powers; but even if that doesn't happen, the agency will have to follow a set of specific ground rules and procedures designed to ensure that new lab tests get to market more rapidly. The new transparency and predictability should also go a long way toward encouraging lab companies to innovate and develop new testing products.*

## COVID-19: Labs Sue National Insurers for Not Reimbursing COVID-19 Testing Claims

Medical testing lab Genesis Laboratory Management is suing UnitedHealth Group for not paying claims for COVID-19 tests. The lawsuit, filed on June 2 in the U.S District Court for the district of New Jersey, claims that United Health and its Oxford Health Plans unit didn't

reimburse 51,000 claims for COVID-19 tests, in violation of both state and federal laws. New Jersey-based Genesis also claims that UnitedHealth issued burdensome requests for medical reports. "Genesis has been, and continues to be, harmed by United's failure to pay valid claims that Genesis submitted to United for reimbursement for services to United's members and beneficiaries," the complaint states.

Meanwhile, it's been reported that UnitedHealthcare recently sent out a letter reassuring its providers saying that it will reimburse pediatric and family medicine clinicians for COVID-19 tests administered in 2021.

## The Genesis Lawsuit

The federal *Families First Coronavirus Response Act* (FFCRA) and *Coronavirus Aid, Relief and Economic Security* (CARES) *Act* require group health plans and health insurance issuers to cover COVID-19 testing services free of deductibles, copayments or any other charges to patients.

In Genesis' complaint, the molecular diagnostic and anatomic pathology lab that provides coronavirus testing services is an out-of-network provider, "notwithstanding multiple attempts to become in-network with United." UnitedHealth paid the majority of the lab's claims for March, April and May 2020, but it began "systematically denying" payment for claims starting in June, even though the lab didn't change its testing, billing or documentation practices.

Genesis contends that it has never refused to treat United members despite the insurer's failure to pay and despite its demands that the lab "produce voluminous patient treatment and other records with tight response time demand."

In addition to FFCRA and CARES, Genesis claims that UnitedHealthCare violated a pair of New Jersey state laws, including the:

- *Healthcare Information Networks and Technologies Act*; and
- *Health Claims Authorization, Processing and Payment Act*.

The complaint also accuses UnitedHealthCare with breach of implied contract, breach of the covenant of good faith and fair dealing, unjust enrichment, quantum meruit and promissory estoppel.

## Takeaway

*UnitedHealthCare, which has yet to answer the complaint, isn't the only national insurer being sued for not paying COVID-19 test claims. Cigna, is facing similar claims from a radiology lab in New Jersey. The lawsuit accuses Cigna of wrongfully denying payment for nearly $400,000 in services provided to COVID-19 patients.*

# Enforcement: Fraud Recoveries Grow as Feds Target Telemedicine and COVID-19 Add-On Test Scams

Despite the COVID-19 pandemic and continued sequestration of enforcement funds, the federal Health Care Fraud and Abuse Control Program (Program) reversed recent trends and recovered more money in FY 2020 than it had the year before. In fact, recoveries for the year reached nearly $3.1 billion, the highest return since 2016. Here's a briefing for lab compliance managers on the July 14 OIG report and what it says about the current state of federal health care fraud enforcement.

## ROI Increases for Second Year in a Row

The Program was created as part of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) under the joint direction of the Attorney General and HHS Secretary, acting through the OIG, to coordinate federal, state and local law health care fraud and abuse enforcement activities. The Annual Report describes the Program's financial performance in the previous fiscal year. While the narrative is somewhat helpful, the real value of these annual reports, at least from a lab compliance officer's perspective, are the enforcement and recovery statistics. Tracking these numbers over a three-year period gives a good sense of the current energy and direction of federal fraud activity, including with regard to labs.

Among the most significant metrics in the annual report is Program ROI, which measures how much money the Program returns for every dollar invested. Program ROI is calculated by dividing the total monetary results to the federal government in judgments, sentences, settlements and other recoveries (not including relator payments in *qui tam* lawsuits) by the annual appropriation for the Program Account in a given year (not including portions of CMS funding dedicated to the Medicare Integrity Program). Because the annual ROI tends to vary from year to year depending on the number and type of cases that are settled or adjudicated during the year, DOJ and HHS use a three-year rolling average ROI for results contained in the report.

And since FY 2013 when ROI peaked at $8.10, ROI has been trending steadily down, with five consecutive years of decline. FY 2019 finally saw the losing streak come to an end, with ROI increasing from $4.00 to $4.20 in 2019. The upward movement continued this year, with the three-year rolling average ROI reaching $4.30 in FY 2020.

**Annual Program ROI, FY 2013 to FY 2020 (3-Year Rolling Average)**

| FY 2013 | FY 2014 | FY 2015 | FY 2016 | FY 2017 | FY 2018 | FY 2019 | FY 2020 |
|---|---|---|---|---|---|---|---|
| $8.10 | $7.70 | $6.10 | $5.00 | $4.20 | $4.00 | $4.20 | $4.30 |

## By the Numbers

During FY 2020, the federal government won or negotiated nearly $3.1 billion ($3,075,834,684) in health care fraud judgments and settlements. That's up from $2.6 billion in FY 2019, even though the number of convictions during the same period actually declined from 528 to 440. Civil actions, which have traditionally been the cash cow of federal health care fraud enforcement efforts, were up sharply in FY 2020, from 1,112 to 1,498, which portends higher recovery levels in the years ahead when these new actions yield judgments and settlements. However, exclusion numbers were fell off by nearly 25 percent to 2,148.

| Metric | FY 2020 | FY 2019 | FY 2018 |
|---|---|---|---|
| Total recoveries | $3.1 billion | $2.6 billion | $2.3 billion |
| New DOJ criminal health care fraud investigations | 1,148 | 1,060 | 1,139 |
| New DOJ Civil Health care fraud investigations | 1,498 | 1,112 | 918 |
| New Criminal cases filed | 578 | 485 | 572 |
| Convictions | 440 | 528 | 872 |
| Exclusions issued by OIG | 2,148 | 2,640 | 2,712 |

The increases in most of the enforcement metrics occurred even though sequestration reduced the enforcement funding available to the DOJ, FBI, HHS and OIG. A total of $11.0 million was sequestered from the Program in FY 2020, for a combined total of $150.6 million in mandatory funds sequestered in the past eight years. Including funds sequestered from the FBI ($70.0 million in the past eight years), $220.6 million has been sequestered from mandatory Program funds since FY 2013.

## Takeaway and Impact on Labs

*Although labs are a perennial favorite target for enforcers, they were especially prominent for the wrong reasons in FY 2020. Genetic and other testing labs played a prominent role in the Operation Rubberstamp national takedown of telemedicine fraud, the biggest takedown collaboration in history.*

*In addition to the usual kickback and Stark recoveries that take place each year, enforcers targeted COVID-19 add-on tests, i.e., high-priced and medically unnecessary tests carried out on patients tested for SARS-CoV-2, including the Respiratory Protection Panel (RPP), antibiotic resistance tests, genetic testing and cardiac panels CPT codes. "Providers are also billing respiratory, gastrointestinal, genitourinary, and dermatologic pathogen code sets with the not otherwise specified code CPT 87798," according to the report.*

# Telehealth: Newly Proposed Medicare Part B Physician Fee Schedule Contemplates Making COVID-19 Telehealth Changes Permanent

On July 13, 2021, CMS published its proposed physician fee schedule rule for FY 2022. One of the key items is the proposal to make the temporary change allowing Medicare providers to deliver healthcare services via telehealth a permanent part of Medicare Part B.

## The Proposed Medicare Changes

During the public health emergency (PHE), Congress added the home of the beneficiary as a permissible originating site for telehealth services for the purposes of diagnosis, evaluation or treatment of a mental health disorder. In addition to updating the fee schedule, the proposed CY2022 rule would allow certain services added to the Medicare telehealth list to remain on the list until the end of December 2023. This would allow CMS to continue to evaluate whether the temporary expansion of telehealth services adopted as an expediency during the pandemic should be permanently added to the telehealth list after the PHE ends.

## The 4 Proposed Changes for Mental Telehealth

CMS is also proposing the following four rules for mental telehealth services:

### 1. The 6-Months' Requirement

Under the CMS proposal, the physician or practitioner furnishing mental health telehealth services, would have to provide the patient in-person, non-telehealth services within six months before the initial telehealth service and at least once every six months after that. CMS is seeking comments on whether a different interval is appropriate for mental health services furnished through audio-only communication technology.

### 2. Audio Only Communication Technology

CMS is looking into amending current requirements for interactive telecommunications systems to allow audio-only communication technology for telehealth diagnosis, evaluation or treatment of mental health disorders of established patients in their homes. The proposal would limit the use of an audio-only interactive telecommunications system to mental health services furnished by practitioners who have the capability to furnish two-way, audio/video communications where the beneficiary is incapable of using or doesn't consent to the use of two-way audio/video technology.

### 3. New Billing Modifiers

The CMS proposal would include a new modifier for billing services furnished using audio-only communications to certify that the practitioner

had the capability of providing two-way audio/video communication, but the beneficiary was incapable of using or didn't consent to use of that technology. There would also be a new modifier for services furnished through audio-only technology due to beneficiary choice or limitations.

### 4. Rural Health Clinics Payments

CMS would allow Rural Health Clinics and Federally Qualified Health Centers to use the same methods they do to report and receive payment for in-person mental health visits for visits furnished via real-time telecommunication technology, including audio-only visits when the beneficiary is incapable of or doesn't consent to the use of video technology.

### Proposed Changes for MDPP

CMS also proposed changes to its Medicare Diabetes Prevention Program (MDPP) "to make delivery of MDPP services more sustainable and to improve patient access by making it easier for local suppliers to participate and reach their communities." Specifically, CMS is proposing to:

- Continue to waive the provider enrollment Medicare application fee the way it has during the PHE on or after January 1, 2022, and beyond the PHE;
- Shorten the MDPP services period to one year by removing the ongoing maintenance sessions phase (months 13 to 24) of the MDPP set of services for beneficiaries starting on or after January 1, 2022;
- Redistribute a portion of the ongoing maintenance sessions phase performance payments to certain core and core maintenance section performance payments, in conjunction with removing the maintenance sessions phase from the MDPP services. This includes payments for the beneficiary's 5 percent weight loss goal and continued attendance in the core maintenance interval.

If finalized, these changes would apply to beneficiaries who start the MDPP set of services on or after Jan. 1, 2022. Beneficiaries who began participating before December 31, 2021 would continue with the maintenance phase if they maintain their 5 percent weight loss and meet other requirements.

Significantly, these proposals **do not** include reimbursement for MDPP services delivered by telehealth or virtual care programs.

### Takeaway

*CMS is also proposing and/or asking for public comments about:*

- *Changes to the Quality Payment Program that would raise the eligibility threshold, making it more difficult for clinicians to earn bonuses*

*Continued on page 10*

■ Telehealth: Newly Proposed Medicare Part B Physician Fee Schedule Contemplates Making COVID-19 Telehealth Changes Permanent, *from page 9*

*(CMS also unveiled its first seven MIPS Value Pathways, including rheumatology, stroke care and prevention, heart disease, chronic disease management, emergency medicine, anesthesia and lower-extremity joint repairs, such as knee replacements);*

- *The potential phase out of coinsurance for diagnostic tests resulting from scheduled colorectal screenings;*
- *Whether to require additional documentation in the patient's medical record to support the clinical appropriateness of audio-only telehealth; and*
- *Whether CMS should preclude audio-only telehealth for some high-level services, such as level 4 or 5 E/M visit codes or psychotherapy with crisis.*

## Enforcement: Texas Provider Pays $214K for Violating Federal COVID-19 Workplace Protocols

In one of the first of what will likely be a flood of enforcement actions, the Texas parent of an Iowa nursing home has agreed to repay $214,200 in federal monies for not following coronavirus safety protocols during an outbreak at the facility from April through July 2020. Among other things, the nursing home didn't properly screen employees or require them to wear personal protective equipment. According to newspaper reports, three employees exhibiting COVID-19 symptoms and who subsequently tested positive for the virus were allowed to come to work and be near vulnerable residents, 11 of whom died during the outbreak.

### The False Claims Act Connection

The relatively small settlement award belies the importance of this case. What the case illustrates is that failure to follow COVID-19 protocols can result not only in public health fines and penalties but liability under the False Claims Act (FCA). **Explanation:** When you bill Medicare, Medicare, Medicaid and other federal health program, you certify that you're compliant with all applicable laws and regulatory requirements. Accordingly, labs that submitted bills during the pandemic knowing that

they were out of compliance with COVID-19 safety rules run the risk of liability for submitting a false.

However, the settlement in this case was actually based not on FCA liability but on "restitution," which is typically used to describe repayment of money received by mistake. It's also worth noting that the company in this case cooperated in the investigation, which is a highly advisable strategy if your lab comes under investigative scrutiny. In the meantime, continue to follow the COVID-19 screening, PPE and other safety rules scrupulously.

## Privacy: Health Care Data Breaches Hit a New High in First Half of 2021, *from page 1*

been exposed as a result of this breach-fest. By comparison, there were 270 reported breaches involving 8 million patients in all of 2020.

### The Breaches Are Getting Bigger

The OCR tracks breaches across all industries. But, as in past years, healthcare was the number one culprit in the first half of 2021, accounting for 162, or nearly half, of the reported total. Breaches are becoming not only more frequent but also more extensive. And that figure doesn't count breaches that have occurred but not yet been reported—remember that the HIPAA deadline for reporting a data breach is 60 days from discovery.

There were no fewer than five data breaches compromising data of over 1 million patients each. Florida health plan Healthy Kids Corp. reported the biggest single breach, a hacking attack on its web hosting platform exposing the information of 3.5 million applicants and enrollees. That figure includes several thousand online applicants for the plan's Florida KidCare coverage whose street addresses that the hackers "inappropriately accessed and tampered with."

### What's Causing the Breaches

At roughly 70 percent, hacking represents the most common cause of the breaches reported by providers, insurers and their respective business associates. Organizations reporting hacking breaches on their systems included CaptureRx, 20/20 Eye Care Network and American Anesthesiology. In addition to accessing data from organizational systems, several attacks resulted in its actual removal. This may be part of the latest form of ransomware in which hackers remove rather than encrypt patient records and threaten to publish or sell the data if the organization doesn't pay a ransom.

*Continued on page 12*

Privacy: Health Care Data Breaches Hit a New High in First Half of 2021, *from page 11*

**5 Biggest Reported Health Care Data Breaches of 2021 (So Far), by Patients Affected**

| Persons Affected | Organization | Incident |
|---|---|---|
| 3.5 million | Florida Healthy Kids Corp. | Hacking of insurer's network servers |
| 3.25 million | Eye Care Network | Hacking of business associate's cloud servers |
| 1.65 million | NEC Networks (Capture Rx) | Hacking of business associate's network servers |
| 1.47 million | The Kroger Co. | Hacking of provider's network servers |
| 1.26 million | American Anesthesiology | Hacking of provider's emails |

Source: OCR, Breach Report

However, even though hacking incidents are on the rise, the data security problem is far more extensive than that. For one thing, the "hacking/IT incidents" category encompasses not only hacking attacks but also breaches resulting from how an organization's IT system is configured. The remaining 30+ percent of breaches resulted from theft, loss, improper disposal and unauthorized access or disclosure.

## A Call for Action

In May, the American Hospital Association (AHA) issued an advisory calling on the federal government to start a "coordinated campaign" to target perpetrators of ransomware attacks in both the U.S. and abroad. In essence, the AHA urged the government to treat ransomware as a kind of terrorist activity and deploy diplomatic, financial, military and intelligence resources to combat it.

On July 14, the federal government launched StopRansomware.gov, a new interagency website that will provide centralized resources, reports and alerts from the FBI and Cybersecurity and Infrastructure Security Agency (CISA) that health care and other organizations can use to prevent and respond effectively to ransomware attacks.