March 2021

Dear Health Law Section Members:

The Florida Bar Health Law Section ("HLS") website has been updated with December 2020 through February 2021 articles on significant developments in the health law arena that may be of interest to you in your practice.

These summaries are presented to HLS members for general information only and do not constitute legal advice from the Florida Bar or the HLS. HLS thanks the following volunteers who have generously donated their time to prepare these summaries for our members:

- **Amy Morse, Esq.,** ***Morse & Morse, LLC***
- **Ashlee Tising, Esq., Bruce Platt, Esq., & Steve Grigas, Esq.,** ***Akerman LLP***
- **Colby J. Ellis, Esq.,** ***Johnson Jackson PLLC***
- **Daria Pustilnik, Esq.,** ***Kobre & Kim, LLP***
- **George Breen, Esq., Erica Sibley Bahnsen, Esq., Elizabeth Harris, Esq., Robert Hearn, Esq., & Kathleen Premo, Esq.,** ***Epstein Becker & Green, P.C.***
- **Gray W. Rifkin, Esq., EMBA, Chief Legal Officer and Chief Operating Officer,** ***Commonwealth Diagnostics International, Inc.***
- **Ian E. Waldick, Esq.,** ***Oertel, Fernandez, Bryant & Atkinson, P.A.***

Thank you,

Jamie B. Gelfman, Esq., ***Nelson Mullins Riley & Scarborough LLP,*** **HLS Editor in Chief**

Christian Perez Font, Esq., ***Thinkeen Legal, P.A.,*** **HLS Team Editor**

Elizabeth Scarola, Esq., ***Epstein Becker & Green, P.C.,*** **HLS Team Editor**

TABLE OF CONTENTS

EMPLOYMENT-RELATED UPDATES

COVID-19 Vaccination Mandates in the Employment Context

On December 11, 2020, the U.S. Food and Drug administration ("FDA") issued an emergency use authorization ("EUA") for Pfizer-BioNTech's COVID-19 vaccine. On December 18, 2020, the FDA issued a second EUA for Moderna, Inc.'s COVID-19 vaccine.

Because vaccine supplies are limited, states have restricted and prioritized who is eligible for receipt. Most states have determined that health care workers, including those who work at long-term care facilities, should be eligible for vaccinations regardless of their age. Although many of these workers have voluntarily chosen to receive a vaccine, some individuals are refusing to obtain the vaccine for various reasons. As a result, some health care employers might consider requiring their employees to be vaccinated, raising the question as to whether employers may do so legally.

Legal precedent is clear that in ordinary circumstances, an employer can require its employees to obtain certain vaccinations, subject to religious and disability-related accommodations.[1] However, the COVID-19 vaccines are fundamentally different. They have only been approved by the FDA through EUA and not by full licensure. No legal precedent has ever analyzed whether an employer can mandate an employee to take a vaccine that has only been authorized by EUA.

Nevertheless, this legal issue will certainly be presented to a court soon, and there are arguments on both sides of whether such a vaccination mandate is lawful. Employees who do not want to be forced to take the vaccine will likely focus on the fact that the vaccinations have not been vetted fully by the FDA and their consequences are unknown. They will argue that mandating vaccination is dangerous policy and unfair. Such employees may also argue that the statute that authorizes the FDA to grant an EUA requires that the public have "the option to accept or refuse administration of the product."[2] The statute authorizing EUAs requires that the Secretary of the U.S. Department of Health and Human Services "ensure that individuals to whom the product is administered [be] informed" of "the option to accept or refuse administration of the product."[3]

Employees might also raise an argument based on 10 U.S.C. § 1107(a), which gives the President the authority to waive the option of refusal for members of the armed forces.[4] Specifically, employees may argue that why the President would be given authority to override a right of refusal if the right did not exist in the first place.

Finally, employees will likely rely on the fact sheets that are approved by the FDA and accompany the vaccines. These fact sheets, which were prepared by Moderna and Pfizer, state that recipients of the vaccine have the option to refuse or accept it.

Employers, on the other hand, will likely disagree with the employees' reading of the EUA statute. Employers may argue that even if the EUA gives recipients of the product the right to accept or refuse the product, that choice is not guaranteed to be free of consequences. Specifically, employers will likely argue that the "right to refuse" only protects recipients against government compulsion. The EUA statute contains no provision that speaks to whether a private employer may impose consequences on employees who exercise their right to refuse a vaccination.

Employers might try to analogize this situation to an employee's Fifth Amendment rights. An employee testifying in an investigation by his employer that may also have criminal consequences can invoke the Fifth Amendment, but the employer can terminate the employee for failing to cooperate in the private investigation. The right against self-incrimination is not absolute and the employer's action is not government compulsion. Employers would argue that the same logic should apply to an EUA vaccine mandate.

An employer may also make some additional legal arguments to support its authority to require a vaccination mandate. First, the employer might argue that the Occupational Safety and Hazard Act imposes on an employer a general duty to keep the workplace free from hazards and dangers.[5] An employer may view a vaccination mandate as an execution of that duty.

Second, under the Americans with Disabilities Act, employers have the right to exclude from employment any employee who is a direct threat to other employees. Employers might rely on guidance from the U.S. Centers for Disease Control and the Equal Employment Opportunity Commission to argue that unvaccinated individuals are direct threats to other employees and should be excluded from employment. Employers might also argue that vaccinated status is an essential function of the job, especially if the health-care employer serves a vulnerable population.

This is an unprecedented and challenging legal issue that will only become more prevalent as the vaccine rollout continues. It is not yet clear which, if any, of the above arguments courts will find persuasive, but employers debating a vaccine mandate in their workplaces will be watching closely as the courts grapple with this issue.

Submitted by: **Colby J. Ellis, Esq., *Johnson Jackson PLLC***

FRAUD AND ABUSE UPDATES

DOJ False Claims Act Statistics 2020: Over 80% of All Recoveries Came from the Health Care Industry, with Several Substantial Recoveries in the Middle District of Florida

On January 14, 2021, the U.S. Department of Justice ("DOJ") reported its False Claims Act ("FCA") statistics for fiscal year ("FY") 2020.[6] More than $2.2 billion was recovered from settlements and judgments in 2020, the lowest level since 2008 and almost $1 billion less than was recovered in 2019. Over 80% of all 2020 recoveries—amounting to almost $1.9 billion—came from the health care and life sciences industries. Consistent with years past, a large portion of the total recoveries came from cases filed in Florida's federal district courts, including the settlement of several significant cases in the Middle District of Florida, which zigzags across the State of Florida, including Fort Myers, greater Tampa Bay, Orlando, Jacksonville and points in between.

Highest Number of New Filings Ever Reported

Significantly, 2020 saw the largest number of new FCA matters initiated in a single year. The government initiated new FCA matters at its highest rate since 1994, with 250 new cases brought in 2020. Strikingly, the number of government-initiated cases against health care entities more than doubled from 2019 to 2020 and was at the highest level ever reported. Likewise, *qui tam* relators filed 672 new matters in FY 2020, an increase over FY 2019 and the fifth highest number of cases in reported history. *Qui tam* relators filed, on average, almost 13 new cases a week. Of the 672 *qui tam* cases filed, 68% were related to health care.

Qui Tam Filings Continue to Be the Driver

Total recoveries from *qui tam*-initiated actions generated almost $1.7 billion. While the largest recoveries continue to come from cases where the government intervenes, cases pursued by relators post-declination generated more than $193 million in FY 2020, the fifth largest annual recovery in non-intervened cases since 1986. These cases continue to be rewarding for relators; over $309 million in relators' share awards were paid in FY 2020, of which more than $261 million were paid in cases pursued against health care entities.

Areas of Focus

Health care-related recoveries in 2020 focused on cases pursued against drug and medical device manufacturers, managed care providers, hospitals, pharmacies, laboratories, and physicians. As has been the case in previous years, the most significant recoveries came from the pharmaceutical industry and involved allegations of improper patient co-pay amounts and illegal kickbacks. This includes recoveries related to the ongoing opioid crisis, which continues to be a point of emphasis for DOJ enforcement actions.

FY 2020 recoveries also included cases alleging electronic health records fraud, violations of the Stark Law and the Antikickback Statute, as well as cases concerning medical necessity and upcoding.

Significant Florida Settlements

Although slowed as a result of COVID-related considerations, there were several FCA settlements in the Middle District of Florida in the health care space throughout 2020. The claims underlying these settlements demonstrate the breadth of concerns and types of health care providers that may be subject to substantial FCA liability, whether through *qui tam* actions or direct government filing.

Doctor's Choice Home Health Care

In October 2020, Sarasota-based Doctor's Choice Home Health Care, Inc., agreed to pay $5.8 million to resolve two whistleblower suits claiming that they violated the FCA. The whistleblowers alleged that Doctor's Choice entered into fraudulent "medical directorship contracts" that were in fact disguised patient referral arrangements. Once Doctor's Choice captured the illegally referred patients, it increased the skilled nursing services provided to the patients in order to avoid becoming subject to the Low Utilization Payment Adjustment, which would have reduced reimbursement to Doctor's Choice.

Ophthalmic Consultants

In June 2020, a Sarasota eye health practice, Ophthalmic Consultants, P.A., and Dr. Robert K. Snyder agreed to pay $4.8 million to resolve fraud allegations that it multi-dosed medications used to treat macular degeneration and related conditions that are packaged for single use but which contain a moderate overfill buffer (Lucentis and Eylea). The multi-dosing practice resulted in excess billing of Medicare, TRICARE and FEHBP. The grounds for the government's claims were developed through a routine audit of the medical practice.

Key Takeaways

Despite the total amount of recoveries decreasing in 2020 as compared to previous years, the number of new matters filed and pursued by both the government and *qui tam* relators increased. Consistent with years past, the health care and life sciences industries continued to predominate new FCA matters, whether initiated by the government or *qui tam* relators. Recoveries are overwhelmingly generated from cases initiated by *qui tam* relators, who range from current and former employees to business associates to competitors. While relators are no doubt incentivized by the substantial rewards they stand to recover for their efforts in pursuing FCA actions, robust compliance efforts still remain the best first line of defense. Even so, the need to defend against these claims either already is—or may ultimately become—a reality for entities and individuals in this space, particularly as COVID-19-related enforcement actions ramp up.

With the advent of a new administration, a single political party in effective control of both Congressional houses and the White House, and the anticipated influx of fraud actions stemming from the Coronavirus Aid, Relief, and Economic Security ("CARES") Act, the number of FCA enforcement actions can only be expected to increase in 2021. For this reason, health care and life sciences entities need to be increasingly diligent, both in ensuring comprehensive and effective

compliance programs and in preparing to aggressively defend against any investigations and litigation that may arise out of government and *qui tam*-initiated fraud allegations.

Submitted by: **George Breen, Esq., Erica Sibley Bahnsen, Esq., Elizabeth Harris, Esq., Robert Hearn, Esq., & Kathleen Premo, Esq., *Epstein Becker & Green, P.C.***

FRAUD AND ABUSE UPDATES

DOJ Increases Enforcement Efforts Related to Telehealth Fraud

The U.S. Department of Justice ("DOJ") recently increased enforcement efforts related to telehealth-related fraud schemes. For example, on January 8, 2021, Ivan Andre Scott was convicted in the Middle District of Florida of health care fraud, receipt of kickbacks and other charges related to running a telemedicine scheme in 2018 and 2019.[7] The evidence at trial established that Mr. Scott was a patient recruiter and operated a telemarketing company, Scott Global, which targeted Medicare beneficiaries. The company represented that Medicare covered a costly cancer screening test, CGx, and through bribes and kickbacks, obtained telemedicine doctors' orders authorizing the testing. The government established that the doctors were not treating the patients for cancer and often did not speak with the patients. Mr. Scott then sold the orders to laboratories in exchange for kickbacks.

The timing of this trial is notable because certain federal and state regulations related to telemedicine were relaxed as a result of the COVID-19 pandemic. For example, on December 1 and December 28, 2020, the Centers for Medicare & Medicaid Services ("CMS") issued a final and interim final rule regarding the Medicare Physician Fee Schedule for Calendar Year 2021, which added more services to the list of covered telehealth services, such as group psychotherapy, low intensity home visits, and psychological and neuropsychological testing.[8] CMS clarified that licensed clinical social workers, clinical psychologists, physical therapists, occupational therapists, and speech-language pathologists can furnish brief online assessments and management services as well as virtual check-ins and remote evaluation services.

The federal government has also modified its enforcement priorities to accommodate broader access to telehealth services. For example, the Office for Civil Rights at the Department of Health and Human Services ("OCR") has announced that it will exercise its enforcement discretion and "will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."[9] The notice indicates that OCR's enforcement discretion would apply when providers use Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, but would not apply to the use of Facebook Live, Twitch, TikTok and other public facing applications.

Furthermore, on March 31, 2020, the Federal Communications Commission ("FCC") adopted a $200 million telehealth program to support healthcare providers responding to the COVD-19 pandemic,[10] and on January 15, 2021, announced the first round of projects, including a pilot in Miami that will provide remote monitoring, video visits and consults and other services to low income and veteran patients suffering from chronic conditions, high-risk pregnancy, infectious disease, including COVID-19, mental health conditions, and opioid dependency.[11]

Despite this relaxed regulatory climate and promotion of telehealth, the DOJ vigorously pursued the *Scott* case involving telemedicine during the pandemic, as well as a number of other telehealth-related fraud schemes, and has indicated that it has made telehealth-related fraud a top enforcement priority.

Submitted by: **Daria Pustilnik, Esq., *Kobre & Kim, LLP***

FRAUD AND ABUSE UPDATES

Sham Websites Offer COVID-19 Vaccine

Pandemic-related cyber schemes are emerging. In one such scheme, sham websites purport to offer COVID-19 vaccines to people desperate for a vaccine; and, instead of providing the vaccine, collect personal identifying information and money.

Recently, Homeland Security investigators announced that by mid-February 2021, the department had "seized roughly $33 million in illicit proceeds and analyzed almost 80,000 COVID-19 domain names."[12] In one such seizure, three Baltimore-area men were arrested and charged with conspiracy to commit wire fraud for operating a sham Moderna, Inc., website, which announced that individuals may "be able to buy a COVID-19 vaccine ahead of time."[13] The site offered "doses" for $30.00 each.[14]

In Maryland, the U.S. Attorney's Office shut down two fraudulent websites that imitated drug companies and sought to collect personal information for phishing attacks. One of the websites, regeneronmedicals.com, claimed it was linked to Regeneron Pharmaceuticals, Inc., the biotechnology company that provided the treatment used on former President Trump last year.[15] Another site, Modernatx.shop, used a web tool to copy Moderna's actual website.

These scams are not limited to the United States. Interpol has warned that phishing schemes and fake websites are mimicking government and health authorities in Europe.[16]

While people are desperate to get back to a normal life, it is essential to use caution when providing identifying information and payment via the internet. Customers should be advised that legitimate vaccines are not available for sale online.

Submitted by: **Amy Morse, Esq., *Morse & Morse, LLC***

LEGISLATIVE UPDATES

The Sun is Rising on COVID Liability Protection for Florida Healthcare Providers

The Florida Legislature is considering bills to protect businesses, including healthcare providers, from frivolous lawsuits filed because of exposure to COVID-19. While only a Senate-version of legislation for healthcare providers has been filed, the chair of the House Health & Human Services committee, Representative Colleen Burton (R-Lakeland), has unveiled a committee bill (PCB HHS 21-1) that has garnered early support from House Speaker Chris Sprowls (R-Palm Harbor).

In the meantime, Senate measure SB 74, recently filed by Senator Jeff Brandes (R-St. Petersburg), was heard in early February in its first committee of reference, the Senate Judiciary, which is chaired by Senator Brandes. As filed, SB 74 provides immunity from civil liability for healthcare providers (including, but not limited to, hospitals, nursing homes, assisted living facilities, home health providers, and doctors) if supplies or personnel were not available to comply with government health standards or guidance related to the COVID-19 pandemic.

Unlike the current draft of similar legislation (HB 7 and SB 72) intended to provide protection from COVID-19-related litigation for non-provider businesses, the current version of this legislation does not require a physician's affidavit in order to file suit. However, this legislation does include significant protections for providers, including the following:

- The initial complaint must be pled with particularity.
- The claimant must prove the provider's gross negligence or intentional misconduct when complying with government health standards or guidance, interpreting or applying the standards or guidance, or in the provision of a novel or experimental treatment.
- The claim must be commenced within one year of the:
    - Death of the injured individual due to COVID-19;
    - Hospitalization due to COVID-19;
    - First diagnosis of COVID-19; or
    - The effective date of the legislation.

There have been four amendments to SB 74 filed for consideration that address concerns about immunity, standard of proof, gross negligence, the commencement timeline, and providers previously cited by the state or federal governments for control deficiencies and infection prevention but all of them failed.

Further, the scope of coverage and parties entitled to such coverage may continue to evolve. It is also not clear at this time what actions would potentially constitute "gross negligence" as provided in the legislation. Also, the legislation identifies various professions as "health care providers,"

including some professions, such as athletic trainers, that are not traditionally considered health care providers.

There are many stages to go before this legislation, or any similar legislation, is passed and becomes law, if at all. It is likely that there will be many revisions to it, and interest groups will continue to file amendments to protect their specific concerns. This legislation would become effective upon the Governor's signature, and most of its provisions would apply retroactively. The primary exception to this retroactivity is for civil actions against specifically named health care providers that are filed before the effective date of the legislation. Should this legislation become law, businesses concerned about COVID-related-liability should review with counsel the applicability of these protections.

Submitted by: **Ashlee Tising, Esq., Bruce Platt, Esq., & Steve Grigas, Esq.,**
Akerman LLP

PRIVACY UPDATES

Potential Liability for Healthcare Systems and Providers Attacked by Ransomware

It is imperative for healthcare systems and providers to plan and prepare for the potential legal consequences of, and fallout from, a ransomware attack on their systems. A ransomware attack is characterized by a malicious actor gaining access to the victim's computer network and encrypting the data stored within to lock out the owners and hold it hostage until the owner pays a ransom.

Ransomware attacks are becoming a common occurrence in today's digitized world. This is particularly true during the COVID-19 global pandemic, when countless people are working remotely from unsecure networks at home.

Healthcare providers and systems are particularly vulnerable to, and increasingly being targeted by, ransomware attacks because of the organizations' size and their near-constant need to retrieve electronically stored patient information quickly. In fact, such attacks have become such a pervasive problem that on October 28, 2020, the Cybersecurity and Infrastructure Security Agency ("CISA"), the Federal Bureau of Investigation ("FBI"), and the U.S. Department of Health and Human Services ("HHS") issued a Joint Cybersecurity Advisory warning of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[17]

This is not a hypothetical or anticipated threat—ransomware attacks have been affecting healthcare systems worldwide and interfering with patient care throughout, and before, 2020. For instance, a ransomware attack in September 2020 reportedly disabled all IT systems at Universal Health Services, "which operates 400 hospitals and behavioral health facilities in the U.S. and the U.K."[18] Another suspected ransomware attack in September 2020 caused "failure of IT systems at a major hospital" at the Duesseldorf University Clinic. That attack resulted in transportation of a critically ill patient being diverted to another hospital approximately 20 miles away, where she later expired. [19]

More recent ransomware attacks affecting healthcare systems and other institutions have been conducted by foreign actors. In an attack on six separate hospitals from California to New York, the attackers were apparently foreign actors, as they were reported to be "Russian-speaking."[20] These ordeals can last months, as recently shown by the attacks on the University of Vermont Medical Center and the Greater Baltimore Medical Center.[21] Further, these attacks are not limited within the healthcare field to healthcare systems—a company providing software used in clinical trials and an online provider of healthcare services was recently targeted by attacks that resulted in disclosure of protected health information ("PHI").[22]

The effects of an attack could trigger liability under several federal laws, as briefly discussed below, in addition to the obvious potential tort liability to patients. For instance, these attacks can trigger obligations under the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA regulations require healthcare systems to have in place security policies and procedures to address response to and recovery from a ransomware attack. [23] In addition, a breach

of PHI resulting from a ransomware attack could be considered a "security incident" under HIPAA rules, which requires compliance with certain breach notification requirements.[24]
Moreover, a hospital experiencing a ransomware attack could face both administrative enforcement of the Emergency Medical Treatment and Labor Act ("EMTALA") and private actions if it is forced to turn away a person seeking care due to interruptions in its emergency services.[25] Any receiving facility that suspects it has received an improperly transferred patient must, within 72 hours, report the incident to the Centers for Medicare and Medicaid Services ("CMS") or the relevant state surveying agency or risk losing its certification.[26]

Even an attempt to quickly pay the ransom and restore access to patient files could trigger federal anti-money-laundering regulations. Some providers that are targeted by ransomware attacks hope to quickly move forward by simply paying the ransom.[27] However, the Department of the Treasury's Office of Foreign Assets Control ("OFAC") recently issued guidance "to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities."[28] OFAC warns that "facilitat[ing] ransomware payments to cyber actors on behalf of victims . . . not only encourage[s] future ransomware payment demands but also may risk violating OFAC regulations" because such payment "may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims."[29] The advisory explains that "U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities . . . on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)."[30] Severe civil penalties for sanctions violations can be imposed based on strict liability.[31] To avoid such sanctions, affected organizations should involve the OFAC, the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection, and the Financial Crimes Enforcement Network in development of an appropriate and legal response.

Ultimately, the most effective way to address a ransomware cyberattack is by having in place robust security measures to prevent attacks and policies to mitigate harm if an attack occurs. Healthcare systems and other providers should consult with cybersecurity experts to implement cybersecurity plans that clearly explain preventative steps, as well as corrective and reporting actions to take if the institution suffers a ransomware attack. The above-referenced Joint Cybersecurity Advisory published by CISA, FBI, and HHS includes a detailed section on plans, policies, and best practices that should be implemented to protect against such an attack and mitigate any damage resulting therefrom.[32] Examples of such policies could include regularly backing up data, employing air gaps, and password protected, encrypted offline backups.[33]

Such plans should ensure alternative access to patient health records in the event of an attack as well as a streamlined process for notifying patients of any disclosure of their PHI. Early and proactive implementation of these best practices can aid targeted healthcare systems in preventing and addressing a security breach, and can allow for quick recovery of backed-up information as well as mitigation of any harm caused. They can also serve to demonstrate that a targeted organization has taken all reasonable steps within its power to protect its patients.

Healthcare systems or organizations may report ransomware attacks to their local FBI field office at www.fbi.gov/contact-us/field or the FBI's 24/7 Cyber Watch (CyWatch), by telephone at (855)

292-3937, or by e-mail at CyWatch@fbi.gov, and should provide as much information as possible in the report including: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, healthcare systems or organizations may also contact CISA at central@cisa.gov.

Submitted by: **Ian E. Waldick, Esq., *Oertel, Fernandez, Bryant & Atkinson***

REGULATORY UPDATES

In Vitro Clinical Tests (IVCTs), In Vitro Diagnostics (IVDs) and Laboratory Developed Tests (LDTs)

HHS Announcement Regarding Laboratory Developed Tests (LDTs)

On August 19, 2020, the U.S. Department of Health and Human Services ("HHS") issued a formal announcement regarding the regulation of Laboratory Developed Tests ("LDTs").[34] In a post titled "*Recission of Guidances and Other Informal Issuances Concerning Premarket Review of Laboratory Developed Tests*" (the "HHS Announcement"), HHS announced that the FDA "will not require premarket review of LDTs absent notice-and-comment rulemaking, as opposed to through guidance documents, compliance manuals, website statements, or other informal issuances."[35] This new mandate of "notice and comment" rulemaking was both significant and controversial in light of the FDA's longstanding preference of utilizing the less burdensome mechanism of issuing guidance documents to regulate LDTs under the FDA's purported jurisdiction separate and apart from the Clinical Laboratory Improvement Amendments ("CLIA"), the division of the Centers for Medicare and Medicaid Services ("CMS") that regulates clinical laboratory testing.[36]

In the days following the HHS Announcement, the FDA did not formally respond to any questions during town hall meetings, but instead directed all questions regarding the HHS Announcement to HHS.[37]

Now that President Joe Biden has taken office, transition of senior officials at the FDA and HHS is imminent, and with the Health and Finance Committees of the Senate expected to convene to approve confirmations in late February,[38] it appears likely that the HHS Announcement may be repealed or otherwise amended.[39]

VALID Act and VITAL Act

While many expect that the new presidential administration will usher a period where HHS will recede from recent attempts to restrain or limit the FDA's ability to regulate LDTs, it is unclear whether the Biden administration will formally support any of the pending legislation aimed at clarifying and establishing a comprehensive regulatory framework for IVCTs and LDTs.[40] In March 2020, two competing bills—the VALID Act and the VITAL Act—were introduced into Congress as proposed frameworks for resolving regulatory and jurisdictional ambiguity historically surrounding LDTs.

VALID Act

On March 5, 2020, bipartisan lawmakers from the U.S. House of Representative and Senate simultaneously introduced the *Verifying Accurate Leading-edge IVCT Development Act of 2020* (the "VALID Act").[41] The VALID Act is comprehensive bill that seeks to define and set out a

robust regulatory framework for in vitro clinical tests ("IVCTs"), including LDTs and in vitro diagnostics (IVDs).[42] "At its core, the VALID Act would explicitly grant the FDA authority to regulate LDTs through a risk-based framework that categorizes LDTs as high risk or low risk, with high-risk tests facing approval requirements that are comparable to existing medical device regulations."[43]

For a more detailed overview of the VALID Act, please see the HLS Updates from June 2020.[44]

VITAL Act

On March 17, 2020, another bipartisan coalition introduced the *Verified Innovative Testing in American Laboratories Act* ("VITAL Act"), which offers a competing framework to the VALID Act for the comprehensive oversight and regulation of IVCTs and LDTs.[45] Unlike the VALID Act, which would confirm the FDA's jurisdiction and regulatory authority over the laboratory testing industry and impose a risk-based classification system on the review of IVCTs and LDTs, the VITAL Act would explicitly exclude the FDA from the regulatory oversight of LDTs and confirm that CLIA is the sole body with federal jurisdiction and regulatory authority over LDTs.[46] The American Association of Clinical Chemistry ("AACC") and other laboratory industry groups have offered their support of the VITAL Act, consistent with the decades-long contention that IVCTs and LDTs are already regulated under the oversight of CLIA, and thus do not require an additional layer of superfluous oversight from the FDA.[47]

It was anticipated that congressional committees with oversight over the FDA would commence stakeholder discussions and hold hearings on the VALID Act and the VITAL Act in the Summer of 2020.[48] With transitions in the executive and legislative branches of government underway, and COVID-19 lasting well into 2021, it remains unclear when congressional committee meetings and public meetings to solicit recommendations on the VALID Act and VITAL Act will commence.

Submitted by: **Gray W. Rifkin, Esq., EMBA**
Chief Legal Officer and Chief Operating Officer, Commonwealth Diagnostics International, Inc.
Board of Directors, My Total Health, Inc.
Board of Directors, Alpha Logic, Inc.

[1] *EEOC v. Mission Hosp., Inc.*, Case No. 1:16-cv-00118-MOC-DLH, 2017 WL 3392783 (W.D. N.C. Aug. 7, 2017); *see Robinson v. Children's Hosp. Boston*, Case No. 14-10263-DJC, 2016 WL 1337255 (D. Mass. Apr. 5, 2016).
[2] 21 U.S.C. § 360bbb-3.
[3] *Id.* § 360bbb-3(e).
[4] 10 U.S.C. § 1107(a).
[5] 29 U.S.C. § 654.
[6] *See generally*, https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020.
[7] *U.S. v. Scott*, Case No. 6:19-cr-00209 (M.D. Fla.).
[8] Final Policy, Payment, and Quality Provisions Changes to the Medicare Physician Fee Schedule for Calendar Year 2021, *available at* https://www.cms.gov/newsroom/fact-sheets/final-policy-payment-and-quality-provisions-changes-medicare-physician-fee-schedule-calendar-year-1; Medicare Program; CY 2021 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment Policies; Medicare Shared Savings Program Requirements; Medicaid Promoting Interoperability Program Requirements for Eligible Professionals; Quality Payment Program; Coverage of Opioid Use Disorder Services Furnished by Opioid Treatment Programs; Medicare Enrollment of Opioid Treatment Programs; Electronic Prescribing for Controlled Substances for a Covered Part D Drug; Payment for Office/Outpatient Evaluation and Management Services; Hospital IQR Program; Establish New Code Categories; Medicare Diabetes Prevention Program (MDPP) Expanded Model Emergency Policy; Coding and Payment for Virtual Check-in Services Interim Final Rule Policy; Coding and Payment for Personal Protective Equipment (PPE) Interim Final Rule Policy; Regulatory Revisions in Response to the Public Health Emergency (PHE) for COVID-19; and Finalization of Certain Provisions from the March 31st, May 8th and September 2nd Interim Final Rules in Response to the PHE for COVID-19, Centers for Medicare & Medicaid Services (CMS), Health and Human Services (HHS), 85 FR 84472 (Dec. 28, 2020), *available at* https://www.federalregister.gov/documents/2020/12/28/2020-26815/medicare-program-cy-2021-payment-policies-under-the-physician-fee-schedule-and-other-changes-to-part.
[9] HHS.gov, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*, *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.
[10] FCC.gov, *FCC Approves Emergency COVID-19 Telehealth and Connected Care Pilot Programs*, *available at* https://www.fcc.gov/fcc-approves-emergency-covid-19-telehealth-and-connected-care-pilot-programs.
[11] FCC.gov, FCC Announces Initial Projects Selected for Connected Care Pilot Program, *available at* https://docs.fcc.gov/public/attachments/DOC-369274A1.pdf (accessed Feb. 25, 2021).
[12] Brooke Henderson, *Covid-19 Vaccine Scams Grow, Leveraging Confusion About How to Get the Shot*, THE WALL STREET JOURNAL, Feb. 23, 2021, *available at,* https://www.wsj.com/articles/covid-19-vaccine-scams-grow-leveraging-confusion-about-how-to-get-the-shot-11614076200.
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Id*.
[17] Joint Cybersecurity Advisory: Ransomware Activity Targeting the Healthcare and Public Health Sector, CISA, FBI & HHS (Oct. 28, 2020), https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.
[18] Kevin Collier, *Major hospital system hit with cyberattack, potentially largest in U.S. history*, NBC NEWS (Sept. 28, 2020), https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254.
[19] *German hospital hacked, patient taken to another city dies*, ASSOCIATED PRESS (Sept., 17, 2020), https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.
[20] Ellen Nakashima & Jay Greene, *Hospitals being hit in coordinated ransomware attack*, WASHINGTON POST (Oct. 29, 2020), https://www.washingtonpost.com/national-security/hospitals-being-hit-in-coordinated-targeted-ransomware-attack-from-russian-speaking-criminals/2020/10/28/e6e48c38-196e-11eb-befb-8864259bd2d8_story.html; Bill Swindell, *Sonoma Valley Hospital hit by cybercriminals with ransomware attack*, THE PRESS DEMOCRAT (Oct. 30, 2020), https://www.pressdemocrat.com/article/news/sonoma-valley-hospital-hit-by-cybercriminals-with-ransomware-attack/.

[21] Paul Gessler, *GBMC Nurse: Hospital 'Crippled' by Ransomware Cyberattack*, WJZ CBS BALTIMORE (Dec.18, 2020), https://baltimore.cbslocal.com/2020/12/18/gbmc-ransomware-cyberattack-nurse-speaks-latest/; Wilson Ring, Marion Renault, and The Associated Press, *Hospitals fighting COVID face another challenge: Hackers*, FORTUNE (Dec. 5, 2020), https://fortune.com/2020/12/05/hospitals-ransomware-covid-hackers/.
[22] Jessica Davis, *484K Aetna ACE Plan Members Impacted by EyeMed Email Hack*, HEALTH IT SECURITY (Dec. 29, 2020), https://healthitsecurity.com/news/484k-aetna-ace-plan-members-impacted-by-eyemed-email-hack; Nicole Perlroth, *Clinical Trials Hit by Ransomware Attack on Health Teach Firm*, NEW YORK TIMES (Oct. 3, 2020), https://www.nytimes.com/2020/10/03/technology/clinical-trials-ransomware-attack-drugmakers.html?auth=login-google1tap&login=google1tap.
[23] FACT SHEET: Ransomware and HIPPA, U.S. Department of Health & Human Services, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.
[24] *See* 45 C.F.R. § 164.400-414.
[25] *See* 42 U.S.C. § 1395dd(d)(2).
[26] *See* State Operations Manual, Appendix V--Interpretive Guidelines--Responsibilities of Medicare Participating Hospitals in Emergency Cases, CMS, at 5 (Rev. 191, 07-19-19), https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/downloads/som107ap_v_emerg.pdf.
[27] *See, e.g.*, Chris Brook, *Following Ransomware Attack Indiana Hospital Pays $55k to Unlock Data*, DIGITAL GUARDIAN (Aug. 12, 2020), https://digitalguardian.com/blog/following-ransomware-attack-indiana-hospital-pays-55k-unlock-data; Chris Brunau, *Hospital Pays King's Ransom After Ransomware Attack*, DATTO (Feb. 19, 2016), https://www.datto.com/blog/hospital-forced-to-pay-kings-ransom-after-cryptolocker-attack.
[28] Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Department of the Treasury, OFAC (October 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.
[29] *Id.* at 3.
[30] *Id.*
[31] *Id.*
[32] Joint Cybersecurity Advisory, *supra*, at note 29, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.
[33] Further detailed examples can be found in the Ransomware Guide published by the Multi-State Information Sharing & Analysis Center and the CISA, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.
[34] HHS.gov. *Rescission of Guidances and Other Informal Issuances Concerning Premarket Review of Laboratory Developed Tests* (Aug. 19, 2020), https://www.hhs.gov/coronavirus/testing/recission-guidances-informal-issuances-premarket-review-lab-tests/index.html.
[35] *Id.*
[36] CMS.gov, *Clinical Laboratory Improvement Amendments* (Feb. 19, 2021), https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA.
[37] Turna Ray, *Stakeholder Scramble to Predict Impact of HHS Move Limiting FDA Ability to Regulate LDTs* (Sept. 19, 2020), https://www.genomeweb.com/molecular-diagnostics/stakeholders-scramble-predict-impact-hhs-move-limiting-fda-ability-regulate#.X2Nm3mhKiUk.
[38] Jacqueline Lapointe, *Spotlight on the Biden Administration Healthcare Team* (Feb. 21, 2021), https://revcycleintelligence.com/news/spotlight-on-the-biden-administrations-healthcare-team.
[39] *See, e.g.*, Dennis C. Gucciardo, et al, Morgan Lewis Bockius LLP, *How a Biden Administration will Affect FDA's regulation of medical devices* (Feb. 21, 2021), https://www.lexology.com/library/detail.aspx?g=db13016c-d827-4b87-bb64-73811c9d2dab.
[40] *Id.*
[41] S. 3404, 116th Congress: VALID Act of 2020 (Apr. 30, 2020), https://www.govtrack.us/congress/bills/116/s3404.
[42] *Id.*
[43] Boston Healthcare Associates, *The VALID and VITAL Acts: What do they Mean for Diagnostic Innovators* (Feb. 21, 2021), https://www.bostonhealthcare.com/what-the-valid-and-vital-acts-mean-for-diagnostic-innovators/#:~:text=The%20VITAL%20Act%20is%20intended,during%20a%20public%20health%20emergency.
[44] Gray W. Rifkin, *Legislative Updates: Regulation of In Vitro Clinical Diagnostic Tests*, https://www.flabarhls.org/resources-menu/document-library/health-law-updates/349-hls-monthly-updates-2020-june/file.
[45] S. 3512, 116th Congress: Vital Act of 2020 (Feb. 21, 2021), https://www.congress.gov/bill/116th-congress/senate-bill/3512.
[46] *Id.; see also supra* note 43.

[47] Kimberly Scott, AACC.org, *HHS Decision Raises Questions About Future Oversight of All LDTs* (Nov. 1, 2020), https://www.aacc.org/cln/articles/2020/november/hhs-decision-raises-questions-about-future-oversight-of-all-ldts.
[48] *See, e.g., supra* note 44; *see also* Aaron L. Josephson, *The VALID Act, Aiming to Reform the Regulation of Diagnostic Products, is Finally Introduced in Congress*, THE NATIONAL LAW REVIEW (Apr. 30, 2020), https://www.natlawreview.com/article/valid-act-aiming-to-reform-regulation-diagnostic-products-finally-introduced.