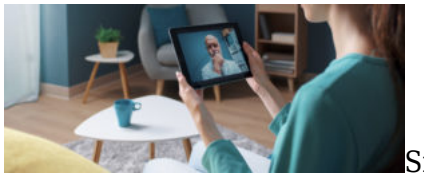
DOJ-HHS Announces False Claims Act Working Group, Emphasizes Healthcare Fraud Enforcement Priorities

 The Trump administration recently announced the renewal of a new cross-agency collaboration between the Department of Justice (DOJ) and the Department of Health and Human Services (HHS) in the form of the **DOJ-HHS False Claims Act Working Group**. The Working Group will be jointly led by Deputy Assistant Attorney General (DAAG) of the Commercial Litigation Branch Brenna Jenny, HHS Acting General Counsel Sean Keveney, and HHS Office of Inspector General Acting Chief Counsel Susan Edwards, and will include the Centers for Medicare & Medicaid Services (CMS) Center for Program Integrity and U.S. Attorneys' Offices.

Read the full alert **here.**

DEA Publishes Temporary Rule on the Extension of COVID-19 Telemedicine Flexibilities for Prescription of Controlled Substances

 Since the declaration of the public health emergency due to the COVID-19 epidemic, Drug Enforcement Administration (DEA) registered practitioners have been able to prescribe controlled substances, without a prior in-person visit with a patient, subject to certain conditions as outlined in our earlier **blog post**. Additionally, DEA waived the requirement for practitioners to obtain additional registrations with DEA in the states where the dispensing (including prescribing, and administering) occurs, for the duration of the public health emergency, if the practitioner registers with DEA in at least one state and has permission under state law to practice using controlled substances in the state where the dispensing occurs.

In anticipation of the expiration of the public health emergency on May 11, 2023, on March 1, 2023, DEA and the Department of Health and Human Services issued two notices of proposed rulemakings (NPRMs), reviewed in our earlier **blog post**, to authorize the prescription of controlled substances

based on a telehealth consultation in certain limited circumstances. The NPRMs received over 38,000 comments from the public, all of which DEA will review to implement revisions to the NPRMs and develop a permanent rule.

Since the permanent rule is still in development, on May 10, 2023, just one day before the end of the public health emergency, DEA and the Substance Abuse and Mental Health Services Administration published a **temporary rule** that extends the public health emergency telemedicine flexibilities**[1]** for the prescription of controlled substance medications until November 11, 2023.

The temporary rule, which took effect on May 11, 2023, allows DEA-registered practitioners to prescribe controlled substance medications under the public health emergency telemedicine flexibilities to all patients through November 11, 2023. Additionally, until November 11, 2024, DEA-registered practitioners are further permitted to prescribe controlled substance medications under the public health emergency telemedicine flexibilities to patients if the practitioner established a telemedicine relationship with the patient on or before November 11, 2023. In other words, if a provider and patient established a telemedicine relationship on or before November 11, 2023, the same public health emergency telemedicine flexibilities that previously governed the relationship will apply until November 11, 2024.

In the text of the rule, DEA notes that it plans to issue one or more final rules, based on the two proposed rules, which will extend certain telemedicine flexibilities on a permanent basis and ensure a smooth transition for patients and practitioners that rely on the availability of telemedicine for controlled substance medications.

*Follow our **blog** to receive additional updates and alerts on the DEA's proposed rules regarding extension of the COVID-19 telemedicine flexibilities for the prescription of controlled substance medications.*

---

[1] In the temporary rule, the DEA references the **DEA letter** that authorized certain telemedicine flexibilities, including the waiver exceptions related to DEA registrations in individuals states and the in-person evaluation requirement.

DEA Announces Temporary Extension of COVID-19 Telehealth Flexibilities for Prescription of Controlled Medications

The Controlled Substances Act, as amended by the Ryan Haight Act, generally prohibits prescribing controlled substances via telehealth without a prior in-person examination, subject to certain very limited exceptions. Those exceptions include

prescriptions issued during a public health emergency. Thus, since the January 31, 2020 declaration of a public health emergency due to the COVID-19 epidemic, eligible providers have been able to prescribe controlled substances, without a prior in-person visit with a patient, provided:

- The prescription is issued for a legitimate medical purpose by a practitioner acting in the usual course of his/her professional practice;
- The telemedicine communication is conducted using an audio-visual, real-time, two-way interactive communication system; and
- The practitioner is acting in accordance with applicable Federal and State laws.

The public health emergency is scheduled to end on May 11, 2023.

Read the client alert **here**.

President Biden Signs Into Law Medicare Telehealth Coverage Extension Post-Public Health Emergency

On March 15, 2022, President Biden signed into law the $1.5 trillion Consolidated Appropriations Act of 2022 (the "Omnibus Bill"). Included in the 2,700+ page Omnibus Bill is an extension of Medicare coverage of professional consultations, office visits, and office psychiatry services conducted via telemedicine for 151 days after the end of the designated public health emergency ("PHE").**[1]**

Prior to the PHE, in order to qualify for Medicare coverage:

- A patient receiving telehealth services had to be physically located at a physician's office, hospital, or other healthcare facility that is located in a geographical health professional shortage area (HPSA) that met certain requirements, a county that was not included in a Metropolitan Statistical Area as of December 31st of the preceding year, or an entity participating in a Federal telemedicine demonstration project in order for telehealth services to be covered by Medicare.
- Further, the patient had to obtain telehealth services furnished through technology that enabled real-time audio visual communication, with limited recent exceptions, as discussed in our Client Alert titled ***CMS Continues to Modernize by Expanding Reimbursement for Digital Health Services***.

Administrative and legislative changes made in March 2020 as part of the government's response to the COVID-19 pandemic waived these location and technology requirements for the duration of the

PHE. These waivers of location and technology requirements are now extended further under the Omnibus Bill.

Additionally, the Omnibus Bill expands the types of practitioners eligible to provide telehealth services to patients. Prior to the PHE, Medicare covered telehealth services only if offered by physicians, physician assistants, nurse practitioners, clinical nurse specialists, nurse-midwives, clinical psychologists, clinical social workers, registered dieticians or certified registered nurse anesthetists. Under the Omnibus Bill, qualifying practitioners now include occupational therapists, physical therapists, speech-language pathologists and audiologists. Other changes include delaying in-person requirements for the provision of mental health services and extending coverage of telehealth services rendered by federally qualified health centers to provide telehealth services for the same 151 day post-PHE period.

While these changes are welcomed by many in the healthcare industry as a necessary resource and buffer for telehealth patients and providers, it remains to be seen whether additional coverage flexibilities, beyond certain limited opioid treatment program expansion and counseling therapy telehealth coverage expansion under **CY 2022 Medicare Physician Fee Schedule Final Rule**, established during the PHE will become permanent moving forward. The Omnibus Bill requires the Medicare Payment Advisory Commission to provide Congress with a report by June 15, 2023 on the expansion of telehealth services as a result of the PHE. The Department of Health and Human Services, Office of Inspector General is similarly required to provider Congress with a report by June 15, 2023 on program integrity risks associates with Medicare telehealth services. In addition, the Department of Health and Human Services must post quarterly data, starting July 1, 2022, on Medicare claims for telemedicine services.

We will continue to monitor these and other legislative and regulatory changes impacting telehealth industry stakeholders.

---

[1] The PHE determination was recently renewed by Xavier Becerra, Secretary of the U.S. Department of Health and Human Services on January 16, 2022. A public health emergency declaration expires 90 days after the declaration or renewal or renewal is made, unless terminated prior. It is unclear whether the latest PHE declaration will be renewed or not or whether the PHE declaration will be terminated prior to the 90-day deadline.

Changes to Stark Law Special Compensation Rules for Group Practices Go into Effect on January 1, 2022

The final rules regarding special compensation under **42 U.S.C. § 1395nn**, the Physician Self-Referral or Stark Law, go into effect on January 1, 2022 and will require many physician group practices to modify their compensation methodologies, specifically the pooling and distribution of profits for the provision **designated health services** ("DHS").

Under the **current regulations**, a physician in a group practice that relies on the in-office ancillary services exception can be paid a share of overall group profits, so long as that share is determined in a way that is not "directly related to the volume or value of referrals of DHS by the physician." The same is true of productivity bonuses based on services that a physician has performed. "A physician in the group practice may be paid a productivity bonus based on services that he or she has personally performed, or services 'incident to' such personally performed services, or both, provided that the bonus is not determined in any manner that is directly related to the volume or value of referrals of DHS by the physician (except that the bonus may directly relate to the volume or value of DHS referrals by the physician if the referrals are for services 'incident to' the physician's personally performed services)."

This provision had previously been interpreted to allow "split pool" profit-sharing plans that create pools of DHS-derived profits for different services, in which only certain physicians benefit from certain profit pools.

Effective January 1, 2022, split pooling is no longer permitted. In the **final regulation**, which modifies the special compensation rules under 42 C.F.R. §411.352(i), CMS clarifies that "if a group practice wishes to pay shares of overall profits to any of its physicians, it must first aggregate: (1) The entire profits from the entire group; or (2) the entire profits from any component of the group that consists of at least five physicians. Once aggregated, the group practice may choose to retain some of the profits or distribute all of the profits through shares of overall profits paid to its physicians." Therefore, although a group practice may employ different profit distribution methods for the provision of DHS for each component of the group practice that consists of five or more physicians, the group practice must employ the same method for distributing overall profits to every physician within such a component. It is important to note that although CMS limited the general definition of DHS to "only DHS payable in whole or in part by Medicare" in § 411.351, "overall profits" for the purpose of the special compensation rules for group practices continues to include "the group's entire profits derived from DHS payable to Medicare or Medicaid."

Group practices that currently employ the split pool compensation structure for physicians and rely on the in-office ancillary services exception will need to modify their compensation structures to comply with this clarification.

DOJ Announces New Initiative to Use False Claims Act to Enforce Compliance with Data Privacy and Security Laws and Contract Requirements

The Department of Justice recently announced the launch of its new Civil Cyber-Fraud Initiative (the "Initiative") which intends to use the False Claims Act to pursue "cybersecurity-related fraud by government contractors and grant recipients."

Specifically, the Initiative will target those who:

1. knowingly provide deficient cybersecurity products or services,
2. knowingly misrepresenting their cybersecurity practices or protocols, or
3. knowingly violate obligations to monitor and report cybersecurity incidents and breaches.

This new initiative significantly expands the potential liability of federal contractors and healthcare provider that participate in federal healthcare programs related to data privacy and cybersecurity issues.

False Claims Act

The False Claims Act broadly prohibits anyone from, among other things, knowingly presenting, or "causing to be presented" a false claim for payment if the claim will be paid directly or indirectly by the federal government. The False Claims Act is the government's main enforcement tool for fighting healthcare fraud, with over $2.2 billion recovered in 2020. Penalties for False Claims Act violations include three times the actual damages sustained by the government, mandatory civil penalties of between $11,181 and $22,363 for each separate false claim, and attorneys' fees and costs. Further, the False Claims Act allows whistleblowers to bring lawsuits on behalf of the federal government. Also known as a "qui tam" realtor, a whistleblower who brings a successful *qui tam* action can receive 15 to 30 percent of the damages the government recovers from the defendants. The ability for an individual within one's own organization to raise flags with the federal government under the False Claims Act especially heightens risk.

HIPAA

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), "covered entities" and their "business associates" are subject to certain obligations and limitation related to their use and disclosure of "protected health information" ("PHI"). Covered entities are health care providers, health plans and health care clearing houses that transmit any information in an electronic form in connection with a transaction for which HHS has adopted standards. A business associate is a person or entity that performs certain services for or functions on behalf of the covered entity that involve the use or disclosure of PHI. Finally, PHI is any individually identifiable

information, including demographic data, that relates to an individual's past, present or future health or payment for the provision of healthcare.

The obligations imposed on covered entities and business associates under HIPAA include maintaining and following specific privacy and security policies and procedures regarding access to, use, processing, transfer, storage, and disclosure of PHI and implementing physical, technical, and administrative safeguards to protect the privacy and security of PHI. In addition, covered entities are required to notify affected individuals, the Department of Health and Human Services, and, for certain larger breaches, the media of data breaches. Similarly, business associates are required to notify covered entities of data breaches.

Implications

The goal of holding accountable those who "knowingly provide deficient cybersecurity products or services, knowingly misrepresent their cybersecurity practices or protocols, or knowingly violate obligations to monitor and report cybersecurity incidents and breaches" presents particular risk for covered entities and their business associates.

For example, consider a revenue cycle management ("RCM") company that submits claims on behalf of a healthcare provider (including claims to government payors) that experiences a security incident, conducts a HIPAA risk assessment, and shares that assessment with the Covered Entity customer who determines the RCM company did not implement the necessary physical, technical and administrative safeguards required under HIPAA. Could the customer, the government, or a whistleblower allege that the RCM company knowingly misrepresented its cybersecurity practices or protocols and thereby caused the submission of false claims?

Further, consider an electronic health records company ("EHR") that is certified by the Office of the National Coordinator who experiences a breach of unsecured PHI, conducts a HIPAA risk assessment and determines it is not obligated to report the breach based on a low risk of compromise in accordance with 45 C.F.R. 164.402. Could the government or a whistleblower allege that the EHR company failed to report a breach and thus caused the submission of false claims by healthcare providers that use its EHR and are able to avoid reductions in Medicare reimbursement by using a certified EHR?

False Claims Act cases are commonly pursued under what is known as the "false certification theory". A claim is considered false when a claimant "certifies compliance with a statute or regulation as a condition to governmental payment." The false certification theory considers a claimant's *request* for payment as "implied certification" of compliance with said statutes or regulations. Despite the broad implications of the false certification theory, there is some check on the ability of the government or a whistleblower to bring cases on failure to comply with HIPAA through what is known as the materiality requirement under the False Claims Act. In *Universal Health Services v. United States ex rel. Escobar*, the U.S. Supreme Court held that the government and whistleblowers bear the burden of proving the "rigorous and demanding" materiality requirement under the False Claims Act. The Supreme Court further stated that the False Claims Act is "is not a means of imposing treble damages and other penalties for *insignificant* regulatory or contractual violations." Accordingly, the government and whistleblowers must demonstrate that allegedly insufficient technical safeguards or that an alleged failure to report a breach are actually *material* to the government's payment decision.

The potential use of the False Claims Act to enforce HIPAA compliance may also change how due diligence is conducted on covered entities who bill government payors and their and business associates. While security incidents are common, the potential for liability under the False Claims

Act related to such an incident increases the importance of conducting thorough diligence related to such incidents. The importance of conducting due diligence on a seller's compliance with HIPAA's requirements related to administrative, technical, and physical safeguards is also magnified by the potential for liability under the False Claims Act for failure to comply with those requirements. The risk related to conducting a risk assessment related to a data breach is similarly increased and such assessments should be scrutinized carefully in due diligence.

OIG Advocates for Increased Oversight of Medicaid Telehealth Services in Behavioral Health

Telehealth's exponential growth –in part due to the COVID-19 pandemic – has highlighted both its value in increasing access to care and the potential for misuse. The U.S. Department of Health and Human Services' Office of Inspector General (OIG) released a **report** in September 2021 that found many state Medicaid programs do not sufficiently evaluate whether telehealth improves access to care, reduces costs, or boosts the quality of care for Medicaid recipients receiving behavioral health services. Further, the OIG found that many state Medicaid programs do not provide the appropriate oversight necessary to reduce fraud, waste, and abuse. In fact, only two (2) states have measured the efficacy of telehealth on access to behavioral health services for Medicaid beneficiaries. In short, the OIG concludes that more steps should be taken to maintain oversight over telehealth, especially in the behavioral health context.

Background

When it comes to behavioral health services such as mental health assessments and therapy, generally, depending on insurance coverage limitations, telehealth can be used and could be covered. The OIG report addresses this concept and states: "As the nation confronts the psychological and emotional impact of COVID-19, the use of telehealth will be important in addressing behavioral health needs for Medicaid enrollees." However, providers must first understand where the value lies, how best to deliver these services, and how to avoid fraud and abuse; and that begins with monitoring and evaluating telehealth services in the Medicaid program.

OIG Findings

The OIG report found the following:

- A few states (3 of 37) could not identify which telehealth services are even offered to Medicaid beneficiaries. Not being able to identify services provided to Medicaid beneficiaries limits the state's ability to analyze the effects of telehealth for Medicaid enrollees, monitor and provide oversight specific to telehealth, or detect and prevent fraud.

- Only a few states assessed the impact of telehealth usage on behavioral health services for Medicaid beneficiaries, despite states' responsibilities to ensure access to care and address quality of care. An **accompanying** report showed that states described the challenges and limitations of using telehealth to meet the behavioral needs of Medicaid enrollees. As the reimbursement landscape continues to change and there is an increased shift towards telehealth service offerings to Medicaid beneficiaries, the OIG stated that it is critical for all states to evaluate the impact of telehealth.

- Despite concerns of states about telehealth abuse (e.g., inappropriate billing for delivering both telehealth and in-person services, billing for services not rendered, and billing for services provided from outside the country) and states' joint responsibility to monitor their Medicaid programs, the OIG report concluded that many states (26 of 37) do not perform adequate monitoring or oversight on telehealth services to detect any fraud, waste, and abuse meaningfully. Because of the virtual nature of telehealth services and the complex regulatory environment, states cannot monitor telehealth services to the same degree as in-person services. The report also found that several states' program integrity efforts are insufficient to monitor telehealth.

OIG Recommendations

Because the Centers for Medicare & Medicaid Services (CMS) plays an equally important role in evaluating and overseeing state Medicaid programs, the OIG recommends that CMS work with the three states that are unable to distinguish telehealth from in-person services to ensure implementation of indicators to identify which services are provided via telehealth. The OIG suggests that CMS conduct evaluations, and support state efforts to evaluate the effects of telehealth on access, cost, and quality of behavioral health services and conduct monitoring for fraud, waste, and abuse. Furthermore, the OIG encourages CMS to specifically support state efforts to oversee and monitor telehealth for behavioral health services.

Notably, CMS agreed with at least one of OIG's recommendations; namely, CMS indicated that "it is currently monitoring the impact of the COVID-19 pandemic on behavioral health services delivered via telehealth by managed care organizations and has provided States with a Risk Assessment Template to assist State efforts in identifying and addressing program risks." Further, CMS stated that "it will consider the results from OIG's study to develop ways to support State efforts to oversee behavioral health services delivered via telehealth by managed care organizations." Whether these efforts from CMS will be sufficient to help the states at issue remains to be seen.

Takeaways

Telehealth providers should be mindful that states may begin to undertake more robust and comprehensive measures to assess and ultimately restrict access to Medicaid funds for telehealth services. Based on the OIG's report, we anticipate that, because states are charged with determining how their Medicaid programs cover the use of telehealth, the OIG's report may trigger more active and meaningful monitoring and oversight of the use of telehealth with Medicaid beneficiaries. States may also start to more thoroughly evaluate the impact of telehealth on access, quality, and cost. And, we anticipate that state Medicaid programs will likely undertake more significant analysis as they determine which services will continue to be covered in a post-COVID-19 pandemic world.

Accordingly, providers should heed CMS's anticipated increased monitoring of behavioral health services delivered via telehealth. Providers receiving state-based healthcare reimbursement, for

example, should undertake a risk assessment and remedial steps to ensure that telehealth services provided to Medicaid beneficiaries are in compliance with that state's telehealth laws. This includes reviewing credentialing policies to ensure that each healthcare professional is licensed in the state in which the patient is receiving services and that the company is tracking compliance. Further, as a general practice, telehealth providers should verify that the correct Current Procedural Terminology medical codes are utilized when providing behavioral health telehealth services to Medicaid enrollees. Lastly, telehealth providers should confirm that they are properly tracking the effects of their telehealth program on Medicaid beneficiaries to better understand the impact telehealth has on access, cost, and quality.

Pharmaceutical Manufacturers Beware: New State Drug Transparency Laws and Enforcement Mechanisms Are Coming In 2022

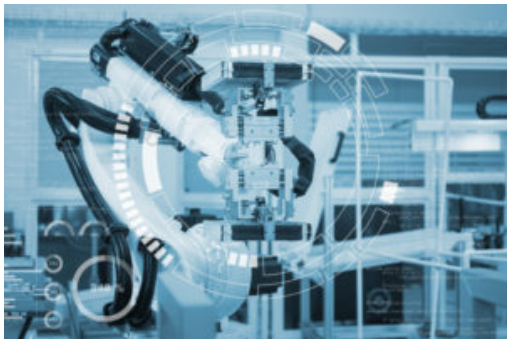
In 2016, states began passing pharmaceutical price reporting laws. These laws are designed to bring transparency to a pharmaceutical manufacturer's drug pricing process by requiring drug manufacturers to report pricing and other information related to the cost, development, and sale of drugs. By October 2021, approximately twenty states have passed or are implementing transparency laws. While many of these laws are applicable to drug manufacturers, pharmacy benefit managers, and health carriers, recent enforcement of these laws has focused only on drug manufacturers.

Each state has its own set of unique requirements that drug manufacturers must meet in order to distribute drugs within each individual state. Reporting is often completed via an online portal administered by the state's implementing agency. Some states will use this submitted data to produce public reports about the cost of prescription drugs with a goal of educating the state legislature and the public about the cost of drugs and to provide accountability for increased prices.

Enforcement of these state reporting laws is beginning to take shape as states pass legislation and implement administrative guidance – the majority of which provide for civil or administrative penalties. Enforcement authorities typically assess fines for each day a manufacturer is in violation and may increase penalties the longer the violation persists. Additionally, the appeals process for any enforcement action typically follows either a prescribed process codified by the state law or defaults to the appeals process under the state's administrative procedure act.

Accordingly, pharmaceutical manufacturers will need to be vigilant as more sates pass and implement drug transparency laws. These laws require different reporting deadlines, the reporting of different information, disclosures based on different dollar thresholds, and have different requirements and processes for protecting confidential information and trade secrets. For the latest developments in this area, please see Goodwin's recent **client alert**. For an in-depth analysis of these laws, please see our publication, **State Drug Transparency Laws: Considerations for Pharmaceutical Manufacturers**, in Chapter 8 of the American Health Law Association's 2021 edition of *Health Law Watch*.

Five Emerging Concerns for the Health Care Industry as AI & Telehealth Converge



The use of telehealth continues to grow rapidly across the U.S. Given legislative **proposals** and the Centers for Medicare & Medicaid Services **efforts** to expand access to telehealth, we can only anticipate that remotely engaging with healthcare providers is here to stay. In fact, the National Center for Health Statistics and the Centers for Disease Control and Prevention **reported** that between April and July 2021, 24.5% of adults in the U.S. had a virtual care appointment with a healthcare professional over video or phone. Given the continued persistence of COVID-19 and the ease and convenience for both provider and patient, telehealth services will most likely remain popular even as the option of in-person appointments regains footing.

On a parallel front, artificial intelligence (AI) is also driving considerable advancements in patient care. Advances in AI offer a powerful way to create clinical and operational efficiency in today's healthcare system. According to a **study** by MIT, 72% of healthcare professional respondents showed interest in implementing AI in healthcare delivery. In the field of radiology, as just one of many examples, AI can already be used to find patterns in CT scans, mammography, and other imaging modes that help **radiologists more accurately diagnose** cancer and a whole spectrum of other sometimes hard-to-identify diseases.

Telehealth is one of the newest services to utilize AI widely, and there is great promise in its application. Telehealth typically involves a synchronous, real-time electronic communication from person-to-person. Subject to limitations in certain states, telehealth also can be furnished through asynchronous communication, whereby a physician reviews and makes medical assessments based on information that a patient has uploaded or stored in a database. Even though it is asynchronous, this remains a person-to-person communication. Recently, however, we see more and more opportunities for AI to augment the person-to-person nature of and enhance the capabilities of telehealth. For example:

- **Clinical Evaluation** – leveraging AI to take patient histories and make collecting patient information more efficient. This could include a series of AI-developed questions during telehealth intake designed to ask the right questions in the proper sequence to better assist a physician in determining the cause of a patient's symptoms.

- **Telemonitoring** – the potential for AI and telemonitoring extends beyond just collecting patient data and turning them into reports. Implementing AI into remote patient monitoring (RPM) devices can promote preventative care and equip the RPM with the ability to predict adverse events.

- **Quality Improvement** –further integration of AI technology in telehealth services can help with quality improvement processes by enhancing clinical decision-making and disease diagnosis, ultimately optimizing patient care and significantly improving healthcare outcomes.

- **Virtual Health Assistants** – AI-enabled interfaces allow patients to have more power and control over their healthcare paths. AI applications in virtual health assistants can provide the patient with precise information about their healthcare condition and assist with better healthcare management.

With the promising future of the continued convergence of AI and telehealth and the increased use of digital and consumer technologies to deliver virtual care, there are several legal and regulatory considerations for telehealth providers. These include:

- **Protecting Patient Health Information.** One of the biggest issues related to data privacy and security with the application of AI in healthcare is the need to either use de-identified information or obtain patient authorization to use identifiable information. Absent patient authorization, it is difficult to use protected health information (PHI) for machine learning. But sometimes de-identified information is insufficient for machine learning. If the developer of the AI is using de-identified information, it must have the right to de-identify the PHI. Typically, a business associate (BA) is developing the AI. BA's must have the right to de-identify under the business associate agreement (BAA); otherwise, they can't de-identify PHI. Further, there is a separate risk that the AI can be used to re-identify de-identified information. Studies have **demonstrated** the potential to re-identify de-identified patient records by combining it with other data sources that AI collects such as facial recognition or iris scans. Because only a few states, like **California**, have banned re-identification of de-identified data, a Covered Entity may want to include provisions in a BAA with an entity developing AI to protect against that.

Another significant consideration with AI implementation in digital health is patient health information protection and verification. Healthcare providers are subject to state privacy and security regulations as well as the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations, which protect the privacy and security of health information and give individuals certain rights concerning their health information. According to a 2019 University of California Berkley **study**, due to the nature and functionality of AI, current laws and regulations appear inadequate to keep an individual's health status private. The findings demonstrate that using AI makes it possible to identify individuals by learning daily patterns collected by remote patient monitoring devices such as smartwatches and smartphones and correlating them to demographic data. If bad actors gain access to such information, they can piece together patients' identities. According to a 2020 cybersecurity **survey**, 70% of the healthcare providers that responded stated that they experienced significant security incidents between 2019 and 2020. Telehealth providers should be mindful of the potential gaps in data protections that could be created with the addition of

AI. This includes continued vigilance when it comes to HIPAA compliance and reexamining their internal risk assessments, policies, and practices considering the additional risks raised by AI.

- **Corporate Practice of Medicine Considerations.** As telehealth platforms leverage AI to help physicians deliver care to patients, there is an increasing opportunity for providers to use AI, through machine learning, for example, to diagnose and/or identify the appropriate treatment regimen for patients. Potential corporate practice of medicine (CPOM) concerns could ensue. **Generally, CPOM laws** are designed to prohibit corporations from practicing medicine: only individual practitioners can diagnose and treat patients, and CPOM prohibitions prevent corporate interference with a healthcare professional's independent professional judgment. Without the right level of physician supervision, it is conceivable that an advanced AI-enabled telehealth platform could potentially diagnose or recommend patient treatment options or otherwise blur the lines demarcating where the machine's judgment ends, and the physician's judgment begins. A company offering AI-enabled telehealth services should be mindful of and create clear supervision requirements and boundaries to avoid running afoul of these longstanding laws. These boundaries should identify important guardrails, including whether and how a physician can overrule AI-driven diagnoses, and when must a physician sign off on an AI-generated treatment regimen. Since telehealth is often practiced in multiple states, and because CPOM laws vary from state-to-state, providers utilizing telehealth services must structure their operations to account for the variability of the CPOM prohibitions in various states.

- **Health Disparities.** The implementation of AI-enabled telehealth services also raises important ethical questions about the availability of innovative care. There is a potential that adding AI to telehealth services might shrink the gap between those accessing advanced care technologies and those that are not. For example, **studies** have shown that those with limited English language skills have lower rates of telehealth use. Adding AI virtual assistants to telehealth technology could, for example, help to ensure that language barriers do not get in the way of appropriate care. Rather than finding a provider that speaks a particular language, an AI-enabled telehealth platform could assist by providing translation services in real time in multiple languages. This could allow an AI virtual assistant, for example, to collect more comprehensive medical history during a telehealth visit, thereby providing a greater opportunity for better care and treatment. Incorporating AI into telehealth visits might also allow for better questions that account for how different cultures view disease and treatment, or for diseases that might only affect a narrow sub-population.

But, there is also the possibility that AI-enabled telehealth services might exacerbate the gap between those who have access to the latest innovative technology and those who do not. The growing expansion of telehealth services could risk widening disparities among marginalized populations who may have limited access to necessary **resources**: for example, those who lack access to a computer or smartphone or lack reliable broadband access. The deployment of AI by telehealth providers is likely to lower costs and should improve disparities in access to care. However, in the short term, access to AI-aided telehealth services may be uneven and contribute to a greater disparity in access to care. The addition of AI to telehealth will likely not solve the physical access or cost problems, and it could conceivably add more costs to telehealth technology. Further, many state Medicaid programs do **cover** telehealth visits for their beneficiaries, but the infusion of AI may require state regulators to further examine telehealth coverage policies.

- **Professional Liability & Malpractice.** As AI advances and its capabilities are better leveraged, how will the highly litigious American people respond? Who will be responsible when AI-enabled telehealth results in an unfortunate misdiagnosis? AI and machine learning

are not immune to mistakes. For example, the visual nature of a skin examination lends itself well to the use of machine learning as a potentially valuable tool in teledermatology and the **diagnosis and management** of dermatologic diseases, especially in areas where a dermatologist may not be available. However, just like humans, AI might not always get it right. AI algorithms have some shortcomings, including inapplicability outside of their training domain or bias. We know that **blind spots** in machine learning machines can sometimes imitate the worst societal biases, with a risk of **unintended consequences** that have particular effects on **minority groups**, which can open up providers to increased liability if they depend on these algorithms to assist in diagnosing patients. Who can be held liable for malpractice if a patient undertakes a series of damaging treatments – or fails to seek treatment based on an AI-enabled diagnosis the patient receives through a telehealth platform? The AI developer? The telehealth platform? The individual physician who signed off on the misdiagnosis? And which law applies, especially if the patient is in one state, the telehealth provider in another state, and the AI data platform in yet another state? Further, how much training must a telehealth platform provide its individual physicians regarding the use of AI-infused tools? If a healthcare provider uses AI to treat or diagnose a patient, both the AI developer and the healthcare provider may be exposed to tort liability related to an adverse event. The AI developer can be exposed to products liability claims and the provider may be exposed to malpractice claims. However, without clear legislative direction, it is conceivable that litigants will use the courts to lay out these rules.

- **FDA Implications.** The regulatory framework governing AI is complex. A threshold question for any AI developer is whether their AI-enabled product will be actively regulated by the U.S. Food and Drug Administration (FDA), a question that hinges not only on the product's functionalities, but also its proposed marketing claims. Further, the FDA continues to develop its framework for regulation of AI-enabled products that the agency actively regulates. On January 12, 2021, the FDA **released** the agency's first Artificial Intelligence/Machine Learning (AI/ML)-based Software as a Medical Device (SaMD) Action Plan. This action plan describes a multifaceted approach to advance the FDA's oversight of AI/ML-SaMD, and offers stakeholders several opportunities to engage with the FDA to discuss the agency's oversight approach. For example, upcoming opportunities include the FDA's planned virtual public **workshop** on October 14, 2021 on the role of transparency in enhancing the safety and effectiveness of AI/ML-based SaMD. Stakeholder feedback continues to inform the evolution of FDA's regulatory framework for oversight of AI/ML-based SaMD, including FDA's expectations for such products during premarket review. A thorough understanding of such expectations early in development can inform more efficient development strategies.

Advances in the use of AI in telehealth will no doubt continue. AI's application in telehealth platforms is not just limited to potentially diagnosing a wide range of diseases (like analyzing data from tele-dermatological visits to more accurately diagnose skin cancer); but it can also improve the patient experience (by asking more pinpointed intake questions, for instance), make telehealth visits more efficient (by, for example, more rapidly analyzing a patient's history for a physician in advance of a visit), and help ensure more effective treatment (with AI-generated follow-up adherence or refill calls). AI can reduce differences in clinical practice, improve efficiency, and prevent avoidable medical errors that can help with healthcare costs and improve health outcomes and the patient experience.

But a fundamental component to achieving a safe and effective deployment of AI in telehealth services is ensuring that AI developers, telehealth platforms, and the physicians that leverage these tools have the necessary legal and regulatory guardrails in place. This includes addressing the

application of current privacy and data security regimes, how telehealth providers supervise the use of AI technology to ensure compliance with CPOM laws, and how telehealth providers address growing disparities in access to care.

Value-Based Arrangement Exceptions and Safe Harbors Have Narrow Utility for Medical Device and Pharmaceutical Companies

 On December 2, 2020, the Department of Health & Human Services (HHS) published its long-awaited two final rules – one by the **Office of Inspector General** (OIG) and one by the **Center for Medicare & Medicaid Services** (CMS) – finalizing changes to regulations implementing the federal anti-kickback statute (AKS), the beneficiary inducement provisions of the civil monetary penalty law (CMPL), and the physician anti-self-referral law (Stark Law) and their safe harbors and exceptions. Among the most anticipated aspects of the final rules are the new value-based arrangement AKS safe harbors and Stark Law exceptions.

The two final rules, while complicated, are aligned in their definitions of value-based arrangements.

A **value-based enterprise (VBE)** is two or more participants that: (1) are collaborating to achieve at least one value-based purpose; (2) are each a party to a value-based arrangement with the other (or at least one other participant in the same VBE); (3) have an accountable body or person responsible for financial and operational oversight of the VBE; and (4) have a governing document describing the VBE and how its participants intend to achieve the VBE's value-based purpose(s).

A **value-based arrangement** is an arrangement entered into between (1) a VBE and one or more of its participants, or (2) among participants in the same VBE, for the provision of one or more value-based activities for a target patient population.

A **value-based purpose** is (1) coordinating and managing the care of a target patient population; (2) improving the quality of care for a target patient population; (3) appropriately reducing the costs to, or growth in expenditures of, payors without reducing the quality of care for a target patient population; or (4) transitioning from health care delivery and payment mechanisms based on the volume of items and services provided to mechanisms based on the quality of care and control of costs of care for a target patient population.

While the new AKS safe harbors exclude pharmaceutical and medical device manufacturers, distributors, and wholesalers; DMEPOS suppliers; laboratories; compounding pharmacies; and pharmacy benefit managers, there is a narrow exception intended to facilitate the deployment of

health technologies for care coordination. These entities are eligible for protection under the care coordination safe harbor as "**limited technology participants**" that exchange "**digital health technology**" (defined broadly) with a VBE or VBE participant. The OIG Final Rule provided as an **example** "a medical technology company could partner with physician practices, to better coordinate and manage care for patients discharged from a hospital with digitally-equipped devices that collect and transmit data to the physicians to help monitor the patients' recovery and flag the need to intervene in real time (e.g., a device that monitors range of motion that could inform what an appropriate physical therapy intervention may be). The technology company could provide the physician group with necessary digital health technology that improves the physician group's ability to observe recovery and intervene, as necessary." However, the OIG final rule requires that the exchange of digital health technology by a limited technology participant is *not* conditioned on any recipient's exclusive use of, or minimum purchase of, any item or service manufactured, distributed, or sold by the limited technology participant.

The Stark Law final rule does not exclude such entities from qualifying as VBE participants under any exception for value-based arrangements. However, because the Stark Law is focused on prohibiting self-referrals by physicians, the new Stark Law exceptions for value-based arrangements will be of limited value to medical device and pharmaceutical companies.