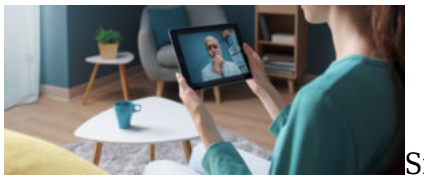
DEA Publishes Temporary Rule on the Extension of COVID-19 Telemedicine Flexibilities for Prescription of Controlled Substances

 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.

CMS Continues to Modernize by Expanding Reimbursement for Digital Health Services

The COVID-19 Public Health Emergency ("PHE") fundamentally changed the healthcare industry, forcing healthcare providers and patients onto their computers and phones to enable continuation of care when patients were mandated to stay home across the country. Prior to the COVID-19 PHE, approximately 12,5000 Medicare beneficiaries received telehealth services and only 106 telehealth services were reimbursable. By October 2020, over 24.5 million (of 63 million) Medicare beneficiaries received telehealth services.

Read the **client alert**.

On Remote Control: FDA Issues Draft Guidance to Facilitate Use of Digital Health Technologies for Remote Data Acquisition in Clinical Trials

 During the COVID-19 pandemic, decentralized clinical trials and remote patient monitoring and data acquisition became a necessity, accelerating the use of digital health technologies in clinical trials. Acknowledging that technological advances "have revolutionized the ability to remotely obtain and analyze clinically relevant information from individuals" and that "DHTs [ ] are playing a growing role in health care and offer important opportunities in clinical research," the FDA issued during the last week of December 2021 a draft guidance, ***Digital Health Technologies for Remote Data Acquisition in Clinical Investigations***, which provides recommendations for sponsors, investigators and other stakeholders to facilitate the use of DHTs for remote data acquisition in clinical trials, including clinical trials that will be submitted to the FDA in a marketing application for a medical product.

The draft guidance defines a digital health technology (DHT) as a system that uses computing platforms (such as a mobile phone, tablet, or smart watch), connectivity, software, and/or sensors for healthcare and related uses. Some DHTs may meet the definition of "device" under the Federal Food, Drug and Cosmetic Act, but the draft guidance specifically does not address the circumstances under which a DHT would meet the statutory definition of a device and notes that DHTs used in clinical investigations generally are exempt from premarket clearance or approval requirements, as long as the clinical investigation is compliant with 21 CFR Part 812.

The draft guidance explains that sponsors must foremost ensure that a DHT is "**fit-for-purpose**" for its proposed use in a specific clinical investigation. In essence, the level of verification and validation associated with the DHT must be sufficient to support its use and interpretability in the clinical investigation. This may require sponsors to work with the developer or manufacturer of the DHT, patients, caregivers, and other technical and clinical experts to assure that the DHT is suitable for its intended purpose in the clinical investigation. The draft guidance advises sponsors to select a DHT that corresponds to the clinical outcome to be assessed, and that considers the clinical trial population and the design/operating characteristics of the DHT that may affect trial participants' use of the DHT.

Sponsors should also be prepared to describe how they will analyze data collected from DHTs in their statistical analysis plan, including prespecifying "**intercurrent events**" (defined as events that occur after treatment initiation that result in missing or erroneous data associated with the clinical outcome of interest) that may be related to the DHT and/or the general purpose computing platform, and how these events will be accounted for in the analysis. To maintain data integrity, FDA recommends that the output of the DHT and associated metadata be transmitted to a **durable electronic data repository** that is protected from alterations and maintained until the end of the record retention period. FDA generally will consider data in such a repository to constitute the source data and should be made available for inspection and to reconstruct and evaluate the clinical investigation.

FDA further notes that "unique privacy risks" may arise when DHTs are used in a clinical trial. Sponsors are advised to evaluate the risk of potential disclosures of personally identifiable

information through breaches of the DHT, the general computing platform on which the DHT runs, and/or the durable electronic repository, assure appropriate security safeguards are in place, and consider including such information in the informed consent documents for the clinical trial.

The draft guidance recommends that sponsors:

- train trial participants and trial personnel on the use of DHTs and develop a plan to provide technical assistance to trial participants and study personnel;
- develop a risk management plan to address potential problems with the DHT (e.g., interference between mobile applications, or loss, damage and replacement);
- develop a safety monitoring plan that addresses how abnormal measurements related to participants' safety measured by DHTs will be reviewed and managed; and
- develop a contingency plan for any changes to the DHT (e.g., discontinuation of a specific model, operating system updates)

The draft guidance includes appendices with specific examples of how different types of DHTs could be incorporated into a clinical investigation. Given the particular circumstances of each DHT and clinical investigation, the draft guidance encourages sponsors to engage early with the appropriate FDA Center responsible for the medical product under development to discuss the proposed use of DHT(s) in a clinical investigation and, for DHTs or DHT-collected endpoints that require qualification, engage with an appropriate FDA qualification program, such as the **Medical Device Development Tool Qualification Program**.

Comments on the draft guidance are due March 23, 2022.

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.

The Office of the National Coordinator for Health Information Technology Interoperability and Information Blocking Final Regulation: Key Concerns for Health Information Technology Companies and Developers

As of April 5, 2021, **health information technology companies and developers are required to comply with the information blocking provisions** of the Centers for Medicare and Medicaid Services' (CMS) and the Office of the National Coordinator for Health Information Technology's (ONC) Information Blocking Final Regulation ("Final Rule"), implementing specific provisions of the **21st Century Cures Act** (the "Cures Act"). The objective of the Final Rule is to (i) promote interoperability and support the access, exchange, and use of electronic health information; and (ii) reduce burdens and costs related to accessing electronic health information and to reduce occurrences of information blocking.

While compliance with the Final Rule is required, enforcement mechanisms are still evolving and are not yet final. This affords health information technology ("Health IT") companies and developers the time and opportunity to familiarize themselves with the Final Rule and the **exceptions** outlined by the ONC.

What does the Final Rule require or prohibit?

The Final Rule prohibits so-called "Actors" from engaging in information blocking practices—such as *interfering, preventing, or substantially discouraging the use, access, and exchange of electronic health information*. An "Actor" is any individual or entity that is a (i) health care provider, (ii) developer of Health IT, (iii) health information network, and/or (iv) health information exchange. There is no duty to proactively make electronic health information available, but these entities must not engage in information blocking practices in response to a legal request for electronic health information.

What is information blocking and why is it discouraged? What are examples of information blocking?

The Final Rule was promulgated by the ONC because Congress expressed concern that Health IT companies were knowingly interfering with the free exchange of information. Information blocking is such a practice, and involves any efforts that are likely to materially discourage the access, use, and/or exchange of electronic information when the entity knows that the practice is likely to do so.

The types of behavior that would be considered information blocking include (i) refusing to provide electronic health information or ignoring reasonable requests; (ii) imposing any unreasonable limitations on the use or requests for access to share electronic health information; (iii) establishing contracts, business associate agreements, licensing terms, and/or policies that would unnecessarily restrict the sharing of electronic health information; and (iv) configuring technology in a way to limit interoperability.

Put another way, if an electronic health record platform were to restrict its software such that a user is able to export electronic health information for its own use without a fee, but any request to transfer or exchange electronic health information to a competitor's platform would require a fee, the company's activity would likely be considered inappropriate information blocking under the

Final Rule.

What constitutes electronic health information?

"Electronic health information" includes electronic protected health information ("ePHI") as defined under HIPAA, if such ePHI is maintained in a HIPAA designated record set ("DRS"). However, unlike HIPAA the new information blocking regulations do not apply to hand written or verbal health data. Additionally, it is important to note that records do not have to be used or maintained by or for a HIPAA covered entity to fall within the definition of electronic health information.

What agency is responsible for enforcement of the Final Rule?

The Cures Act authorizes the Office of Inspector General ("OIG") to investigate any allegations of information blocking. Health IT companies and developers could face up to $1,000,000 in civil monetary penalties per violation. If an OIG's investigation and determines that an Actor has engaged in information blocking activities, the OIG will refer the provider to the appropriate agency to address the alleged violation (e.g. a HIPAA privacy violation would be referred to the Office for Civil Rights to address the violation). The OIG has issued a proposed rule for enforcement outlining enforcement priorities and has requested input on the proposed rule. Any conduct prior to the effective date of the OIG's rule will not be subject to civil monetary penalties.

How does the Final Rule impact the health information sharing community and Health IT companies and businesses?

Companies should ensure current privacy policies and practices with respect to sharing electronic health information comply with the Final Rule. Companies' vendors and Health IT systems should also ensure that the information infrastructure simultaneously protects the transfer electronic health information and facilitates the flow of electronic health information between Health IT systems. Companies should also review current business associate agreements and consider any updates that may be necessary to comply with the new information blocking regulations.

Additionally, companies may also want to consider implementing a policy and procedure that covers the review of all proposed transactions and arrangements, which involve the transfer of electronic health information, to ensure compliance with the Final Rule. This is especially important for Health IT companies to consider as developers and managers of software solutions for providers and other customers.

As regulators continue to push for accountability in the Health IT industry and ultimately the improvement of overall patient care, Health IT developers and businesses must welcome and embrace software and technologies that facilitate compliant sharing of electronic health information.

*Follow our **blog** to receive additional updates and alerts on the Final Rule and the OIG's proposed final rule. Our health care regulatory team intends to publish more in-depth guidance on the nuances of these regulations for Health IT companies and developers.*

Federal Audits and Enforcement Actions of

Telehealth Providers: Future Trends and Mitigating Risk

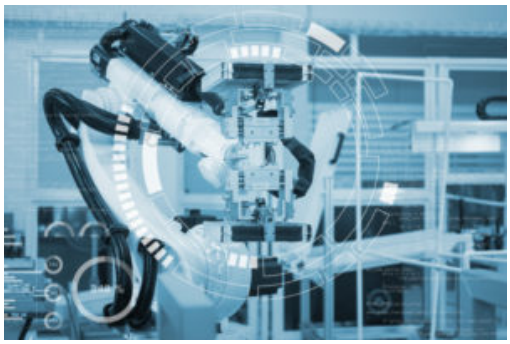
 As the COVID-19 pandemic progresses and the expanded use of telehealth has appeared to stabilize over the past year according to a **July report from McKinsey & Company**, Federal agencies have continued the recent trend of enforcement actions and audits of telehealth providers.

On September 17, 2021, the U.S. Department of Health and Human Services Office of Inspector General (HHS OIG) and U.S. Department of Justice (DOJ) **announced their latest enforcement action**, totaling $1.4 billion, with approximately $1.1 billion involving alleged telehealth fraud. This is the latest action taken by enforcement agencies, with a **$143 million COVID-19 enforcement action announced in May 2021** and a **$4.5 billion telehealth enforcement action announced in September 2020**. These actions have focused in part on the use of telehealth to submit fraudulent claims to private payors as well as Federal health care programs. The May 2021 enforcement action involved fourteen defendants in seven Federal judicial districts and the September 2020 enforcement action involved over three-hundred defendants in fifty-one Federal judicial districts.

This most recent round of enforcement actions from September 2021 targeted telemedicine executives who were alleged to have paid physicians the nurse practitioners in exchange for ordering durable medical equipment, genetic testing, other diagnostic tests, and pain medications that were considered unnecessary. The government charged that items were ordered without patient interactions or minimal telephonic conversations, and that the physicians and nurse practitioners at issue had never even met or seen their patients. Additionally, in January 2021, HHS OIG announced a **series of audits** reviewing Medicare Part B payments to telehealth providers during the public health emergency to determine whether Medicare requirements were met. The first phase of audits focus on whether services such as evaluation and management, opioid use disorder, end-stage renal disease, and psychotherapy met Medicare requirements. The second phase includes additional audits regarding distant and originating site locations, virtual check-in services, electronic visits, remote patient monitoring, use of telehealth technology, and annual wellness visits.

While the long-term effects of Federal agency actions remain unclear, so long as telehealth is utilized at a substantial level, government agencies will likely continue to scrutinize telehealth industry practices to mitigate fraud, waste and abuse. Telehealth providers and others in the industry can decrease the likelihood and impact of being audited or charged in an enforcement action by structuring their compliance programs and operations to abide by Federal health care program requirements such as provider credentialing, sufficient medical necessity documentation, program integrity requirements and other coverage and reimbursement issues.

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.