

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 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.

[List of Artificial Intelligence and Machine Learning \(AI/ML\)-enabled Devices Available on FDA's Website](#)



The U.S. Food and Drug Administration (FDA) now provides a list of [Artificial Intelligence and Machine Learning \(AI/ML\)-Enabled Medical Devices](#) that are legally marketed in the United States. These include devices (1) cleared via 510(k) premarket notifications, (2) authorized pursuant to De Novo requests, and (3) approved via premarket approval applications, or PMAs. FDA explains that the list, developed by FDA's Digital Health Center of Excellence, while not exhaustive or comprehensive, is intended to increase transparency and access to information on these devices that span across medical disciplines.

Read the [client alert](#).

[Judge Dismisses Pfizer's Lawsuit Over HHS Limits on Drug Copay Assistance](#)



In a previous [post](#) published on the Washington Legal Foundation's Legal Pulse blog, Goodwin Partners Matt Wetzel and William Jackson discussed the potential implications of a high-profile recent lawsuit lodged by Pfizer against the U.S. Department of Health and Human Services ("HHS") Office of Inspector General's ("OIG") over Pfizer's drug

copay assistance.

Pfizer's lawsuit sought a declaration that two copay assistance programs it designed to help patients afford its drug for the treatment of Transthyretin Amyloid Cardiomyopathy ("ATTR-CM") would not violate the Anti-Kickback Statute or Beneficiary Inducement Statute. The drug is the only FDA approved treatment for such disease. Originally, Pfizer, under the advisory opinion process, had requested OIG determine if either of the programs would violate the Anti-Kickback Statute. In an earlier [post](#), we identified the need for the federal government to issue clear standards that would provide drug companies and others with clear notice as to the rules in this area.

On September 30, 2021, the U.S. District Court for the Southern District of New York [ruled](#) against Pfizer, (a) refusing to make a determination on one of the proposed copay programs and (b) ruling that the government's appropriately made its prior prohibition of the company's other copay program. We examine each below.

The Independent Charity Program

Pfizer originally requested an advisory opinion approving the company's proposal to fund an existing third-party charity's copay assistance fund, which would in turn provide financial support to qualifying patients to cover the costs of their co-pays. The OIG refused to provide such an opinion. OIG indicated it was investigating a substantially similar course of action. Further, OIG stated that a Corporate Integrity Agreement with Pfizer prohibited OIG from approving a second similar program. [HHS regulations prohibit OIG](#) from issuing an advisory opinion where "[t]he same, or substantially the same, course of action is under investigation, or is or has been the subject of a proceeding involving the Department of Health and Human Services or another governmental agency."

Pfizer then brought suit in the U.S. District Court for the Southern District of New York, arguing that the Court had the power to issue a determination on whether the Independent Charity Program would violate the Anti-Kickback Statute or Beneficiary Inducement Statute. The Court, however, refused. The Court asserted the claim was too far remote and the facts too underdeveloped to satisfy the prudential ripeness criteria.

The Direct Program

While OIG refused to issue an advisory opinion on Pfizer's independent charity program, it did issue a advisory opinion against Pfizer's other proposal to directly fund patients' co-pays, including for government beneficiaries. OIG's [opinion](#) found Pfizer's controls and patient qualifications insufficient to curb the risk of fraud and abuse. It stated that, because there existed off-label treatments alternative to the FDA-approved treatment, the program would risk of patient steering and have anti-competitive effects. Further, OIG stated the program circumvented one of HHS's key pricing controls - i.e. requiring Medicare beneficiaries to cover some portion of the costs for their care in order to help ensure more considerate, comprehensive care decisions - and thereby exposing beneficiaries to the economic effects of drug pricing.

When the OIG's advisory opinion was challenged in the lawsuit, the Court stated that OIG's conclusion was *not* contrary to law. Because (i) the Anti-Kickback Statute prohibits "all remuneration that induces purchases of drugs (unless payments fall into one of the safe harbors)", and (ii) the intent of the program was to increase the number of Medicare beneficiaries who purchase the drug, the Court stated it was unable to issue a judgment in Pfizer's favor.

Key Takeaways

What is the impact of the Court's decision? Outside of its obvious impact on Pfizer's ability to fund the specific independent charity program and its own copay assistance plan at issue in the litigation, we believe the impact will be slim. The government has made clear for many years that it expects any sort of charity support or copay assistance to come with significant controls and guardrails in place. Those principles still stand. The Court's decision in the Pfizer matter reaffirms the OIG's significant discretion in deciding how to enforce and interpret the health care fraud and abuse laws. The government will continue to expect strong controls in place for these sorts of arrangements – especially if Medicare beneficiaries are involved – and will continue to scrutinize single-drug assistance funds carefully.

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.

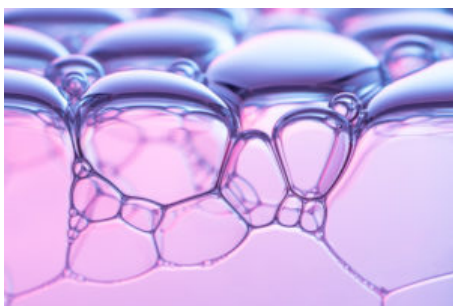
On September 17, 2021, the U.S. Department of Health and Human Services Office of Inspector General (HHS OIG) and U.S. Department of Justice (DOJ) [announced their latest enforcement action](#), totaling \$1.4 billion, with approximately \$1.1 billion involving alleged telehealth fraud. This is the latest 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.

[Goodwin Virtual Series: Foundations in Healthcare Compliance for Life Sciences Companies](#)



In the ever-evolving life sciences industry, compliance is top-of-mind for investors, business leaders, the public and the government. Life sciences companies are subject to increased enforcement efforts and greater public scrutiny, and boards, investors, and other key stakeholders call for more and better compliance controls. As a result, there are increased expectations on what compliance programs should cover and what resources should be dedicated to making these programs successful.

With the growing importance of compliance for emerging life sciences companies, Goodwin and the Berkeley Research Group are pleased to announce our inaugural **Foundations in Healthcare Compliance** series, a multi-part training series where participants will learn from experienced lawyers and professionals about the various considerations when building and growing a compliance program in the life sciences industry.

This five-week series is designed for new compliance officers, in-house counsel or their delegates and investor clients seeking more information about compliance in the life sciences market. We will offer CLE credit for lawyer attendees and non-lawyer compliance certification (HCCA), if available.

For further information and to request an invitation to the series check out the [Foundations in Healthcare Compliance mini site](#).

Exactly One Year Later, CMS Reverses Course on Covering Innovative MedTech



In September 2020, the Centers for Medicare & Medicaid Services (CMS) [proposed](#) a new rule that would expedite Medicare coverage for medical technology approved through the Food & Drug Administration's (FDA's) "Breakthrough Devices Program." CMS's proposal – the Medicare Coverage of Innovative Technology, or MCIT, Pathway – was groundbreaking in that innovative medical technology would be afforded a new, expedited coverage avenue that would significantly reduce the time it takes for Medicare beneficiaries to gain access to and benefit from innovative technology. It published the [final rule](#) on January 14, 2021.

But, just one year later on September 15, 2021, CMS plans to rescind the MCIT pathway altogether. As a result, the medical technology industry, providers, and patients, which had looked favorably upon the agency's MCIT proposal, will continue to face the uphill climb of traditional Medicare coverage for medical devices.

Medicare Coverage of Medical Technology

Prior to CMS's proposal, FDA marketing authorization of a breakthrough device did not mean immediate access for Medicare beneficiaries. Instead, Medicare rules required even greater effort on the part of manufacturers and providers for Medicare to actually pay for the technology.

Under traditional Medicare coverage rules, even if the FDA granted a particular product marketing authorization, CMS separately determines if the device should be considered "reasonable and necessary" for patient diagnosis and treatment via a National Coverage Determination (NCD) from CMS or via a Local Coverage Determination (LCD), made by one or more Medicare Administrative Contractors, or MACs. This process, which includes evidence-based reviews, is lengthy and – in the case of an LCD – may even result in different standards in different geographies, based on the location of the MAC. And, as the medical technology industry has repeatedly emphasized, the result is that America's seniors and others dependent upon Medicare coverage, would have to wait – in some cases for years – to access the most innovative technology.

MCIT Proposal - An Expedited Avenue to Coverage for Innovation

Under the original 2020 proposal's MCIT coverage path, CMS would offer a four-year period after FDA marketing authorization for breakthrough status medical technology to be reimbursed by Medicare, thereby bypassing the NCD or LCD process. If the technology did not have an existing

Medicare benefit category or was excluded from Medicare coverage by statute, MCIT would not be available. During the MCIT path's four-year period, medical device makers would be encouraged (not required) to develop additional clinical evidence and to collect additional data. And at the end of the four years, the device would be subject to an NCD that either grants or denies Medicare coverage or offers MACs the discretion to conduct claim-by-claim adjudication or an LCD.

Put another way, the MCIT path would significantly abbreviate what has become a lengthy coverage process and would provide Medicare beneficiaries with quicker access to advanced, innovative technology.

In promulgating the MCIT coverage path, then-CMS Administrator Seema Verma [emphasized](#) its goal of expediting the delivery of advanced, innovative technology to Medicare beneficiaries, and diminishing administrative burdens on that hamper or slow this process. Verma noted, "Government processes have slowed beneficiaries' access to innovative treatments. Despite being deemed safe and effective by the FDA, Medicare beneficiaries have not had predictable, immediate access to innovative breakthrough devices . . . [t]he MCIT rule will eliminate this lag time for both seniors and innovators."

MCIT Proposal's "Reasonable and Necessary" Definition

The MCIT rule also addressed another critical issue for the Medicare program: defining the term "reasonable and necessary." Under the [current regulatory framework](#), Medicare may only cover items and services that are classified as "reasonable and necessary" for the diagnosis or treatment of an illness or injury. Notably, this term – despite its clear significance – is not defined in the statute or regulations. The term is defined only in informal guidance (i.e., the [Medicare Program Integrity Manual](#)).

The [MCIT Final Rule](#) sought to codify and expand the definition of "reasonable and necessary" as laid out in the Medicare Program Integrity Manual. In expanding the definition, the [MCIT Final Rule](#) stated that, in addition to meeting any of the qualifications outlined in the [Medicare Program Integrity Manual](#), items and services may be deemed "reasonable and necessary" based on CMS review of commercial insurer coverage decisions and policies. At the time of the [MCIT Final Rule](#), CMS stated that it would publish a draft methodology for determining when commercial insurers' policies could be considered to meet the definition of "reasonable and necessary." Most notably, Verma [emphasized](#) that this portion of the rule would help give innovators a clearer understanding of CMS standards.

A New Administration, a New Approach

Despite the clarity provided by the MCIT rule, despite the certainty offered Medicare beneficiaries to accessing innovative technology, and despite the release of a final rule in January 2021, the Biden Administration now plans to kill the MCIT path outright, citing the following reasons for its decision to rescind what had promised to get seniors better access to advanced technology:

- **Lack of Adequate Studies:** There is no FDA requirement that Medicare beneficiaries be included in clinical studies needed for market authorization. CMS, not FDA, typically requires and reviews evidence specific to medical devices for the Medicare population. By automatically granting national Medicare coverage to devices that receive FDA market authorization, the MCIT path would have eliminated CMS's ability to ensure whether medical device makers have generated adequate evidence that the breakthrough device would be reasonable and necessary for the Medicare patients that have the particular disease or

condition that the device is intended to treat or diagnose.

- **Limited Ability to Revoke Coverage:** Traditionally, CMS reserves the right to deny coverage if it learns that particular devices may be harmful to Medicare beneficiaries. The MCIT path limited such rights for breakthrough medical devices with FDA market authorization. Under the MCIT path, CMS would only be able to expeditiously remove a Breakthrough Device from MCIT coverage for limited reasons, such as if FDA issued a warning letter or removed marketing authorization for the device.
- **Disincentivizing Development:** According to CMS, by incentivizing devices eligible for FDA breakthrough device designation, the MCIT path may have the unintended consequence of disincentivizing development of innovative second-to market devices and subsequent technologies of the same type that would not be eligible for breakthrough device designation.

CMS also plans to return to the drawing board on the definition of “reasonable and necessary,” noting the following:

- **The Definition Removes Flexibility for the Agency:** Suggestions to codify or expand the definition of “reasonable and necessary” to include commercial insurer policies may remove existing flexibility and could even impact CMS’s ability to ensure equitable health care access.
- **Need for a Separate Rule.** Given the implications the definition has for Medicare policy above and beyond just the coverage of innovative medical technology, the agency notes that the definition should be included in a separate rule.

Conclusions

While CMS’s decision to rescind the MCIT Pathway appears to be a *fait accompli*, **comments to the agency’s proposed rule are due on or before October 15, 2021**. If finalized, it is unclear whether the agency will revisit the concept in the future or whether the industry will continue to face lengthy delays between the time a medical device is authorized and the time America’s seniors will benefit. CMS will continue to require and review evidence specific to the Medicare population to cover medical devices– a lengthy process that is above and beyond any clinical evidence produced as a result of any clinical studies required for FDA authorization.

Further, stakeholders will continue to face uncertainty. This includes **providers** (who will not be certain that their claims for procedures or products will be paid, especially if handled on a claim-by-claim basis or if subject to varied and differentiated local decisions from contractors); **patients** (who may or may not be able to access innovative technology), and **medical device makers** (who may be required to undergo significant evidence collection processes, not to mention delays in recouping the funds invested into developing and building the medical technology in the first place).

We will continue to monitor and provide updates on this important issue for the medical technology industry. If you have any questions or would like to submit comments, please reach out to Matt Wetzel (mwetzel@goodwinlaw.com).

Florida Joins List of States Requiring Licensure for Genetic Counselors



Many allied health professionals are subject to state-level licensing requirements that can vary from jurisdiction-to-jurisdiction. What may be required in New York to hold a medical professional license may differ dramatically from what is required in Illinois or Texas, for instance. One state's requirements may be onerous and administratively taxing; another state's requirements to serve as the same type of medical professional may be quite simple. Assessing licensing requirements for medical professionals from state to state can also involve rapid change, with state legislatures and state licensing boards revising and changing standards on a regular basis.

Most recently, Florida has joined a number of states that require the licensure of genetic counselors by the Florida Department of Health. Genetic counselors play an increasingly important role in the delivery of care. These professionals hold specialized training in genetics and help patients better understand family history, heredity, and how conditions can arise. Genetic counselors can also aid family members in making better and more knowledgeable choices when it comes to selecting patient care, assisting with questions about the most appropriate testing, educating about genetic disorders, and even helping people cope with troubling diagnoses. The [National Society of Genetic Counselors](#) ("NSGC") describes genetic counselors as "not doctors" but having advanced training in medical genetics and counseling to guide patients on inherited diseases and conditions.

Given this advanced training, and given the critical role that genetic counselors can play with patients, according to NSGC, at least 30 states require licensure for the practice of genetic counseling, Florida being the latest state to join this list.

The New Florida Genetic Counseling Licensing Requirement. Florida's [Genetic Counseling Workforce Act \(the "Law"\)](#), which became effective on July 1, 2021, requires genetic counselors to meet specific qualifications and examination requirements and to register to hold a genetic counseling license. The Law defines "genetic counseling" to include activities such as: obtaining and evaluating individual, family, and medical histories to determine genetic risk for genetic or medical conditions and diseases in a patient, his or her offspring, and other family members; Integrating genetic laboratory test results and other diagnostic studies with personal and family medical history to assess and communicate risk factors for genetic or medical conditions and diseases and providing written documentation of medical, genetic, and counseling information for families and health care professionals. The Law prohibits the unlicensed practice of genetic counseling, calling it a second degree misdemeanor to, among other things, "[p]ractice genetic counseling or hold [oneself] out as a genetic counselor or as being able to practice genetic counseling or to render genetic counseling services without a license," unless specifically exempted. § 483.916. This is a broadly worded prohibition and could very conceivably be applied to out-of-state practitioners. The only exemptions are for commissioned medical officers in the U.S. Armed Forces or Public Health Service or health care practitioners (like physicians, nurses, or physicians assistants) operating within the scope of his or her license.

For those who are required to register and hold a Florida genetic counseling license, the Law requires that an individual (1) has a master's degree in genetic counseling or a doctoral degree from a medical genetics training program; and (2) has passed an examination to be certified by such by either the American Board of Genetic Counseling, the American Board of Medical Genetics or Genomics, the Canadian Association of Genetic Counsellors, the American Board of Medical Genetics and Genomics or the Canadian College of Medical Geneticists.

The Telehealth Gap. Genetic counseling is unique in that evaluating a patient's health and family history and genetic test results could be done almost entirely via telehealth technologies. Genetic counselors could conceivably see patients all over the country and deliver equally effective services whether someone is next door or several time zones away. But, the law includes a gap: under the new Florida Law, the legislature did not add genetic counseling to the list of Florida's telehealth providers.

The Law's failure to include genetic counselors on the list of Florida's "[telehealth providers](#)" (Florida Statute Sec. 56.47(1)(b)) is quite likely a legislative oversight and is not intended to prohibit genetic counselors from leveraging telehealth technologies to deliver their services. As written, however, under the new Law, if genetic counselors do employ telehealth to deliver genetic counseling services to patients in Florida, it could technically be found to fall outside the scope of practice and could conceivably be considered the unlicensed practice of genetic counseling, which is a misdemeanor (FL Stat. §§ 483.916(2)).

This concern is highlighted when it comes to out-of-state genetic counselors. The Law does not distinguish between in-state and out-of-state genetic counselors. This means that out-of-state genetic counselors may also find themselves subject to the Law's background and registration requirements if providing services to Florida residents. In fact, the Law does not require that applicants for licensure be Florida based or pass a Florida specific exam. The examinations required for licensure are national and international board exams. Accordingly, an out-of-state genetic counselor would most likely be required to obtain licensure to provide services to Florida residents. But, taken together with the Law's silence on telehealth usage, this means that a genetic counselor based elsewhere in the country could conceivably register as a genetic counselor in Florida but not be able to use telehealth technologies to deliver that care.

Next Steps. The Florida Department of Health's [genetic counseling licensing page is available here](#). We will continue to monitor if Florida legislature updates the Law to add genetic counselors to the definition of telehealth providers, and whether the state issues additional guidance for out-of-state practitioners and the requirements they must meet. We will also continue to assess whether other states will join Florida in requiring licensure for genetic counselors.

[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.

[HHS, Labor, and Treasury Departments Defer Enforcement of Transparency in Coverage and No Surprises Act Requirements](#)



The No Surprises Act and Transparency in Coverage final rules go into effect January 1, 2022. Implemented as Titles I and II of Division BB of the Consolidated Appropriations Act, these rules are intended to protect patients from surprise medical bills and increase transparency by requiring certain health care facilities and insurers to disclose certain information. The U.S. Departments of Health & Human Services, Labor, and Treasury are jointly charged with implementing specific sections of the [No Surprises Act](#) and [Transparency in Coverage](#) final rules. On August 20, 2021, however, these agencies jointly announced through an [FAQ](#) published on HHS's website that they are deferring enforcement of certain requirements from the final rules.

One of the No Surprises Act's final rule's requirements is that certain health care providers and facilities must provide a good faith estimate of an individual's expected charges for health care items or services, if the individual is enrolled in a health plan and seeks to submit a claim to the plan. The government, recognizing that providers and facilities must develop complex technical infrastructure to comply with this provision, has decided to defer enforcement of this portion of the final rules until it can issue further rules on implementing these requirements. For nearly identical reasons, the government also decided to defer enforcement of requirements that plans and health insurance issuers provide individuals an advanced explanation of benefits pending further rulemaking.

The government further stated its plan to streamline some of the overlapping requirements in the No Surprises Act and the Transparency in Coverage final rules. For example, the Transparency in Coverage rule requires certain group health plans and health insurance providers to publicly disclose specified information about their in-network provider rates, out-of-network allowed amounts and billed charges for covered items and services, and negotiated rates and historical net prices for prescription drugs in separate, machine-readable files for plan years beginning on or after January 1, 2022. ("Grandfathered" health plans and health insurance providers, however, are exempt from these rules if they were in place prior to the March 2010 enactment of the Affordable Care Act.)

The government has decided to defer enforcement of the Transparency in Coverage rules that require plans and health insurance issuers to publish machine-readable files related to prescription drug pricing pending further rulemaking, given overlap with similar requirements in the No Surprises Act. The government also indicated it will defer enforcement of all other machine-readable file publication requirements of the Transparency in Coverage final rule until July 1, 2022.

The requirements of the No Surprises and Transparency in Coverage final rules are complex and will require significant effort from health plans, healthcare facilities, and others to implement. Despite the government's decision to defer enforcement of certain requirements, health care facilities and health insurance providers should begin preparing to meet as many of these requirements as possible - and should do so as soon as possible. This starts with understanding which of the myriad remaining No Surprises Act and Transparency in Coverage requirements still apply to which health plans or healthcare facilities.

Partnering with trusted legal counsel early on can help ensure health care providers and insurers are prepared when the full requirements of the No Surprises Act and Transparency in Coverage rules begin being enforced by the government.

DOJ Recoups a total of \$1.8 Billion from Health Care Fraud in 2020, Laboratory Recoupments Alone Account for Hundreds of Millions



The Department of Justice (“DOJ”) **has reported** that in 2020, the government prosecuted dozens of laboratory owners and operators for anti-kickback related offenses responsible for hundreds of millions in alleged federal health care program losses. DOJ recouped a total of \$1.8 billion dollars in connection with healthcare fraud allegations.

Since the public health emergency was announced in March 2020, the Centers for Medicare & Medicaid Services, the U.S. Department of Health and Human Services (“HHS”), Office of the Inspector General (“OIG”), and other law enforcement agencies partnered to investigate and prosecute health care fraud from identified risk areas, including unnecessary laboratory testing related to the COVID-19, genetic sequencing, and cardiac panels.

Laboratories prosecuted in the last two years for health care fraud include: UTC Laboratories Inc. (RenC) (\$41.6 million), Boston Heath Diagnostics Corporation (\$26.7 million), Logan Laboratories Inc. (\$41.0 million), Genova Diagnostics (\$43.0 million).

According the to the report, “[t]hroughout FY 2020, HHS-OIG issued 178 audit reports and 44 evaluations, resulting in 689 new recommendations issued to HHS operating divisions. HHS operating divisions also implemented 286 recommendations during FY 2020.” Laboratory-related audit and evaluation findings are as follows:

- “Medicare Advantage (MA) encounter data continue to lack National Provider Identifiers (NPIs) for providers who order and/or refer durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS); clinical laboratory services; imaging services; and home health services. However, almost all MA organizations have data systems that are able to receive and store these NPIs when providers submit them. In addition, a substantial portion of MA organizations reported that providers already are submitting the ordering provider NPIs on claims or encounter records for DMEPOS, laboratory services, and imaging services. Further, a majority of MA organizations require NPIs to be submitted for their other lines of business. Finally, almost half of MA organizations believe that using NPIs for ordering providers is

critical for combating fraud.”

- “Total Medicare Part B spending for lab tests increased to \$7.6 billion in 2018, despite lower payment rates for most laboratory (lab) tests. The \$459.0 million spending increase was driven by: (1) increased spending on genetic tests; (2) ending the discount for certain chemistry tests; and (3) the move to a single national fee schedule. Congress mandated that the Office of Inspector General monitor Medicare payments for lab tests and the implementation and effect of the new payment system for those tests. This report also provides the fifth annual analysis of the top 25 lab tests by Medicare spending.”

Importantly, the report indicates that in 2021 and 2022, DOJ-OIG will have more resources, more complete data, and will therefore be able to provide even more oversight of health care fraud, resulting in “a steady increase in healthcare related audits, inspections, and investigations.”