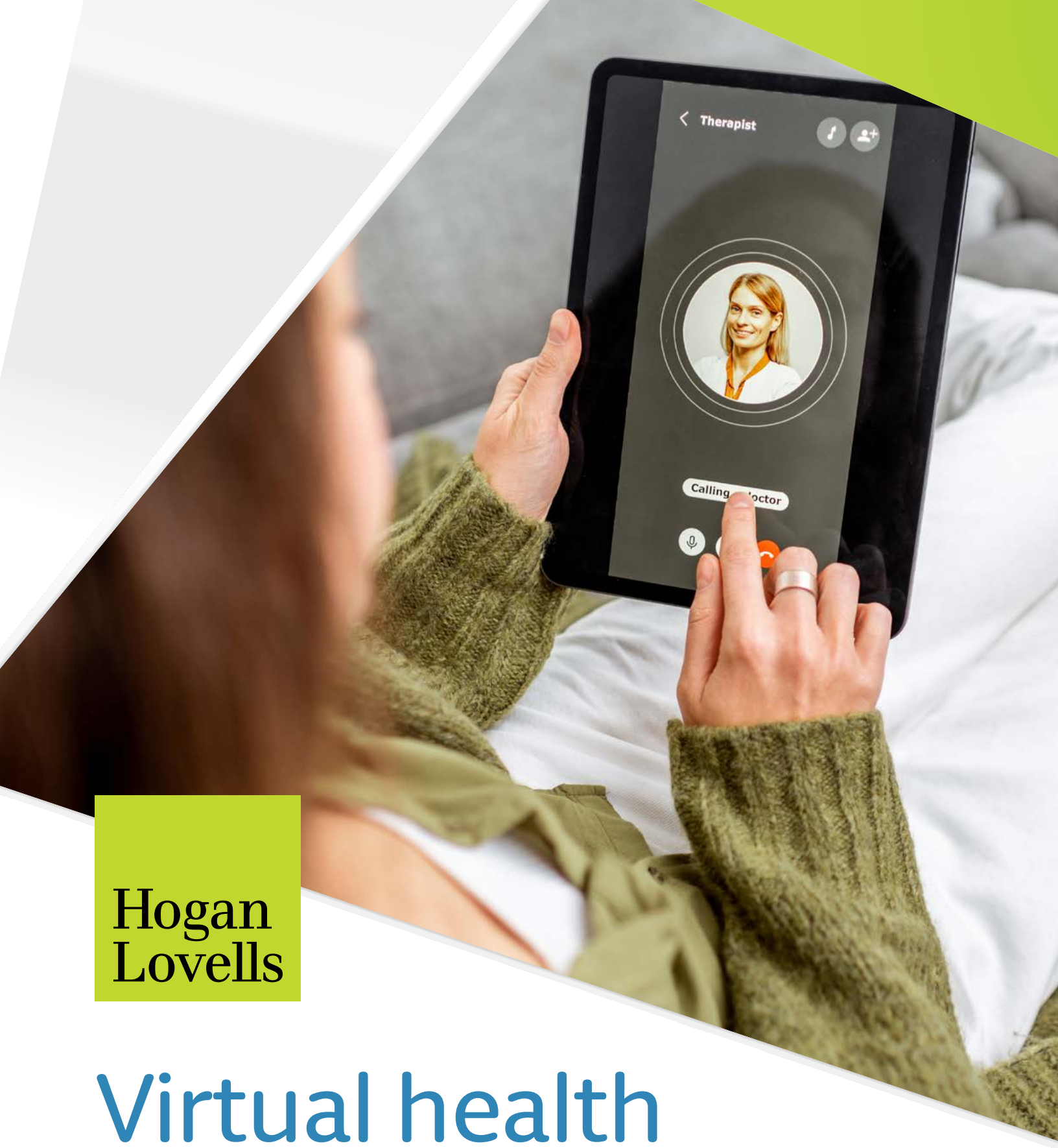


Hogan Lovells

Virtual health

What's on the horizon for telehealth and remote monitoring

What's on the horizon for telehealth and remote monitoring

As the world responds to the COVID-19 pandemic, physicians and patients increasingly turn to virtual health solutions, including telehealth and remote monitoring, as an additional facet of health care delivery.

Health care providers are reaching across regional and national borders using technology to provide medical services directly to patients and other providers. This includes email, interactive video, apps, and other technology platforms that facilitate diagnosis, consultation, treatment, monitoring, and even medical research. Remote second opinions – whereby a health care provider is asked by either a clinician or a patient to verify a diagnosis or treatment from a distance – also have surged, particularly in the international medical sector.

While telehealth solutions continue to be regulated by a complicated patchwork of local and national regulations, some governmental agencies and jurisdictions have eased regulatory burdens for the duration of the pandemic. Yet, when the COVID-19 crisis has ended, the shift to virtual health will likely remain, particularly to the extent there is evidence that it provides high quality services, lowers health care costs, and increases access to care.

In this report, we explore the opportunities and potential legal hurdles for companies involved in telehealth and remote monitoring – addressing both the regulatory exceptions that exist now, and the risks that will endure.

Reimbursement, market access, and international expansion

Complex patchwork of international regulations obscures telehealth rules

Although the practice of medicine and other health professions is regulated across the globe, the practice of telehealth does not always fit within the traditional areas of law and regulation applicable to the medical profession. Requirements regarding data privacy, international data transfer, and confidentiality of medical records may complicate telehealth.

And where states and countries do regulate telehealth – which is a growing trend – such laws do not always mesh with the reality of how health care is provided, with the policies of third party payers, or with government regulation of pricing and reimbursement of health care. Telehealth regulations also may not address the circumstances in which a physician located and licensed in one state or country may market or render remote services to patients or providers in a different state or country. Also, within the European Union, where patients' rights related to cross-border health care between various EU Member States have long been recognized, the practicalities and reimbursement of cross-border telehealth often remain unclear and under development.

In the United States, as well as in countries across the European Union and the world, there has been a dramatic expansion in the use of virtual health services, primarily driven by the COVID-19 pandemic. This has included changes in where and how such services can be accessed, how and when they will be reimbursed by payers, and the licensure and other regulatory requirements that apply to them. Some of these changes are intended to be temporary to address COVID-19, but there is a general consensus that a full return to the "status quo" is unlikely given the positive experiences of both patients and providers.

The use of virtual health services is likely to continue growing, and to become a significant part of the health care delivery system in much of the world, particularly to the extent there is evidence that it provides high quality services, lowers health care costs, and increases access to care. As the reach of health care broadens with technology and globalization, and as the pandemic persists around the world, the use of virtual health services will be more important than ever.

Brooke Bumpers
Counsel, Washington, D.C.
brooke.bumpers@hoganlovells.com

Bill Ferreira
Partner, Washington, D.C.
william.ferreira@hoganlovells.com

Hein van den Bos
Partner, Amsterdam
hein.vandenbos@hoganlovells.com

Regulatory pathways

FDA "remarkably flexible" to increase telehealth-related technologies

The COVID-19 pandemic has made clear the need for telehealth and remote patient monitoring. These solutions are critical to ensure continuity of care while minimizing risk of exposure to both patients and health care providers as well as, to provide care for those patients who do not have ready access to health care resources.

The U.S. Food and Drug Administration's (FDA) regulatory paradigm for remote monitoring and telehealth devices has evolved considerably over the recent years and continues to develop in response to technological advancement allowing for improved communication protocols, miniaturization of sensors, and increasing computer power through smartphones. FDA regulates the digital health products, including software, used in telehealth and remote patient monitoring based on risk and the function performed by the applications, consistent with its regulatory paradigm for other medical devices.

First, for FDA to regulate a digital health product, the product must satisfy the definition of a medical device in that it is "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or affects the structure or any function of the body." Second, it must not be eligible for a statutory carve-out that would remove it from FDA's regulatory oversight. Such carve-outs exist for technology used in administrative support; technology used to maintain or encourage a healthy lifestyle (so-called "general wellness" products); electronic patient records, tools to transfer, store, convert formats, or display (but not analyze) laboratory and device data; and certain clinical decision support software. Furthermore, even if a product is considered a medical device, there are a number of agency policies in place where the agency has elected to exercise enforcement discretion and forego active regulation of digital health products.

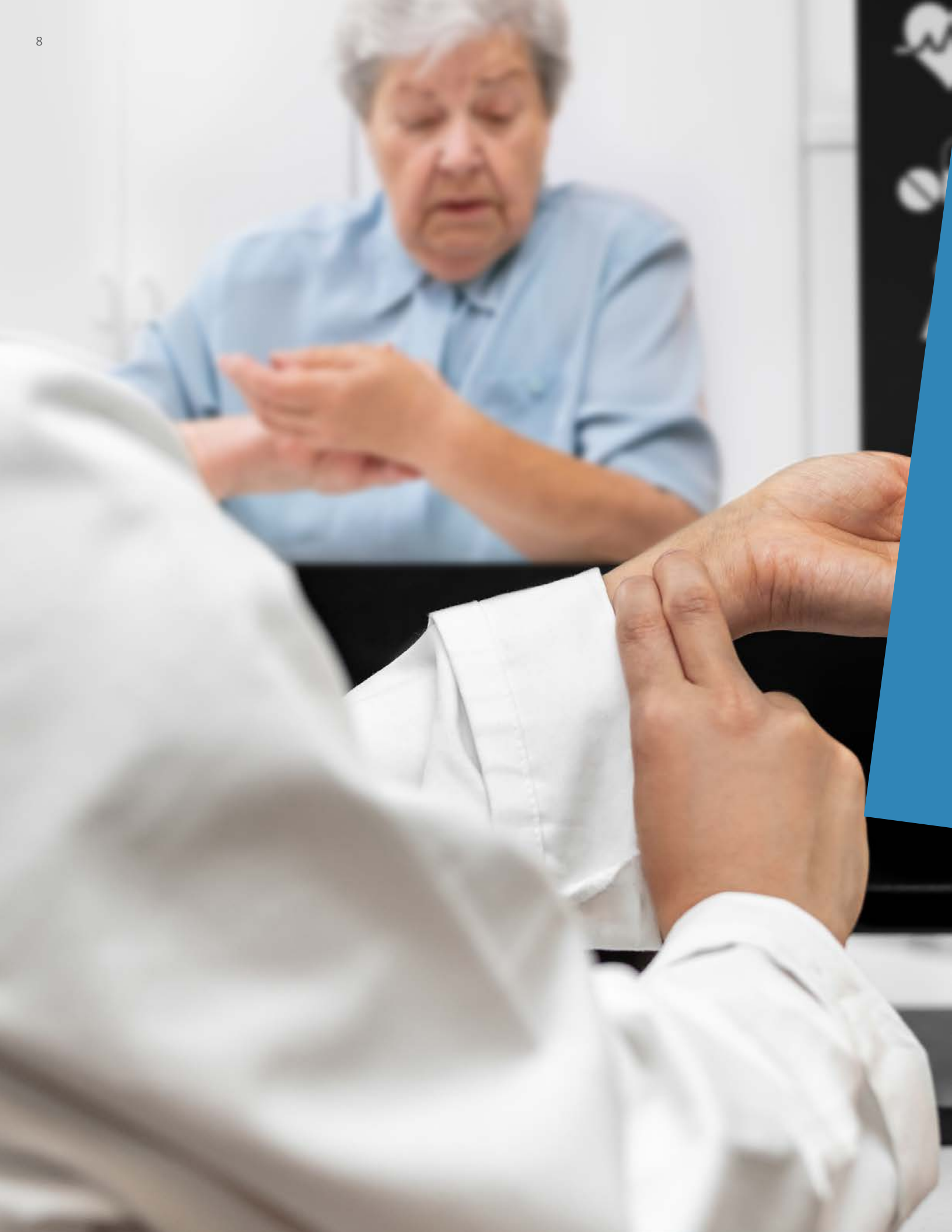
FDA has shown remarkable flexibility to increase the availability of remote monitoring and remote operation of devices to assist with health care during the COVID-19 pandemic. Specifically, FDA has allowed for modifications of existing devices to permit remote monitoring without the submission of a new marketing application, as well as for distribution of new and modified technologies under emergency use authorizations (EUA). These exemptions are only temporary, however, and in order for such technology to remain on the market once the emergency health declaration is lifted, companies will need to submit formal marketing applications to FDA for review.

We expect the demand for telehealth to continue to increase as companies and health care entities develop new best practices and technologies to ensure patients have continued and improved access to health care, even when remote, and also realize the efficiencies that telehealth can offer. Additionally, as patients develop comfort with the technologies and realize the time savings that can be achieved, there will be greater reliance on them to deliver care under normal circumstances. In all probability, the new technologies are here to stay, and may well be part of the evolution into a new normal for the delivery of patient care.

FDA will maintain oversight of such technologies, expanding the body of technology in this area under its regulatory jurisdiction. Given the critical demand for innovation in this area that has been demonstrated, it is possible that the agency will find other new and creative ways to regulate this technology through methods that continue to encourage its use and development.

Lina Kontos
Partner, Washington, D.C.
lina.kontos@hoganlovells.com

Jodi Scott
Partner, Denver
jodi.scott@hoganlovells.com



EU regulations shift software classification rules

Together with vaccines, facemasks, and respirators, medical software has an important role to play in the fight against COVID-19. Software can be used in various different ways: to support clinical decisions, provide medical resources, track COVID-19 patients, help in the management of patients, or in diagnosis. Some of these software solutions fall within the definition of a medical device in the EU and must bear a CE mark prior to marketing and use. Depending on type of software and the legislation against which the verification of conformity is conducted, obtaining a CE mark can be a long and challenging process. This process will become even more challenging under the new EU regulatory framework for medical devices.

The EU legislation applicable to these medical device software includes the Medical Devices Directive 93/42/EEC and the In Vitro Diagnostic Medical Devices Directive 98/79/EC. Both Directives will soon be replaced by Medical Devices Regulation 2017/745 (from 26 May 2021) and the In Vitro Diagnostic Medical Devices Regulation 2017/746 (From 26 May 2022). Both Regulations will substantially change the requirements applicable to software regulated as medical devices in the EU, bringing:

- New classification rules;
- New conformity assessment involving, in the majority of cases, a notified body;
- Increased clinical/performance data requirements;
- Longer timeframe to access the market; and
- Increased surveillance by notified bodies and competent authorities.

Medical device software manufacturers must prepare now to be ready for these new Regulations.

Fabien Roy
Partner, Brussels
fabien.roy@hoganlovells.com

Privacy and cybersecurity

HIPAA compliance rules eased during COVID-19 pandemic

Longstanding resistance to telehealth as a routine mechanism for providing health care has given way to innovative approaches to providing care remotely. With these new opportunities come privacy and security challenges, as health care providers work to maintain the confidentiality of traditional care settings, and technology companies work to develop platforms and create provider-patient experiences that support patient privacy. Existing privacy frameworks both support and challenge these innovations.

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) has issued various guidances on HIPAA compliance in the COVID-19 emergency, including guidance stating that it will exercise enforcement discretion for "good faith provision of telehealth" to provide emergency or routine care. This enforcement discretion – in effect for the duration of the emergency – makes clear that providers may use audio or video communication technology to provide telehealth to patients during the COVID-19 emergency, as long as those technologies are not public facing. This may include providing care to patients in home settings for COVID-19 or other health care services, but also may include communication and coordination between different health care providers. OCR lists several popular video chat applications covered by the enforcement discretion, as well as several public-facing tools that should not be used for providing telehealth.

Providers using – and tech companies offering – virtual health platforms need to assess how much privacy and security to build in and how to structure such arrangements. OCR encourages providers to tell patients about the privacy risks and to take advantage of any enhanced privacy and security modes available in these apps. OCR also offers suggestions for providers that seek additional privacy protections, including that they consider using technology vendors that are HIPAA compliant.

It's unclear whether this enforcement discretion will continue beyond the emergency period or what OCR's expectations will be for virtual health technologies in the long term. While many providers have successfully launched telehealth for crisis purposes, the next step will be to develop strategies for leveraging the value of technology while protecting the privacy and security of the data in a HIPAA-compliant manner, even after the pandemic ends.

Melissa Bianchi
Partner, Washington, D.C.
melissa.bianchi@hoganlovells.com

Regulation and impact of drug delivery systems in the EU

The COVID-19 pandemic has highlighted the growing complexity of drug delivery systems and the need for flexible products and procedures.

The increased sophistication of drug delivery systems means that the systems are not solely governed by medical device laws. The systems, particularly where these are used by patients at home, are often subject to remote monitoring. The data that is collected from patients and stored and shared with health care professionals falls within the definition of sensitive personal data provided in the General Data Protection Regulation (GDPR). As a result, development of drug delivery systems must take account not only of the regulations governing medicinal products and medical devices, but also necessary steps to ensure compliance with data privacy rules and respect and protection of patients' personal data.

The development, supply, and use of drug delivery systems must, therefore, comply with a number of different EU regulatory systems:

- The EU laws governing medicinal products to be delivered through the system;
- The EU laws governing the medical device element of the system;
- The EU data privacy rules governing protection of the patient data that is collected, stored, and processed through use of the system.

When, after demonstration of compliance with the obligations imposed by EU provisions, drug delivery systems are placed on the market in the EU, their supply and use are subject to the national laws of the individual EU Member States governing telemedicine and remote patient treatment. The related national laws of individual EU Member States vary. While some national authorities have embraced the concept of telemedicine others have provided to be more cautious with telemedicine continuing to be fairly unusual.

The COVID-19 pandemic has, however, highlighted the need for flexibility in supply of medicinal products outside the hospital setting and the challenges to which the need for related supervision can give rise. As a result, a number of EU Member States have introduced derogations from existing national rules governing drug supply which include flexibility of means of supply and increased use of telemedicine for supervision of patients by health care professionals. Some countries have underlined that these rules are temporary and intended only to address the issues to which COVID-19 has given rise. The benefits, particularly for patients with limited mobility or limited access to readily available health care may, however, result in these procedures becoming permanent.

EA Wright
Partner, Brussels
ea.wright@hoganlovells.com

Terms of use anticipate legal issues for telehealth products

Legal concerns of digital health solution providers are often addressed in Terms of Use ("ToU"), imposed on the patient and the respective health care professional (HCP) in addition to required privacy consent agreements. Common ToU clauses include:

- **Contracting with a minor:** The patient population may not only involve adults, but also minors. When contracting with a patient who is a minor, ToU often include clauses stipulating that the consent of parents has been obtained; however, such clauses are somewhat of a "grey area" in many EU jurisdictions, and they may not entirely mitigate the risk of contracting with a minor, and so other safeguards are advisable for these contracts.
- **Use of medicine-related data for research:** Telemedicine solutions have purposes aside from facilitating treatment; often health/treatment data is collected alongside pharmaceutical products. In some jurisdictions, gathering data relating to pharmaceutical products for research purposes might be deemed as a specifically regulated non-interventional study. This might trigger additional obligations on the part of the initiator of the service, such as obtaining the opinion of a medical ethics committee. ToU can tackle this issue by declaring the exact use of the data, its specific research purpose, and the manner of collection and use. In addition, the use of data for research may be regulated in several jurisdictions as a non-interventional study.
- **Right of revocation:** In many jurisdictions, patients/consumers must be informed about their right of revocation (also known as "right of withdrawal") in distance and off-premises contracts. This is the case when offering a digital health service over the internet or within an app store. Failure to inform about such rights entitles the patient/consumer to rescind from the use contract – even after having made use of the digital solution – with detrimental commercial and/or scientific effect for the solution's supplier.
- **Medical professional secrecy:** The medical professional secrecy of treating HCPs must be ensured while using digital health solutions. This is subject to professional codes, and civil and criminal laws.
- **Storing of consents and relevant version of ToU:** The circumstances relating to the conclusion of the ToU must be stored, as the provider must be able to assess at which time the respective user agreed to which version of the agreement.
- **Valid ToU amendments:** All amendments to the ToU must be implemented correctly in order to be valid. Requirements for the implementation of such amendments may differ in various EU countries.
- **Clear definition of scope of service:** Depending on how a company wishes to classify its telemedicine service from a regulatory standpoint, ToU need to be consistent with such classification and be explicit on the intended purpose of the service.
- **Availability of the digital service / dysfunctionality and respective liability aspects:** It is important to clearly point out in ToU that the physician alone is responsible for the treatment of the patient, and not the company offering the digital service. However, depending on how an app or service interacts with treatments, ToU may be used to inform patients on how to report any pharmacovigilance or medical device vigilance issues.

Mikael Salmela
Partner, Paris
mikael.salmela@hoganlovells.com

Dr. Jörg Schickert
Partner, Munich
joerg.schickert@hoganlovells.com

Commercial contracts

Contractual issues with telemedicine payer models

Contractual relations with payers will look critically different depending on the business model of a virtual health provider. Telemedicine companies in the post-COVID-19 world will need to consider whether they want services to be paid by patients, employers, or public payers (e.g., statutory health funds). If patients pay directly for telemedicine services, certain consumer protection legislation must be observed, such as: information obligations; consumer rights or restrictions on standard terms; and conditions in business-to-consumer relations. In contracts with public payers, meanwhile, certain public law requirements must be taken into account, such as certain restrictions on the type of entities that are permitted to provide and invoice telemedicine services.

Contracts with large companies that want to offer telemedicine services to their employees will also look different, and may bring cross-border problems. For example, an employer may want to offer telemedicine services for employees in different jurisdictions that have different regulatory landscapes. It is likely that varying business models will exist in parallel so that contractual relations to all kinds of payers may become relevant simultaneously.

Arne Thiermann
Partner, Hamburg
arne.thiermann@hoganlovells.com

Investment landscape

Soaring valuations, investor demand create partnership opportunities

The COVID-19 pandemic has created an unprecedented demand among consumers for telehealth services. For example, New York-based telehealth services provider Teladoc reported that visits nearly doubled to two million in the first quarter of 2020, leading the company to increase its annual revenue expectations by $100 million. This follows Teladoc's January announcement that it plans to acquire InTouch Health, a telehealth company that services the provider market, for $600 million.

Global venture capital funding in digital health companies, including private equity and corporate venture capital, set records in the first quarter of 2020. According to Mercom Capital Group and industry sources, digital health companies raised $3.6 billion in venture capital funding in Q1 2020, as compared to the $1.7 billion raised in Q1 2019. Telehealth, including telemedicine and remote monitoring, was the top funded category, with $930 million raised from 35 deals.

Anecdotally, we have seen valuations of telehealth technologies increase as shutdowns relating to the COVID-19 pandemic are likely to continue into the second half of 2020. In addition to high valuations, we're seeing high investor demand. However, some financial investors experience difficulties with cash calls from their LPs, so any emerging company needs to make sure that investors are actually able to fund them. Large pharmaceutical companies, however, have fewer funding issues, and as a result, their sector expertise and resources make them a prime target for companies seeking investment.

In recent weeks, regulators have been cutting red tape for telehealth start-ups, which are opening their services to larger groups of customers. As a result, telehealth start-ups cannot scale their operations fast enough, and they are experiencing problems growing their staff, software, and doctors to meet booming customer demand. One strategy to respond to these issues is contractual co-operation with bigger players – including health insurance companies, hospitals, pharmaceutical manufacturers, and technology companies – who can help with scaling, resources, and professionalizing processes.

We expect that investors will continue to seek out opportunities to take advantage of the explosion of activity in telehealth spurred by the COVID-19 pandemic. At the same time, emerging companies with telehealth capabilities will be faced with strategic questions about the best path forward for growing their business: whether that is through venture capital financing, partnerships with other industry players, mergers and acquisitions, or other alternatives.

Peter Huber
Partner, Munich
peter.huber@hoganlovells.com

Adriana Tibbitts
Partner, Baltimore
adriana.tibbitts@hoganlovells.com

Liability

Exceptions to telehealth liability concerns

Liability risks for telehealth services range from contractual and regulatory liability to claims for medical malpractice and compliance with professional rules. Where digital health applications are part of the offering, product liability concerns come into play, as well as potential liability for cyber vulnerabilities and data breaches, which have increased since the start of the global pandemic.

With COVID-19, however, special legal protections could apply in some instances. In the United States, there is at least some limited protection under the PREP Act for liability associated with administration or use of a drug, device, or diagnostic (as defined by the FDA) related to the treatment of COVID-19 when FDA has issued a specific Emergency Use Authorization for products for such uses. We see the PREP Act potentially applying to telehealth services involving diagnostic tests, prescription drugs, or other treatments. However, the PREP Act does not apply to claims brought by the U.S., which includes federal False Claims Act claims, or claims based on willful misconduct that leads to serious physical injury or death. The PREP Act also would not cover consumer protection- related liability stemming from medical- based claims or advertising; these liability risks remain for telehealth practitioners and manufacturers of remote diagnostic tools.

Likewise, regarding practice of medicine claims, many states have granted interstate licensing exceptions through their declarations of liability for practicing clinicians from other states and for retired clinicians.

There is no EU counterpart to the U.S. PREP Act applying to telehealth services. It is up to the member states and their national COVID-19 legislation to implement exceptions and protections as appropriate. Yet, as telehealth is a powerful tool to help maintain physical distance, it is likely that we are going to see further legislative efforts concerning telehealth services across Europe.

Eventually, the temporary relaxation of liability rules – including the PREP Act protection and licensing exceptions – will expire, but the telehealth landscape will have already changed. The question remains whether licensing requirements for physicians will keep pace.

Emily Lyons
Senior Associate*, Washington, D.C.
emily.lyons@hoganlovells.com

Stefan Mayr
Associate, Munich
stefan.mayr@hoganlovells.com

Matthias Schweiger
Partner, Munich
matthias.schweiger@hoganlovells.com

Peter Spivack
Partner, Washington, D.C.
peter.spivack@hoganlovells.com


TELEHEALTH

The pharmaceutical perspective

Pharma's push into virtual health creates new legal challenges

With patients quarantined in their homes, we're seeing pharmaceutical manufacturers accelerating their efforts to connect patients to telehealth providers. For example, a growing number of drug makers are providing direct links on product websites that give patients the option to "connect with a doctor now" through a virtual online visit. Others are using telehealth technology to deliver remote nurse education and training to patients in their homes. These have been responses to the COVID-19 emergency, but reflect a trend that is likely to continue after the crisis has passed.

Similarly, developments in artificial intelligence have led to new diagnostic tools that manufacturers are eager to make available to patients who would benefit from their therapies. Remote monitoring and mobile apps are increasingly being explored as ways to promote greater adherence to therapy or to make access to medicines easier and more convenient for patients.

Along with their potential benefits, these technologies bring new legal challenges for manufacturers. In particular, while patients may be increasingly comfortable obtaining health care virtually, manufacturers must be careful not to step too far into medical decision-making. The proper role and independence of health care professionals still must be preserved, and patient health information must be properly handled. In addition, financial arrangements need to be carefully structured to avoid any concerns that the manufacturer is creating unlawful inducements for the use of its products, and communications with patients about these services or tools in the context of a particular product need to be evaluated under FDA's promotional rules.

Careful consideration of the fraud and abuse laws, FDA regulations, privacy law, state licensure requirements, payer coverage rules, and product liability risk are essential for any manufacturer looking to use virtual health technology to promote greater access to its therapies.

Susan Lee
Partner, Washington, D.C.
susan.lee@hoganlovells.com

Ron Wisor
Partner, Washington, D.C.
ron.wisor@hoganlovells.com

Don't forget about patents

The interplay of U.S. patents and telemedicine innovation

When considering patent issues regarding telemedicine, the aspect which has arguably received the most attention is patent eligibility. Following the U.S. Supreme Court's decision in Alice, and in light of the U.S. Patent & Trademark Office's more recent pro-eligibility revisions to its patentability guidelines, it would be prudent for those operating in the telemedicine industry to consider whether their innovations are, in fact, patent eligible and whether they could provide a strategic and competitive advantage for its products and services. For example, telemedicine's incorporation of AI may now be viewed as an essential part of the telemedicine model, but attaining commercially important patented AI that enables the telemedicine provider to differentiate itself from others could help drive growth and profitability.

In addition to an in-depth post-Alice decision analysis of patent eligibility, whether AI related or otherwise, careful consideration should also be given to how patent claims are drafted to maximize the patentees' ability to meet its infringement proofs if asserted. Poor, low quality, claim drafting can often weaken patents and make infringement proofs needlessly problematic. Identifying such claims may be helpful in situations whereby post-grant procedures before the U.S. Patent & Trademark Office can be employed to amend claims to mitigate such problems. To the extent commercially valuable subject matter is not patentable, the innovator should carefully consider what alternative IP protection may be available, including the use of applicable trade secret, trademark, trade dress, and copyright laws.

While we've witnessed courts in the U.S. strike down as unpatentable patents that broadly covered the abstract idea of telemedicine, the industry should be aware that more narrowly-tailored and less abstract innovations have received patent protection that may be less susceptible to such validity challenges. Although telemedicine has tremendous public importance, particularly during this COVID-19 pandemic, the current legal landscape in the U.S. does not provide telemedicine providers with a free license to infringe patents. Only last month a telemedicine dental provider claiming to be the "creator of the first direct-to-consumer medtech platform for teeth straightening" filed a patent infringement suit against a competitor provider. The suit included claims covering aspects of a telemedicine dentistry model for straightening teeth.

Furthermore, there is concern that non-practicing entities (sometimes called patent "trolls") will attempt to take advantage of the increased use of telemedicine and so destabilize the increased availability and progress made by telemedicine due to COVID-19. We have witnessed the beginnings of such actions in the form of a non-practicing entity, Neodron, having filed two complaints at the U.S. International Trade Commission seeking exclusion orders to prohibit the importation of certain touch screen technology on mobile devices that is often used by telemedicine patients. As a consequence, it may be prudent to involve outside patent litigation counsel early, as telemedicine technology is implemented, to provide real-time advice with respect to freedom to operate and be prepared to defend against patent infringement actions should they come.

Simon Roberts
Partner, New York
simon.roberts@hoganlovells.com

Intellectual property protection considerations for telemedicine platforms

The demand for telemedicine platforms in the past several years, and particularly now, has spurred myriad innovations and features that software developers may want to protect to stand out in the marketplace. Having a balanced intellectual property portfolio including not only patents, but copyright and trade secret protection, may provide the most comprehensive protection for telemedicine platform innovation.

Patent protection is one of the strongest and most comprehensive ways of protecting the functionality of software innovation. For example, utility patents may protect innovations on a server or data infrastructure that implements the telemedicine platform, or a new, more-efficient method or process for organizing and recalling data stored remotely. Alternatively, design patents may protect the layout, or graphical user interface (GUI) of the client-facing side of a telemedicine platform. Design patents may be leveraged to protect the overall look of a platform, or can be employed to protect particularly distinctive aesthetic features or aspects of a platform. Patent protection, even if narrow in terms of its coverage, may be a valuable asset, particularly when a unique feature or innovation that is protected becomes a market identifier for that specific platform, or when the presence of patent protection can act as a deterrant from unauthorized copying or promote investment.

Copyright protection may also be employed on its own or in tandem with patent protection for telemedicine software platforms. Copyright can protect not only the look of the layout of a platform or a website, but can also protect underlying computer software code from verbatim or very close copying. Copyright protection is narrower than patent protection (as it protects only the expression of an idea, e.g., computer code, not the idea or functionality/process itself). Copyright is less expensive to obtain than patent protection and may be easier to enforce than patents where there is actual unauthorized copying. Copyrights may also be employed to protect the software code itself when patent protection on the overall functionality is otherwise unavailable.

Trade secrets may also play a role in protecting innovation in telemedicine platforms. Trade secrets may protect customer lists, marketing strategies, and business processes that are valuable to a business and that have been kept secret. Trade secrets, in certain circumstances, may also be used to protect software and code implementing telemedicine platforms. The benefits of trade secrets are, of course, that the disclosure of an innovation (such as by writing up in a patent) is not required to obtain protection, and protection can last as long as the information remains secret. Businesses considering trade secret protection must be able to adequately identify their trade secrets, and implement policies and protocols to protect trade secrets from disclosure. Entities engaged in telemedicine should make sure they have or update their trade secret policies and take tally of their key trade secrets.

Ultimately, the types of IP protection a business employs depends on the nature of the business and the innovations it is seeking to protect. However, knowing what types of protection may be available to telemedicine platforms and in the industry may ultimately help businesses find the most effective IP protection for their innovations.

Kristin Connarn
Partner, Boston
kristin.connarn@hoganlovells.com

Celine Crowson
Partner, Washington, D.C.
celine.crowson@hoganlovells.com

Leading the way in Digital Health

Technology is changing the way the health care industry operates. With changes come new challenges and opportunities – as well as a dramatic shift in the competitive and regulatory landscape. We bring a real-world sensibility to your challenges, helping you to remain competitive and compliant everywhere you operate.

The challenges ahead

Technological innovation is changing the way that health information is collected, used, and consumed. As a result, the way in which drugs and devices are developed, approved, reimbursed, and marketed, and the way health care services are ultimately delivered is changing dramatically as well.

The untapped business potential is tremendous. At the same time, there are new and complex technological, business, legal, and data protection issues which create uncertainty and ambiguity because they cannot be addressed within the borders of our traditional areas of law and local regulation.

We bring a holistic approach

Our cross-jurisdictional team of more than 50 life sciences and health care lawyers with a focus on digital health take a technology-based approach to counseling on digital health products and services. We provide you with strategic guidance on how to leverage opportunities for growth, minimize legal barriers, comply with rules, protect your data, and realize its value.

How we can help

Our team advises on the design, approval process, and regulation of digital health products. We also regularly work with companies and health care providers on pricing and reimbursement frameworks. We advise on all aspects of health privacy and cybersecurity including breach response, risk assessment, privacy policies, and transactions.

We help navigate collaborative arrangements such as commercial joint ventures and research studies and provide full commercial and corporate support for transactions. We advise across the full spectrum of deal aspects including intellectual property rights, licensing, data exploitation, and risk.

We also regularly counsel on risk mitigation strategies for liability, providing preventative strategies for product liability, professional liability and negligence, as well as helping you step by step should new liabilities arise.

Areas of focus

- Clinical trials
- Commercial transactions
- Coverage and reimbursement
- Intellectual property
- Interaction with health care providers
- Medical device regulation
- Pharmaceutical regulation
- Privacy and data security
- Product and professional liability
- Telemedicine
- Wireless communications

50+

lawyers from ten countries participate in our Digital Health team.

Get in touch

Melissa Bianchi
Partner, Washington, D.C.
melissa.bianchi@hoganlovells.com

Matthias Schweiger
Partner, Munich
matthias.schweiger@hoganlovells.com

Jodi Scott
Partner, Denver
jodi.scott@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

Associated offices*
Legal Services Center: Berlin

www.hoganlovells.com