Tech™
REG
CHRONICLE

CONNECTED HEALTHCARE

SEPTEMBER 2022

CPI COMPETITION POLICY™ INTERNATIONAL

Competition Policy International, a What's Next Media and Analytics Company

TechREG EDITORIAL TEAM

TechREG EDITORIAL BOARD

CPI COMPETITION POLICY™ INTERNATIONAL

LETTER FROM THE EDITOR

Dear Readers,

This edition of the CPI TechREG Chronicle concerns "Connected Healthcare" – namely how developments in technology and communications can facilitate the provision of key healthcare services to consumers. While connected healthcare services doubtless provide numerous benefits to patients and healthcare providers, they can also raise numerous regulatory challenges, as the authors of the pieces in this Chronicle set out.

Silvana Togneri MacMahon & Ita Richardson open by providing a satellite view of how technology is changing the provision of healthcare. The authors present a definition of Connected Health, consisting of five components: Technology, Healthcare Pathways, People, Regulation and Data. Naturally, the article focuses on regulation - presenting the importance of recognizing how Connected Health solutions, given that they are Medical Devices in many cases, must be regulated.

Amy Durbin notes how the COVID-19 pandemic further ushered in an unprecedented era of change within the healthcare industry, particularly for telehealth. While pre-pandemic telehealth policy at the state and federal level often focused around payer reimbursement policies, attention during the pandemic has focused on state licensing and prescribing compliance across state lines. The article discusses ever-complicated and evolving medical privacy laws, as well as remaining broadband infrastructure and digital barriers.

Carol K. Lucas & Jennifer M. Guerrero discuss how

U.S. health care providers are heavily regulated by an overlapping patchwork of laws, including fifty different sets of state laws. Technology has outrun the legal framework as providers seek to establish a digital healthcare practice. This complex web of overlapping and sometimes inconsistent laws makes establishing a multi-state medical practice challenging.

Turning to consumer technology, **David Voran** discusses issues surrounding Apple's Health App, which is a pre-installed app on all iPhones. In essence, the app is a localized personal health tracker. It aggregates fitness and health related information from a growing number of applications and devices. Since 2018, the Health app has been able to download data from a patient's health-system medical records using the persons active patient portal as validation and conduit. Later upgrades enable the user to select items in the Health app to share with their physicians. This functionality opens many clinical, regulatory, financial, and management questions.

Heinz Joerg Schwarz discusses how modern workflows that support interactive patient functionality and remote patient monitoring can be integrated with certain legacy infrastructure prevalent in many healthcare organizations. As the article notes, it is possible to seamlessly bridge between the two worlds and accomplish the goals of modern healthcare systems without a need to rip-and-replace reliable and scalable extant infrastructure. However, decisionmakers need to be mindful that connected healthcare today reaches beyond connecting systems inside a hospital system: it involves also connecting with the patient and a wider social community to accomplish better health outcomes.

Turning to specific aspects of patent law, **Carl Kukkonen, Patricia Campbell & Gurneet Singh** discuss drug discovery and artificial intelligence. In the pharmaceutical and biopharmaceutical industries, taking a drug to market is a quite often a tedious process. For example, to create a drug, scientists first predict one or more combinations of molecules that can be transformed into a drug. Next, scientists perform experiments on each molecular combination to test for efficacy. AI can greatly expedite this process, but the use of AI (rather than a traditional scientist or inventor) raises intriguing questions as to the patentability of drugs.

Finally, **Gabriëlle Speijer & Peter Walgemoed** discuss how patients and healthcare professionals need to take the lead in determining how technology is used to serve human values and needs. All stakeholders contributing to health and care should follow the same value: the Hippocratic Oath. A mindset focused on return on data instead of return on investment is needed to exploit the anti-rival nature of data and their value for society.

As always, many thanks to our great panel of authors.

Sincerely,
CPI Team

TABLE OF CONTENTS

CPI COMPETITION POLICY™ INTERNATIONAL

CONNECTED HEALTHCARE

SEPTEMBER 2022

SUMMARIES

REGULATING CONNECTED HEALTH: PATHWAYS, TECHNOLOGY AND THE PATIENT

By Silvana Togneri MacMahon & Ita Richardson

In this paper, we discuss how technology is changing the world around us, particularly focusing on how the introduction of Connected Health solutions can continue providing patient-centered care. We present a definition of Connected Health, which includes five components - Technology, Healthcare Pathways, People, Regulation and Data. Our article focuses on just one of these – that of regulation - presenting the importance of recognizing how Connected Health solutions, given that they are Medical Devices in many cases, must be regulated. We summarize different regulations, discussing how they should be included as a requirement when designing and developing, implementing, and using a connected health solution. Although not specifically focused on Medical Devices, we include some information on the European Union Accessibility Directive. Our conclusion focuses on the need for developers and end users to understand the importance of regulation when designing and developing health solutions.

TRAPS FOR THE UNWARY TELEHEALTH PROVIDER

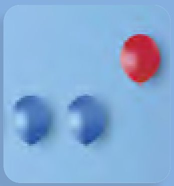
By Carol K. Lucas & Jennifer M. Guerrero

The provision of health care services via telemedicine has been growing in popularity over the last several years. With the arrival of the COVID-19 pandemic, healthcare providers were able to rely on a variety of temporary waivers, executive orders, enforcement discretion and regulations that made the transition to digital healthcare technologies simpler than it had been in earlier times. The use of digital healthcare technologies is now deeply embedded into healthcare services and will continue despite the expiration of the regulatory flexibility afforded by the public health emergency. It is important to remember, though, that health care is largely regulated on a state-by-state basis, and a business structure or payment arrangement that is legal in one state may not readily translate to another state. As the present PHE begins to wind down, providers need to be prepared to face the additional legal and regulatory issues combined with the heightened attention of federal and state authorities to services delivered via telehealth. This article provides an overview of the legislative and regulatory challenges related to the implementation of digital healthcare delivery systems in the United States.

WHAT'S AHEAD FOR CONNECTED HEALTH POLICY: STATE & FEDERAL POLICIES IMPACTING TELEHEALTH ACCESS, PRIVACY LAWS & POLICYMAKER INTERESTS

By Amy Durbin

The COVID-19 pandemic further ushered in an unprecedented era of change within the healthcare industry, particularly for telehealth. While telehealth, medical privacy, and broadband issues are not new to the regulatory environment, pandemic policies have allowed healthcare to become even more connected, raising more questions than ever related to what exists and what's ahead for state and federal telehealth policies. While pre-pandemic telehealth policy at the state and federal level often focused around payer reimbursement policies, attention during the pandemic has lasered in on state licensing and prescribing compliance across state lines. Meanwhile, as providers have ramped up technology implementation in their practices to better utilize telehealth in a relaxed COVID-19 regulatory environment, this article will look at ever-complicated and evolving medical privacy laws, as well as remaining broadband infrastructure and digital barriers. Planned post-public health emergency (PHE) telehealth policies and areas of interest for policymakers contemplating long-term connected health policies are also highlighted in terms of the future of connected health policy.



APPLE HEALTH'S APPROACH TO PATIENT SELF-REPORTED DATA – A GAME CHANGER OR JUST MORE NOISE?

By David Voran

Apple's Health App, a native app on all iPhones, is a localized personal health record aggregating tracking, fitness, and health related information from a growing number of applications and devices. Since 2018 with the release of iOS 10, the Health app has been able to download data from a patient's health-system medical records using the persons active patient portal as validation and conduit. The iOS 15.x upgrade now enables the patient to select items in the Health app to share with their physicians. Physicians are then able to open an Apple Designed and maintained Physician Dashboard in their electronic record. This functionality opens many clinical, regulatory, financial, and management questions.

CONNECTING THE MODERN WORLD OF APIS TO LEGACY HEALTHCARE INFRASTRUCTURE

By Heinz Joerg Schwarz

This article discusses how modern workflows that support interactive patient functionality and remote patient monitoring can be integrated with the legacy infrastructure prevalent in many healthcare organizations. While the legacy world is utilizing the HL7 v2 standard, modern applications require HL7 FHIR. However, it is possible to seamlessly bridge between the two worlds and accomplish the goals of modern healthcare systems without a need to rip-and-replace reliable and scalable extant infrastructure. Connected Healthcare nowadays reaches far beyond connecting systems inside a hospital or between professional care providers, it involves also connecting with the patient and a wider social community to accomplish better prevention and health outcomes.

PATENT LAW CONSIDERATIONS FOR DRUG DISCOVERY INNOVATIONS UTILIZING ARTIFICIAL INTELLIGENCE

By Carl Kukkonen, Patricia Campbell & Gurneet Singh

Taking a drug to market is a complex process that involves prediction of one or more combinations of molecules that can be transformed into a drug, and performance of experiments on each molecular combination to test for efficacy, stability, safety, and other metrics. This road of trial-and-error experimenting with different molecular combinations can take many years, and cost billions of dollars. Artificial intelligence ("AI") tools can substantially reduce the time of trial-and-error experimenting with molecules by trimming the molecules that are not ideal based on historical data. This quickens the process and reduces the investment for finding effective, stable, and safe molecular combinations that can be developed into a drug. This article elaborates on the confluence of drug discovery and AI, some industry partnerships between pharmaceutical and AI companies, implications of pharma-AI confluence for patent law, and various recommendations for protecting technological aspects of the pharma-AI confluence.

TOWARD A SUSTAINABLE HEALTH ECOSYSTEM FIXED ON THE DEEPEST PROFESSIONAL VALUES

By Gabriëlle Speijer & Peter Walgemoed

Patients and healthcare professional need to take the lead in technology as digital starts with human values and human needs. It's crucial that they organize together and don't leave it to the other stakeholders, like tech industry or government. All these stakeholders contributing to health and care should follow the same value: the Hippocratic Oath. Nowadays it's getting harder to uphold this oath lacking the orchestration principles for our human values in IT&C design globally. A mindset focused on return on data instead of return on investment is needed to exploit the anti-rival nature of data and their value for society. Concretizing the vision of Nobel prize winner Elinor Ostrom by organizing cooperatives in specific roles with a shared long-term mission, applying all IT&C principles described in our article lays the foundation for a sustainable health ecosystem that's yielding curated data and embeds the anti-trust law and legislation. It brings in the maximum potential of everyone's qualities and insights, continuously. Performing on top of licence realizing breakthroughs. For many more people and our future generations to learn and create wisdom on it, exponentially.

REGULATING CONNECTED HEALTH: **PATHWAYS, TECHNOLOGY AND THE PATIENT**

BY
SILVANA TOGNERI MACMAHON

&
ITA RICHARDSON

Lero – the Science Foundation Ireland Research Centre for Software, Ireland; School of Computing, Dublin City University, Dublin; Department of Computer Science and Information Systems, University of Limerick, Limerick.

01 INTRODUCTION - CONNECTED: A CHANGING WORLD

Through the use of technology, consisting of hardware and software, the world around us is changing dramatically. It is not unusual in many of our everyday environments to use smart phones, internet, mobile technology, integrated software systems and ubiquitous computing.

How has the advent of technological connectedness changed our everyday lives? Air travel has changed – one can now reach the airport security checks without ever having to interact with a person. Retail has changed – consumers can shop (and auction) online, use personal avatars to visualise how clothes would look, pay using credit cards and track their deliveries. Education has evolved. Students have access to information via the internet. Technology allows students to interact with international peers, working on team projects through discussion via e-mail, skype and similar systems.

And what of healthcare? This is also going through an evolution where healthcare is becoming increasingly computerised. This evolution is happening within hospitals and in the community. Technology is being used by people who are well and those who are ill. However, regardless of technology used, it is important that, within the medical domain, the patient will continue to be the most important consideration. *Healthcare pathways* propose the process for the efficient delivery of care to the patient, and there is a need for this to result in quality outcomes for the patient, and to do this, *patient-centred care* must be provided.[2] In some cases, the traditional healthcare pathway or sections of it will continue to be followed. But, introducing Connected Health solutions will often require it to change. For example, a surgeon will continue to carry out operations, but we see that sections of the traditional pathway can be replaced. For example, robots carry out surgery, while being are controlled by surgeons through computerisation.[3] This combination of the traditional with the technological pathway requires well-defined healthcare pathways, ensuring that each person linked to the pathway understands all roles within that pathway.

> ***How has the advent of technological connectedness changed our everyday lives? Air travel has changed – one can now reach the airport security checks without ever having to interact with a person***

Following the healthcare pathway can be carried out by one or all of the groupings – *healthcare professionals, patients and/or carers*. There may be a Connected Health system where the healthcare professional is required, such as when medicine needs to be prescribed. There are others, where that professional input is not required, as their knowledge has been included in a decision support system. An example of this would be when a patient monitors physiological symptoms, the decision support system can automatically track inputs, and highlight deviations directly to the patient. Once this has been highlighted, the patient can then make a decision to involve the healthcare professional if they so wish. For this healthcare to be "connected," it must be supported by *technology*.

Using technology is what allows significant changes to be made to the healthcare pathway. And, there is an external stakeholder who must be considered – *regulation*. In many countries, software and hardware used as Medical Devices have to be regulated before they can be marketed. Our particular interest is in regulation within the European Union ("EU"), which is similar to other countries such as the U.S. Depending on the safety classification of the product, different regulations apply. In addition, in providing care, there is an increased need for data to be shared between patients and care providers, within and beyond the traditional healthcare setting and often across borders. Data must be shared appropriately ensuring that the dual goals of privacy and accessibility are met.

Health professionals are making increasing use of technology to monitor, diagnose, prescribe, maintain patient records, and generally enhance their healthcare practice. This use of technology within healthcare is now commonly known as Connected Health (see Figure 1) which we define as:

Connected Health is where patient-centred care results from following defined healthcare pathways undertaken by healthcare professionals, patients and/or carers who are supported by the use of technology (software and/or hardware), regulated when used as a Medical Device, and facilitating appropriate health data sharing.

[2] Noel Carroll, Catriona Kennedy & Ita Richardson, "Challenges towards a Connected Community Healthcare Ecosystem (CCHE) for Managing Long-Term Conditions," *Gerontechnology*, 14.2 (2016), 64–77 https://doi.org/10.4017/gt.2016.14.2.003.00.

[3] Christina A. Fleming and others, "A Review of Clinical and Oncological Outcomes Following the Introduction of the First Robotic Colorectal Surgery Programme to a University Teaching Hospital in Ireland Using a Dual Console Training Platform," *Journal of Robotic Surgery*, 14.6 (2020), 889–96 https://doi.org/10.1007/s11701-020-01073-8.

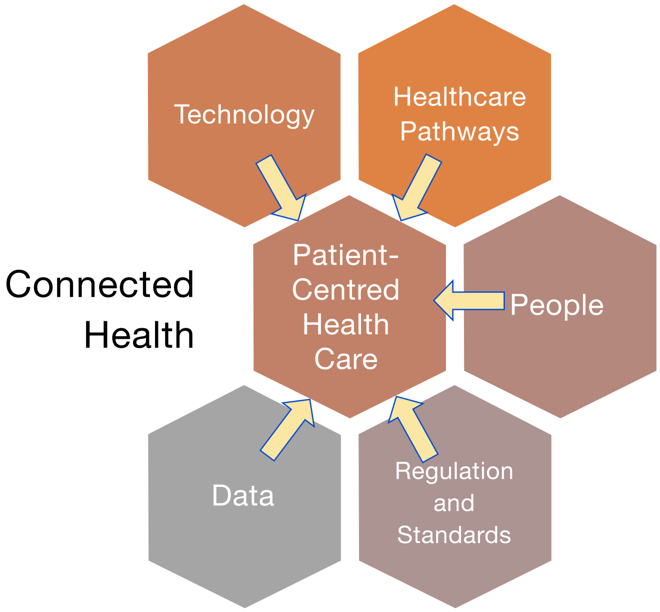


Figure 1 – Connected Health components provide Patient-Centred Health Care

For Connected Health to be implemented successfully and efficiently, each of these five components (Technology, Healthcare Pathways, People, Regulation, and Data) must work together. Therefore, it is incumbent on healthcare professionals, patients, carers (formal and informal), and technologists to develop solutions together. And for solutions to work, processes have to be defined within the Healthcare Pathways. Connected Health solutions have the ability to improve care for the patient – but to do this, all components need to be included. In this article, we focus on regulation (and standards), as it is important to consider these. This discussion of regulation that follows is not intended to be exhaustive but indicative of the considerations of manufacturers and healthcare delivery organisations implementing Connected Health systems.

> *Using technology is what allows significant changes to be made to the healthcare pathway.*

02 WHAT ARE THE DOMAIN SPECIFIC/ DEFINING FEATURES OF THE REGULATION OF CONNECTED HEALTH?

In order to understand the impact of regulations on Connected Health, we focus on the impact of regulation on Medical Device technology. Medical Devices must comply with the regulations of the geographical location in which the device is to be marketed. These devices are often systems of systems and are composed of, for example, hardware, software, networks, interfaces to other systems, Medical Devices and data. They are strictly regulated before they can be placed on the market to ensure their safety. While many Medical Devices were originally designed to be standalone, but ultimately, it was recognised that Medical Devices could be used more efficiently if they were connected to a network so that information could be passed between devices and other systems.

Therefore, when a Medical Device was designed to be connected to a network, generally the manufacturer would supply and control the network. This limited the "connectedness" of the device but was done so that the regulated Medical Device was part of a manufacturer-controlled system. This meant that manufacturer could ensure that the placing of the device onto the network did change the device in any way from the regulated version, thus not compromising the safety of the device. However, there has been an increased requirement for the integration of software and hardware systems, thus removing the possibility of continued use of manufacturer-controlled systems. This means that regulation must not only be considered during design and development of Medical Devices, but also during the integration of devices when implementing them for use.

Today's sophisticated Connected Health systems provide advanced levels of decision support and integrate patient data between systems, across organizational lines, and across the continuum of care. In addition to these benefits, there is also increased likelihood of software-induced adverse events.[4,5] The organizations involved in developing, implementing and operating the many connected health components and services in order to support patient–centred care must ensure that three key properties are preserved across the lifecycle of the system – Safety, Effectiveness and Security.[6]

Safety is defined as "freedom from unacceptable risk of physical injury or damage to the health of people or damage to property or the environment." Effectiveness is defined as "the ability to produce the intended result for the patient and the responsible organisation." In this case, the responsible organisation is the organisation developing, implementing and operating the system. Security is defined as "an operational state of a medical information technology network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability." In order to preserve these properties, the organisation must consider the use of the Connected Health technology in the context of the Medical Device regulation. It should be noted also that there is an interdependence between these three properties. For example, exercising a security vulnerability within a Medical Device could ultimately compromise the safety and therefore, the effectiveness of the device. As such, all three properties must be addressed together.

03

HEALTHCARE SYSTEM REGULATIONS – REGULATIONS AND STANDARDS FOR CONNECTED HEALTH

To understand the interplay of regulations and standards for Connected Health, we need to consider the lifecycle for the development of Health Information Technology (Health IT lifecycle).

The Health IT lifecycle is broken down into three broad phases[7]: Design and Development, Implementation and Clinical Use. Different standards and regulations apply to different phases of this lifecycle.

During the *Design and Development phase* Medical Devices that are designed to be marketed in the EU must comply with Regulation 2017/745 on Medical Devices ("MDR") and Regulation 2017/746 on In-Vitro Diagnostic Devices ("IVDR"). The MDR became fully applicable on 26 May 2021 and the IVDR became fully applicable on 26 May 2022, after a five-year transition period. The MDR and IVDR represent a significant development and strengthening of the existing regulatory system for Medical Devices in Europe and the legislation now being in the form of a Regulation, rather than a Directive, means that the EU law is directly applicable at national level. Thus there is no longer a requirement for transposition through specific national legislation which should prevent variation in the approach taken. These regulations also apply to other phases of the lifecycle.

[4] Silvana Togneri MacMahon, Fergal McCaffery & Frank Keenan, "Development of the MedITNet Assessment Method - Enabling Healthcare Delivery Organisation Self Assessment against IEC 80001-1," in *First International Conference on Fundamentals and Advances in Software Systems Integration (FASSI 2015)*, ed. by Chris Ireland and Petre Dini (Venice, Italy: IARIA, 2015) https://doi.org/ISBN: 978-1-61208-448-0.

[5] S.T. MacMahon, F. McCaffery & F. Keenan, "Development and Validation of the MedITNet Assessment Framework: Improving Risk Management of Medical IT Networks," in *ACM International Conference Proceeding Series*, 2015, xxiv-xxvi-Augu https://doi.org/10.1145/2785592.2785599.reduced costs of care and a reduction in adverse events. Traditionally, medical devices were placed onto a proprietary IT network provided by the manufacturer of the device. Today, medical devices are increasingly designed for incorporation into a hospital's general IT network enabling devices to exchange critical information. However, this can introduce risks and negate the potential benefits to patients. While the IEC 80001-1 standard has been developed to aid Healthcare Delivery Organisations (HDOs).

[6] IEC, "IEC 80001-1 - Application of Risk Management for IT-Networks Incorporating Medical Devices - Part 1: Roles, Responsibilities and Activities" (Geneva, Switzerland: International Electrotechnical Commission, 2010).

[7] ISO, *ISO 81001-1: Health Software and Health IT Systems Safety, Effectiveness and Security — Part 1: Principles and Concepts* (Geneva, Switzerland, 2021).

The EU also states that for the new regulation that "Compliance with a harmonised standard confers a presumption of conformity with the corresponding essential requirements set out in Union harmonisation legislation from the date of publication of the reference of such standard in the Official Journal of the European Union."[8] This means that manufacturers that comply with the requirements of the recognised standards can also claim conformity to the regulations. To date, 14 standards have been recognised and it is expected that the Commission will issue further implementing decisions to add to the list of Harmonised standards later in 2022. Some standards (such as IEC 62304:2006 Medical device software — Software life cycle processes) which conferred a presumption of conformity with the previous Medical Device Directive have not yet been recognised.

During the *Implementation Phase,* Medical Device manufacturers and healthcare delivery organisations ("HDOs") will collaborate to ensure that the three key properties are protected. This phase consists of:

- Acquisition of the device (including manufacturer compliance);
- Installation, customisation and configuration;
- Integration, data migration, transition and validation;
- Implementation, workflow optimisation and training.

HDOs may wish to implement the requirements of the IEC 80001-1:2021 (Application of risk management for IT-networks incorporating Medical Devices — Part 1: Safety, effectiveness and security in the implementation and use of connected Medical Devices or Connected Health software) family of standards. In addition, HDOs will also need to consider regulation related to the data that is being transmitted along with the consideration of the 3 key properties that have previously been discussed. Privacy issues will also need to be addressed. In the EU, the General Data Protection Regulation ("GDPR") [9] recognises data concerning health as a special category of data and provides a definition for health data for data protection purposes. It requires specific safeguards for personal health data which will need to be addressed in the context of Connected Health, including the facilitation of cross border care.

> *The Health IT lifecycle is broken down into three broad phases*

Data standards such as FHIR[10] and DICOM[11] are relevant in this context. In May, 2022, the European Commission published a proposal for a Regulation on the European Health Data Space ("EHDS").[12] With the proposal, the European Commission aims to make significant progress towards a single market for digital health services and products with the overall objective being to ensure that electronic health data are as open as possible and as closed as necessary to facilitate research, innovation, policy-making, and regulatory activities. The aim is to have a single internal market for health data between the EU Member States.

The *Clinical Use phase* consists of Operations and maintenance and Decommissioning. The focus for both the Medical Device manufacturer and the HDO is to ensure that the connected health system continues to be compliant with the relevant regulations and standards as these activities take place. For example, when making a change to a device within an existing system, in order to address a security vulnerability, the manufacturer and HDO will need to ensure that the change is made within the existing risk management process and that the change does not impact the key properties of the system.

Connected Health systems are increasingly including Medical Devices that use sophisticated Artificial Intelligence. The

[8] European Council, "Commission Implementing Decision (EU) 2021/1182 of 16 July 2021 on the Harmonised Standards for Medical Devices Drafted in Support of Regulation (EU) 2017/745 of the European Parliament and of the Council," *EUR-Lex*, 2021 https://eur-lex.europa.eu/eli/dec_impl/2021/1182/oj [accessed 27 July 2022].

[9] European Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC," *EUR-Lex*, 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed 27 July 2022].

[10] HL7, "HL7 FHIR Release 4B," 2022 https://hl7.org/FHIR/.

[11] Medical Imaging and Technology Alliance, "Digital Imaging and Communications in Medicine" (National Electrical Manufacturers Association, 2009) http://medical.nema.org/standard.html.

[12] European Council, "European Health Data Space," *European Commision*, 2021 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en [accessed 27 July 2022].

European Commission published its Proposal for a Regulation on Artificial Intelligence ("AI") in April of 2021,[13] which aims to develop a comprehensive framework for the regulation of AI. Parts of the proposal address high risk AI applications, which would include the use of AI in Medical Devices and Connected Health systems. No international guidance, common specifications and/or harmonised standards currently exist for the use of AI in Medical Devices. Therefore, regulators continue to work to address the challenge of regulation of Medical Device software that include AI algorithms and to address the unique challenges that AI can give rise to in the context of healthcare including, for example, the issues related to the automated processing of data and compliance with GDPR which requires that "meaningful information about the logic" involved in decisions related to their care is provided by manufacturers to patients.

> *European Commission published its Proposal for a Regulation on Artificial Intelligence ("AI") in April of 2021, which aims to develop a comprehensive framework for the regulation of AI*

While the EU Accessibility directive, EN 301 549 V3.2,[14] which came into effect in June 2021,[15] has not been specifically written with Medical Devices in mind, we believe that it should be considered in this discussion. We recognise that many national health services in European countries are public bodies, and the users of such devices will often have accessibility issues through disability, impairment or limitation, for example, visual impairment, intellectual and developmental disability. The Accessibility directive requires that all public sector bodies in the EU have accessible online websites and mobile apps, and many connected health solutions provided are implemented through these means. EN 301 549 is aligned to the Web Content Accessibility Guidelines v2.1, published by the W3C and known as WCAG 2.1.[16] These are internationally recognised requirements for producing web and mobile content, are considered best practice, and are very widely used. It should be noted that the directive also contains requirements not mentioned in WCAG 2.1, and so, there should not be a singular reliance on WCAG 2.1 when developing accessible software.

According to Tsvyatkova et al.,[17] accessibility is concerned with the quality of being "easy to reach and use." This requires the developers to understand that the software should provide the correct functions for the user and that the user interface should adhere to the directive. They also discuss the concept of accessible interaction, which would include, for example, features which support new users in understanding and using the software. Furthermore, designing of interactive elements which support low physical effort should also be considered.

04 CONCLUSION

Connected Health systems have a complex lifecycle as devices are added and removed, data is transferred within and beyond the system, and new types of technology such as AI are integrated. Different regulations apply to these phases and aspects of the lifecycle. The properties of safety, security and effectiveness are protected by these regulations and supported by the implementation of harmonised and voluntary standards. Implementation of these standards needs to be supported by all stakeholders within the broader healthcare socio-technical ecosystem. Those within HDOs, including Clinicians, Clinical Engineers, and Information Technology Specialists, need to be aware of their responsibilities under the regulations in how they design and develop, implement, and use Connected Health solutions.

[13] European Council, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS," *EUR-Lex*, 2021 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 [accessed 27 July 2022].

[14] European Union, "2016, Directive (EU) 2016/2102 of the European Parliament and the Council of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies, EN 301 549 V3.2.1, Web Accessibility Directive,No Title," 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102.

[15] European Commision, "Web Accessibility Directive — Standards and Harmonisation," 2021 https://digital-strategy.ec.europa.eu/en/policies/web-accessibility-directive-standards-and-harmonisation.

[16] WC3, "Web Content Accessibility Guidelines (WCAG) 2.1" https://www.w3.org/TR/WCAG21/.

[17] Damyanka Tsvyatkova and others, "Digital Contact Tracing Applications for COVID-19: A Citizen-Centred Evaluation Framework (Preprint)," *JMIR MHealth and UHealth*, 2021.

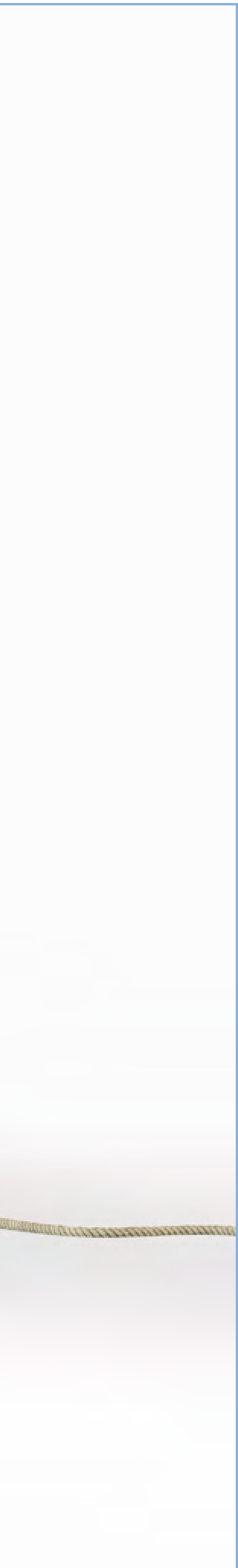
Our thesis is that, given the wide variety of regulations and standards which should be considered when developing Connected Health solutions, some of which we have discussed in the previous section, developers should consider that regulations are an important stakeholder in the design and development phase of the Health IT lifecycle. Too often, it is seen that a Connected Health solution can solve a health care issue, software is developed, and yet, it cannot be used due to the lack of implementing regulations. Users of such systems also need to be aware of these requirements. Indeed, Wykes and Schueller[18] suggested that app stores should take responsibility for providing information on, what they define as Transparency for Trust ("T4T") principles - privacy and data security, development characteristics, feasibility data, and benefits.

Technology is changing rapidly and regulators are working to keep pace. Manufacturers and HDOs need to be aware that the regulations in the space are changing rapidly and that there is a need to stay up to date with the changing position regarding regulations but also regarding recognised harmonised standards in this area.

However, to ensure that standards can support regulation, and to ensure that the standards can be adopted and implemented within specific HDO contexts, Healthcare Stakeholders need to input into the development of standards. They can become involved by engaging with national standards groups relevant mirror committees and providing feedback on their experiences of implementing standards and on this basis provide recommendations for the development of new standards in the area. ■

> *"Connected Health systems have a complex lifecycle as devices are added and removed, data is transferred within and beyond the system, and new types of technology such as AI are integrated*

[18] Til Wykes and Stephen Schueller, "Why Reviewing Apps Is Not Enough: Transparency for Trust (T4T) Principles of Responsible Health App Marketplaces," *Journal of Medical Internet Research*, 21.5 (2019) https://doi.org/10.2196/12390.a light-touch approach to consumer protection is now warranted to give customers a modicum of information to help them choose from the vast array of so-called health apps. We suggest 4 guiding principles that should be adopted to provide the consumer with information that can guide their choice at the point of download. We call these the Transparency for Trust (T4T).



TRAPS FOR THE UNWARY TELEHEALTH PROVIDER

BY
CAROL K. LUCAS

&
JENNIFER M. GUERRERO

Carol Lucas and Jennifer Guerrero are attorneys in the Health Care Practice Group of Buchalter, a Professional Corporation, resident in the Los Angeles office. Ms. Lucas chairs the Group and has over thirty years' experience representing providers in a range of transactional matters. In addition to assisting clients in health care transactional matters, Ms. Guerrero is an expert in data privacy and cybersecurity.

U.S. health care providers are heavily regulated by an overlapping patchwork of laws, including some national law and fifty different state laws. Technology has always outrun the legal framework as providers seek to establish a digital healthcare practice. This complex web of overlapping and sometimes inconsistent laws makes establishing a multi-state medical practice challenging. During the COVID-19 public health emergency ("PHE"), providers and clinicians were able to rely on a variety of temporary waivers, executive orders, enforcement discretion and regulations that made the transition to digital healthcare technologies simpler. As the present PHE begins to wind down, providers must prepare to face additional legal and regulatory issues compounding the already complex regulatory framework that telemedicine providers face.

Even before COVID-19, an increasing number of health care providers were exploring telemedicine, either as an adjunct to their primary brick and mortar practices or as a separate and new venture. The dislocations of COVID-19 accelerated this trend, especially because a number of legal restrictions on the delivery of care via telemedicine were relaxed in connection with the exigencies of the pandemic. Meanwhile, more and more providers have determined that many aspects of the service they provide can be effectively provided remotely if the technology and the tools are adequate.

However, when a provider expands from single-state practice to potentially fifty state practice (or even global practice), the legal and regulatory regime that the provider is used to may not translate to all of the provider's new practice locations. In fact, it almost certainly will not, and telehealth providers need to review a number of different regulatory regimes in each state they propose to practice in. This article will provide insight on multi-faceted digital health regulation to introduce providers and tech entrepreneurs alike to the critical issues they must confront to implement a successful multi-state telemedicine practice.

01

GOVERNMENT ATTENTION TO TELEMEDICINE FRAUD

Meanwhile, possibly because of the exploding popularity of telehealth services, the federal government has turned its attention to telemedicine fraud. On July 20, 2022, the Department of Health and Human Services Office of Inspector General ("OIG") released a Special Fraud Alert warning health care practitioners to exercise caution when entering into arrangements with "purported" telemedicine companies. According to the OIG, unscrupulous telemedicine companies are using kickbacks to reward practitioners for ordering or prescribing medically unnecessary items or services for patients that the provider never examined or meaningfully assessed. Such practices, per the OIG, potentially violate the federal anti-kickback statute, and may also corrupt medical decision-making, drive inappropriate utilization and result in patient harm.

The special Fraud Alert identified a list of suspect characteristics related to practitioner arrangements with telemedicine companies that could present a heightened risk of fraud and abuse. They include:

- The purported patient was recruited by the telemedicine company or its sales agents advertising free or low out-of-pocket cost items or services;
- The practitioner has insufficient contact with or information from the patient to meaningfully assess the medical necessity of the items or services ordered or prescribed; frequently, the provider does not have a medical record but only a questionnaire;
- The practitioner is compensated based on the volume of items or services ordered or prescribed (or the number of records reviewed);
- The telemedicine business only furnishes items or services to federal health care program beneficiaries and does not accept any other insurance;
- The telemedicine company claims not to serve federal health care program beneficiaries, but may, in fact, bill federal health care programs;
- The telemedicine company only furnishes one product or a single class of products, potentially restricting a practitioner's treatment options to a predetermined course of treatment; and
- The telemedicine company does not expect practitioners to follow up with purported patients.

The Special Fraud Alert was careful to note that these factors do not necessarily connote fraud, but were intended to serve a warning that practitioners should be wary of being used by questionable telemedicine businesses. None of this should be surprising to health care providers; paying for referrals or charging for services that were ether not provided or not necessary has always been considered healthcare fraud. What is new is the extra dimension added by purely virtual services and the involvement of the telemedicine company that may not understand a provider's professional requirements, or that may not appreciate how different health care is from other technology-enabled industries.

02

DATA PRIVACY AND CYBERSECURITY

Telehealth providers are bound by federal and state regulations when providing services, just as they would be when providing in-person services. The additional element of providing "remote" care inherently poses risks of unlawful disclosure since it is dependent on the digital infrastructure, which, most often is developed and controlled by a third party that will not guarantee compliance in terms of design, functionality or security. Ironically, the same connectivity provided by telemedicine creates a slew of privacy and security risks, as any data transferred over the internet runs the risk of interception by hackers and other bad actors. While many software programs or platforms purport to comply with Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), there is not a single standard that would certify that the software program or platforms meets all federal and state regulations. Telehealth providers must be aware of the myriad federal and state regulations relating to administrative, physical, and technical safeguards and required notifications, consents and data sharing agreements that may be required to launch a telemedicine practice.

> *Telehealth providers are bound by federal and state regulations when providing services, just as they would be when providing in-person services*

HIPAA. The main federal law that governs the collection and use of patient/consumer health information is HIPAA. The U.S. Department of Health and Human Services ("HHS") published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" ("e-PHI").

Telehealth providers should be familiar with HIPAA and its privacy and security requirements as it not only applies to telemedicine, but to any traditional medical practice that transmits health information in electronic form. However, since HIPAA only applies to individuals and entities who qualify as a covered entity or a business associate, and not necessarily all third party vendors, many technology partners are ignorant to its requirements. Since HIPAA is not applicable to these technology partners, the software platform or mobile application may not incorporate all the required administrative, technical, and physical safeguards. Likewise, if they use other vendors (cloud service providers, help desk, etc.), chances are such vendors are not compliant either. Further, HIPAA does not directly apply to many consumer-based digital health software or applications. For example, information (including medical information) provided by a consumer to a medical device or other company that is not a covered entity or business associate is not required to comply with HIPAA.

This gap in coverage places the burden on the telehealth providers to ensure their own compliance and their vendor's compliance (including subcontractors) with HIPAA through their third-party contracts (commonly called business associate agreements or "BAAs"). Telehealth providers can review the HHS Health Industry Cybersecurity Practices ("HICP"): Managing Threads and Protecting Patients, for practical guidelines to manage cyber threats and protect patients.

State Privacy Law Considerations. In addition to HIPAA, telehealth providers must take into account numerous state privacy laws when establishing a national telehealth practice. While some state laws are duplicative of the requirements under HIPAA, a number of state laws impose more stringent requirements that impact consumer/patient consent and notice requirements, employee training requirements, patient records request and other privacy requirements. For example, under California law a patient authorization is not HIPAA-compliant unless it is in fourteen point font. In Texas, a covered entity only has fifteen days from the patient's request to produce electronic copies of their electronic health record, reducing the timeframe of thirty days under HIPAA. Similarly, other state laws are potentially triggered based upon the type of information a company collects and uses. If genetic data is collected, states like California, Wyoming, and Utah impose additional notice and consent requirements. Both Illinois and Texas impose additional regulations on companies who collect and use biometric identifiers.

To make things more complicated, a number of states, including California, Utah, Colorado, Virginia, and Connecticut, have passed comprehensive privacy laws that impact the delivery of telemedicine services, notice requirements (privacy policies), consent requirements from consumers not only subscribing to the telehealth services but also those browsing telehealth provider's websites, and data breach notification requirements. The misconception that these laws are inapplicable is a fatal mistake, since most telehealth providers engage in some form of e-commerce and collect consumer data of non-patients that is governed by state law rather than HIPAA.

PCI Compliance. Telehealth providers that store, process, or transmit credit card data are required to adhere to the same standards as a business in any other industry. Typically, a brick and mortar provider may have implemented a payment system that did not require them to store, process, or transmit credit card data. However, with the rise of technology and e-commerce, most providers are at minimum transmitting credit card data to a third party provider, like Stripe or Clover.

If a provider stores, processes, or transmits credit card data, it must maintain Payment Card Industry ("PCI") compliance to ensure that all transactions using credit or debit cards are safe and secure in order to protect the patients and the provider from unauthorized access. While there are many overlapping security measures between PCI compliance and HIPAA, telehealth providers still need to undergo an annual PCI compliance audit. Telehealth providers that utilize third party payment processors should also ensure that their vendor is PCI Compliant.

Cybersecurity Insurance. Cybersecurity insurance can help hedge the costs of a cyber-security incident or data breach. In some cases, liability insurance may cover telehealth services, but may carve out costs related to a cyber-security incident or data breach. Before procuring any insurance, telehealth providers should review the coverage limitations.

03

TECHNOLOGY REGULATION AND ADVERTISING ISSUES

The U.S. Food and Drug Administration ("FDA") regulates many types of digital health technologies that are considered "medical devices" such as mobile health/medical applications and software, health information technology, wearable devices, telehealth, and telemedicine. Interestingly, the FDA expands the definition of telemedicine to include the delivery of medical information or counseling to patients over the phone, including the use of home specimen collection kits where the distributors deliver the results of the test and counseling to the consumer via phone or technology platform purporting to cast a larger net of companies. However, the FDA has stated that it intends to enforce compliance where the medical device poses more than a minimal risk to consumers.

Section 5(a) of the Federal Trade Commission Act ("FTC Act") (15 USC §45) also applies to telehealth providers and prohibits "unfair or deceptive acts or practices in or affecting commerce." Telehealth providers and their vendors are prohibited from making deceptive or misleading claims, and engaging in acts or practices that cause, or are likely to cause, substantial injury to consumers that they cannot avoid and that do more harm than good.

Any developer of` a mobile health app that collects, creates, or shares consumer information, telehealth providers can use the tool on the Federal Trade Commission's website to find out when the FDA, Federal Trade Commission ("FTC"), or HIPAA laws apply.

04

TELEHEALTH CONTRACT ISSUES

Telemedicine providers should be weary of blindly entering into telemedicine contracts with developers (if they are creating their own platform/application), document storage vendors, software and mobile application vendors, and other types of technology agreements. Many of these agreement (if not all) contain one-sided limitation of liability clauses, lack appropriate indemnification and data security provisions, do not appropriately protect the telemedicine provider's intellectual property and/or consumer data, or fail to meet regulatory requirements. Negotiating a fair vendor contract is essential to protecting the telehealth provider's practice from noncompliance and liability.

Limitation of liability clauses should include a value large enough to cover the damages that could be reasonably assumed by the vendor. Carve outs for incidental, consequential, and punitive damages may prevent recovery caused by the vendor's negligence, or any fines or penalties imposed from a data breach of the system. Indemnification should be fair given the scope of services and should work in conjunction with the limitation of liability. Intellectual property indemnification is typically provided by the vendor since the vendor supplies the intellectual property. Data security and privacy provisions for telemedicine services should comply with HIPAA, including the execution of a business associate agreement.

05

LICENSING AND PARITY

Licensing. Licensing can create many issues for telehealth programs. Generally telehealth providers need to be licensed in the states in which the patients are located. A physician physically located in Missouri, for example, could treat a patient located in California if the physician is licensed in California, the state in which the patient resides. Therefore, with limited exceptions, telehealth consultations with a physician across state lines require some form of licensing paperwork depending on rules set by the state where the patient is located.

Interstate compacts (agreements among two or more states) can streamline the process for health care providers to practice in multiple states — expediting the licensing process or allowing members to practice under a single multistate license. These include:

- The Interstate Medical Licensure Compact ("IMLC") streamlines the licensing process for physicians so they can practice medicine in multiple states. About 80 percent of physicians meet the criteria for licensure through the Compact, according to the Interstate Medical Licensure Compact Commission ("IMLCC"). Thirty-nine states have joined the compact.
- The Nurse Licensure Compact ("NLC") authorizes eligible nurses to practice across multiple member states while maintaining a single license.
- The Psychology Interjurisdictional Compact ("PSYPACT") authorizes eligible psychologists to practice telepsychology across member states.
- The PT Compact authorizes eligible physical therapists to work in multiple member states under a single license.

> *"Limitation of liability clauses should include a value large enough to cover the damages that could be reasonably assumed by the vendor*

Just as licensure requirements depend on the patient's location, so do regulations governing a provider's mode of practice, including scope of practice issues, supervision requirements and consent requirements. Simply stated, a medical (or other provider) licensed in a particular state carries with him or her that state's regulation of a licensee. For example, a nurse practitioner's scope of independent practice (i.e. what a nurse practitioner may lawfully do without physician supervision) may be vastly different in California than in Arkansas. Even if practitioners obtain their licenses via a single application through a multi-state compact, they are charged with compliance of the laws in each such state.

Parity. The term "parity" means two different things in connection with insurance coverage for telehealth services: coverage parity and payment parity. Coverage parity requires payors to reimburse providers for services provided via telehealth if the same service is covered in person. Payment parity goes a step further and requires payors to reimburse the same amount for a service provided via telehealth means. Approximately 40 states have passed laws mandating coverage parity. Of those, 31 mandate payment parity. Even in states with parity requirements, however, coverage varies. Some laws cover only physician services; others more broadly cover virtual care and remote patient monitoring as well, services that only exist in a telehealth environment.

Additional parity mandates were implemented in response to the COVID-19 pandemic, including coverage for services delivered via telephone and requiring waiver of patient co-payments. It is not clear how long any special pandemic rules will last or the extent to which certain new rules may become permanent.

06

UNIQUE TELEHEALTH LAWS THAT APPLY TO A MULTI-STATE PRACTICE

A comparison of how California and Texas regulate the establishment of a physician-patient relationship is instructive. For California, the physician must conduct an "appropriate" initial examination. Depending on the nature of the service, that examination could be accomplished remotely, but may need to be conducted in person. The California Medical Board leaves that decision to the professional judgment of the physician.

Texas requires physicians to have an established relationship with the patient before prescribing medications via telehealth. Previously, establishment of a relationship required an in-person encounter, although Texas now permits the relationship to be established through a live video telemedicine visit.

Further, the federal Ryan Haight Act requires a controlled substance prescription to be issued by a practitioner who has conducted at least one in-person medical evaluation or by a covering provider if the primary provider is unavailable. This requirement was waived for the duration of the COVID-19 public health emergency, but as of now is set to become effective once again 151 days after the end of the public health emergency. The public health emergency currently expires on October 13, 2022, but may be extended again.

Corporate Practice of Medicine: The corporate practice of medicine prohibition generally prohibits lay (i.e. non-professional) entities from providing medical services. In most corporate practice states, that means that a general business corporation cannot provide and charge for physician services. A telemedicine provider located in a state without a corporate practice ban may be organized as a general business entity and may employ physicians. Consider this example: Oklahoma is not a corporate practice of medicine state; Texas is a corporate practice state. If a telemedicine provider in Oklahoma were to provide services to a patient in Texas through a Texas-licensed physician employee, the payment by the Texas patient to the telemedicine provider could be held to violate Texas's corporate practice of medicine ban. Further, not all states permit foreign (i.e. sister state) professional entities to practice there. If they do, they generally require local licensure by some or all of the entity's owners, officers and directors or managers. New York, for example, permits the qualification of foreign professional service corporations in New York, provided that all of the shareholders, officers, and directors are licensed to practice medicine in New York.

> *Further, the federal Ryan Haight Act requires a controlled substance prescription to be issued by a practitioner who has conducted at least one in-person medical evaluation or by a covering provider if the primary provider is unavailable*

Telemedicine provider businesses in corporate practice of medicine states generally adopt a management services organization ("MSO")/friendly professional corporation ("PC") model. Under this model, an MSO, owned wholly or in part by non-licensed individuals, provides administrative support services to a medical practice pursuant to a written services agreement. Often, the MSO provides everything that that does not require a medical license to provide, including space, supplies, equipment, non-professional staff, accounting, billing and collection, and payables management. A well-crafted management services agreement clearly recognizes the PC's control over all clinical decisions and the medical practice itself, including the authority to hire physicians, set clinical protocols and enter into agreements to provide medical services. In the telemedicine context, the MSO is the technology-enabled platform company. There is risk, however, if the MSO fails to observe the professional separateness of the PC or its providers.

Physician Dispensing: If the telehealth provider dispenses medication to patients in remote locations, laws relating to physician dispensing will be implicated. Here again, state laws vary. The New York Board of Pharmacy takes the position that physicians may not dispense in New York at all. In California, physicians may dispense as long as they comply with all statutory requirements regarding labeling, etc. Florida permits physician dispensing upon registration with the Florida medical licensing board as a dispensing practitioner and compliance with pharmacy disclosure regulations.

Language Interpretation Services: Telemedicine providers are subject to the Americans with Disabilities Act ("ADA") and the federal Civil Rights Act. The ADA requires public accommodations to ensure that no individual with a disability (including deafness or hearing impairment) is excluded, denied services, segregated or otherwise treated differently than other individuals because of the absence of auxiliary aids or services. Health care providers are places of public accommodation for purposes of the ADA, which means that telemedicine services for hearing or vision impaired patients should be made available. States also vary widely in requirements to provide services for variously impaired patients. For example, Mississippi requires the telemedicine equipment and network used for remote patient monitoring services to accommodate non-English language options. New York requires culturally competent translation services for telepsychiatry.

The federal Civil Rights Act of 1964 may also apply. The Act prohibits discrimination based on race, color, or national origin, which includes limited English proficiency individuals. The Act applies to entities receiving "federal financial assistance," including Medicare Part A. To the extent that a hospital provides telemedicine services, its remote services, as well as its in-person services, are required to provide language assistance.

For telemedicine providers, licensing laws are only the starting point. Telemedicine providers should be aware that a business model that complies with one state's laws may not be exportable without review and some tweaking. ■

> “*If the telehealth provider dispenses medication to patients in remote locations, laws relating to physician dispensing will be implicated. Here again, state laws vary*

WHAT'S AHEAD FOR CONNECTED HEALTH POLICY: STATE & FEDERAL POLICIES IMPACTING TELEHEALTH ACCESS, PRIVACY LAWS & POLICYMAKER INTERESTS

BY
AMY DURBIN

Policy Advisor, Center for Connected Health Policy

01 BACKGROUND: TELEHEALTH POLICY AT THE STATE AND FEDERAL LEVEL

State and federal governments have had connected health policies related to telehealth, privacy and the technological infrastructure required for it on the books for decades. Historically, telehealth policies have focused on payer reimbursement with the federal government focusing on Medicare telehealth coverage and deferring most Medicaid and private payer policies to the states. As providers have increasingly implemented telehealth, however, state licensing boards have become more involved and started adopting their own policies around licensure and prescribing specific to telehealth.

As the healthcare world has become more electronic, federal privacy laws, the most recognized of which being the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[2] were adopted to primarily ensure providers were protecting patient medical information when they shared it with insurers electronically. However, most of those laws did not contemplate a world of telehealth vendors and medical app manufacturers, including connected devices much broader than healthcare such as smartphones and smartwatches that could begin to track, store, and share health information. Unfortunately, as with the pandemic, technological advancements have also exacerbated existing disparities amongst underserved populations that have not been afforded equitable access to most services, including healthcare, digital devices, and broadband infrastructure.

All of these issues rose in importance the moment COVID-19 hit the United States and policymakers realized that increasing access to telehealth was vital in order to maintain the healthcare delivery system during a pandemic. Existing state and federal policies were expanded, waived, or relaxed to promote telehealth, while new policies were implemented. Now more than two years into the pandemic, many temporary policies have expired, and restrictions re-implemented. Some new state and federal policies have been passed that may apply temporarily, permanently, or post-PHE, leaving both providers and patients struggling to keep up with what policies are in place and how to comply in order to continue providing and accessing services via telehealth into the future.

A. Telehealth Regulatory Environment Prior-to and During the COVID-19 Pandemic

Federal telehealth policies center around reimbursement related to Medicare, which prior-to the pandemic was very restrictive in covering services provided via telehealth. Not only was coverage limited to certain services and providers, but also certain patients. Most of the restrictions were waived at the start of the pandemic and most policy expansions remain in effect given their attachment to the ongoing federal PHE.[3]

State reimbursement policies varied widely prior to COVID, though most expanded their coverage of telehealth substantially during the pandemic, especially related to audio-only and payment parity. In terms of licensure, when telehealth is used it is typically considered to be rendered at the physical location of the patient, therefore, providers generally must adhere to the laws and regulations of the state the patient is physically located in – meaning having a license, participating in a Compact or falling under a licensing exception. Licensing exceptions pre-pandemic were limited, but once COVID hit, almost all states implemented some type of temporary policy related to out-of-state providers.[4] Emergency state orders related to out-of-state providers varied widely as some states allowed blanket licensure waivers while others had a very specific process put into place that required approval and association with in-state health care facilities. Many states also relaxed policies related to prescribing limitations. Remaining COVID-19 flexibilities can be found utilizing the Center for Connected Health Policy's ("CCHP") Policy Finder tool.[5]

> *"Federal telehealth policies center around reimbursement related to Medicare, which prior-to the pandemic was very restrictive in covering services provided via telehealth*

B. Overlapping Connected Health Privacy Laws

One of the main federal PHE flexibilities instituted at the beginning of the pandemic included relaxed enforcement of certain federal privacy laws related to the use of various telehealth technologies.[6] The Telehealth Notification issued states that the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") will exercise discretion in penalizing providers under HIPAA related to

[2] *Health Insurance Portability and Accountability Act of 1996*, 110 Stat. 1936, 42 U.S.C. §§ 101-521, https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

[3] Office of the Assistant Secretary for Preparedness & Response, U.S. Department of Health & Human Services, Renewal of Determination that a Public Health Emergency Exists, (July 15, 2022), https://aspr.hhs.gov/legal/PHE/Pages/covid19-15jul2022.aspx.

[4] Juan J. Andino et. al., *Interstate Telehealth Use by Medicare Beneficiaries Before and After COVID-19 Licensure Waivers*, HEALTH AFFAIRS, June 2022, https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2021.01825?journalCode=hlthaff.

[5] Center for Connected Health Policy, Policy Finder, https://www.cchpca.org/all-telehealth-policies/.

[6] Office for Civil Rights, U.S. Department of Health and Human Services, Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, (April 21, 2020), https://www.govinfo.gov/content/pkg/FR-2020-04-21/pdf/2020-08416.pdf.

their good faith use of audio or video remote communication technologies during the federal PHE. While states often refer to federal guidance related to privacy issues, especially during the pandemic, some may have their own privacy laws as well. Not only do federal and state privacy laws overlap, with states sometimes adopting more-strict requirements, but general privacy and medical privacy laws can also both apply. For example, California has their own medical privacy laws that are more expansive than HIPAA,[7] as well as laws that apply to personal information outside of medical information.[8] Since HIPAA only really applies to electronic information and medical providers, with the increased use of devices that track and receive health information, policymakers are now focused on adopting laws that apply medical privacy requirements beyond medical entities, such as computer and phone applications used by businesses as well as the manufacturers of connected devices that maintain and potentially share such information.

In addition, schools that may provide access to healthcare services either in-person and/or via telehealth must comply with their own set of privacy rules, and often laws may be different and specific in the case of a minor's privacy. Sometimes mental health information is governed by even more heightened requirements. Varying regulatory environments and authorities when it comes to privacy have thus become even more complicated the more connected healthcare has become. Understanding who (i.e., medical provider, school, or general business) and what (such as medical information, personal information, medical records, or an actual device) exactly a law applies to is increasingly important. In terms of telehealth, rules may also vary based on the type of modalities used (i.e., audio-only, live video, or store-and-forward messaging applications), meaning providers need to be mindful of compliance across all different platforms or systems used.

Some states and insurers have their own policies governing the types of technologies that can be used as well. Regardless of platform or modality, under HIPAA, safeguards to limit incidental uses or disclosures of personal health information ("PHI") should be implemented, such as conducting telehealth in a private setting, using low voices, and recommending patients be in private setting.[9] OCR has also identified certain public-facing communication products to be unacceptable forms of remote communication as they are inherently designed to be open to the public, such as TikTok, Facebook Live, Twitch, or public chat rooms.[10]

> *Some states and insurers have their own policies governing the types of technologies that can be used as well*

C. Broadband and Infrastructure Issues

While audio-only has not always been contemplated underneath telehealth policies, attention during the pandemic to the telephonic modality has largely risen due to remaining broadband and digital infrastructure barriers across the country, which often impact underserved communities in particular. Not only do technological issues often arise more frequently for providers and patients attempting to use live video telehealth, but for patients in rural areas and those without access to affordable broadband or digital devices, audio-only may be their primary option to accessing healthcare. As connected as it may seem we've all become, the digital divide – which refers to the gap between Americans with access to telecommunications and information technologies and those that do not[11] – shows that is not always the case. This issue has become apparent in many other areas as well, for instance in education which struggled to provide distance learning to all students during the pandemic. Since the digital divide impacts numerous aspects of our lives, a real solution requires engagement across an expanding group of stakeholders and state and federal agencies. In response, numerous initiatives and investments into broadband have been made at all government levels just over the past couple of years, further necessitating outreach across communities to ensure those needing additional resources are aware of the options that may be available. In addition, some states are seeking to further regulate broadband providers directly so that they pro-

[7] *Confidentiality of Medical Information Act*, California Civil Code §§56, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV.

[8] *California Consumer Privacy Act of 2018*, California Civil Code §§ 1798, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[9] Office for Civil Rights, U.S. Department of Health and Human Services, FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency, https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.

[10] *Id*.

[11] Congressional Research Service, *The Digital Divide: What Is It, Where Is It, and Federal Assistance Programs*, (March 9, 2021), https://sgp.fas.org/crs/misc/R46613.pdf.

vide additional resources and access to affordable, high-speed, and high-quality broadband.

02
WHAT'S NEXT: THE FUTURE OF TELEHEALTH POLICY

The pandemic opened a policy window for the future of telehealth policy and connected healthcare. While advocates continue to press for policies to be made permanent at the state and federal levels related to telehealth there are certain policies that are still likely to end. The status of state COVID telehealth policies vary widely as some have ended due to a specific expiration date or the end of the state's PHE, while other policies have been made permanent or extended to a future date. Federally, at the time this article is being written, we've seen the Administration taking some steps towards permanent policy for Medicare, but many of the temporary telehealth COVID policies on the federal level would require Congressional action to make them permanent.

At this time, there's only been a small grace period provided after the PHE to extend some of the temporary telehealth policies. Part of the reason for the slower action by Congress is not only the continued existence of the PHE, but hesitation from some members on the efficacy of telehealth. Several Congressional members have been vocal in comments regarding needing more studies on telehealth utilization, potential inequities, and fraud, as well as the quality of care provided via telehealth, to officially guide their adoption of future telehealth policy. However, action on certain issues may be prompted by other factors. For example, regarding privacy, additional indicators exist pointing toward the potential for change and highlighting it as an area of continued focus for policymakers, regulators, and both healthcare providers and consumers – especially in light of *Roe v. Wade* recently being overturned by the Supreme Court in *Dobbs v. Jackson*. Therefore, while the opportunities for policy change in regard to telehealth and privacy may seem endless, opposing adjacent interests could further impact the ability to expand access to telehealth and connected healthcare generally.

A. Planned Post-PHE Telehealth Policies

With the renewal of the federal PHE on July 15, 2022 for another 90 days, federal Medicare telehealth expansions will remain in effect until at least mid-October 2022, including federal privacy and prescribing flexibilities.[12] In addition, recent federal legislation passed to ensure continuation of most emergency Medicare telehealth expansions for 151 days post-PHE expiration as well.[13] While Congress and CMS have made some policies permanent, many are set to expire either at the end of the PHE or at the end of the 151-day extension. State policies vary, but many have already entered into the post-PHE landscape and adopted long-term policies, especially related to reimbursement and licensure. Prescribing and privacy policy areas have the most unknowns but future changes at both the state and federal level are possible.

1. Permanent Policies

Some of the main Medicare telehealth billing rules relaxed during the PHE were those related to audio-only reimbursement and rules limiting where the patient is located when the telehealth encounter takes place, or originating site rules,[14] including allowing the home to be an eligible originating site. As discussed in a recent CCHP Newsletter,[15] overall, Medicare reimbursement for eligible telehealth services[16] when the patient is located in a geographically rural area AND in an eligible originating site will continue permanently after the PHE, similar to pre-PHE policy. There are some new allowances for mental health services and audio-only modalities post-PHE that CMS outlined through their approach to the 2022 Physician Fee Schedule ("PFS").[17] For instance, PFS policies will continue reimbursement of telemental health services, includ-

[12] Office of the Assistant Secretary for Preparedness & Response, *supra* note 2.

[13] *Consolidated Appropriations Act, 2022*, 136 Stat. 49, https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf.

[14] Center for Connected Health Policy, Federal Medicare Overview, https://www.cchpca.org/federal/?category=medicaid-medicare&topic=overview.

[15] Center for Connected Health Policy, *Insight from CCHP: Telehealth Policies Impacted by Anticipated Upcoming End to PHE,* (April 12, 2022), https://mailchi.mp/cchpca/insight-from-cchp-on-telehealth-policies-impacted-by-anticipated-upcoming-end-to-phe-and-much-more.

[16] Centers for Medicare and Medicaid Services, List of Telehealth Services, (June 17, 2022), https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes.

[17] Centers for Medicare and Medicaid Services, 2022 Physician Fee Schedule, (November 19, 2021), https://www.govinfo.gov/content/pkg/FR-2021-11-19/pdf/2021-23972.pdf.

ing audio-only, and when the patient is located at home in some instances, as well as reimbursement to federally qualified health centers ("FQHCs") and rural health clinics ("RHCs") for mental health visits on a permanent basis. Therefore, changes taken thus far at the federal level related to Medicare have been minimal and limited, as CMS is restricted in their ability to act without Congress making broader changes to remaining statutory requirements. The main statutory policy changes made by Congress were through H.R. 133 in December 2020, which added rural emergency hospitals as an eligible originating site and removed geographic restrictions for mental health services provided via telehealth, permitting the ability for patients to receive such services at home. However, the new allowances for mental health are attached to new in-person visit requirements and require an existing patient-provider relationship.[18]

As far as prescribing, in one permanent federal development, the U.S. Food and Drug Administration ("FDA") announced in December 2021 through an update on its FAQ webpage that it would be ending a longstanding policy to require the in-person dispensing of mifepristone (a drug used to terminate pregnancy).[19] Prior to the PHE, dispensing of the drug had to occur at a clinic, medical office or hospital. However, the requirement was temporarily waived during the PHE when a mail order distribution model was launched and remains in use today.

> *At this time, there's only been a small grace period provided after the PHE to extend some of the temporary telehealth policies*

At the state level, common permanent policy changes seen in Medicaid included allowing the home to be an eligible patient originating site, expanding covered services and providers, and adding audio-only reimbursement, which doubled from this time last year, reflecting its gained importance as a result of the pandemic. More states are explicitly allowing the ability to prescribe and a patient-provider relationship to be established through a telehealth exam, for instance West Virginia explicitly allows audio-only calls to establish the relationship. Many states have also updated their licensure policies, with joining licensure compacts continuing to be increasingly common.

As of Spring 2022, 15 states now have licensure processes and exceptions specific to practicing telehealth across state lines,[20] although the criteria to participate in each vary widely. Some states still require certain fee and application processes similar to licensure, some of those processes only apply to certain boards/practitioners, and other exceptions only apply in very specific circumstances. Given nuances in state laws and requirements that continue to frequently evolve, it is best to check with state licensing boards both in the state where the provider is located and in the state the patient will be located to ensure the state doesn't have any additional rules or unique interpretations of the law.

2. Extended Policies Set to Expire

Medicare reimbursement for telehealth services provided to patients at home and the expanded list of eligible providers allowed during the PHE in Medicare, such as occupational therapists, physical therapists, speech language pathologists and audiologists, are policies only protected during the PHE and during the 151-day extension period. During the COVID-19 pandemic, additional services were also temporarily made eligible for reimbursement if provided by telehealth. Some of these services have been approved to be made permanently available after the PHE, others were put into a special category that will make them temporarily available through the end of 2023, and the rest would have not been eligible to be provided via telehealth in the Medicare program after the PHE is declared over. However, in July 2022 CMS released proposed changes for the FY 2023 Medicare PFS[21] clarifying that they will continue to cover those latter services as eligible Medicare telehealth services[22] through the 151-day extension period.

[18] Center for Connected Health Policy, *Telehealth Provisions in the Consolidated Appropriations Act, 2021 (HR 133)*, (January 2021), https://www.cchpca.org/2021/04/Appropriations-Act-HR-133-Fact-Sheet-FINAL.pdf.

[19] U.S. Food and Drug Administration, *Questions and Answers on Mifeprex*, (December 16, 2021), https://www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/questions-and-answers-mifeprex.

[20] Center for Connected Health Policy, State Telehealth Laws and Reimbursement Policies, (Spring 2022), https://www.cchpca.org/2022/05/Spring2022_Infographicfinal.pdf.

[21] Proposed Rule, Centers for Medicare and Medicaid Services, *Medicare and Medicaid Programs: Calendar Year 2023 Payment Policies under the Physician Fee Schedule*, (July 29, 2022), https://www.federalregister.gov/public-inspection/2022-14562/medicare-and-medicaid-programs-calendar-year-2023-payment-policies-under-the-physician-fee-schedule.

[22] Centers for Medicare and Medicaid Services, *supra* note 15.

Some states have gone the temporary extension route, for instance Maryland[23] and Minnesota[24] passed laws extending COVID-19 audio-only reimbursement and payment parity requirements until June 30, 2023. Connecticut[25] also extended some policies including audio-only until June 20, 2023, and California[26] extended their COVID-19 telehealth policies until the end of 2022. Many states also seem poised to study COVID telehealth expansion impacts to govern further long-term regulatory changes.

3. What We Don't Know

Currently, emergency federal prescribing and privacy flexibilities are slated to end post-PHE. When the PHE ends, the in-person requirement (with limited exceptions that allow a patient to be located in a doctor's office or hospital registered with the Drug Enforcement Agency (DEA)) will likely go back into effect. Congress directed the DEA to promulgate regulations to allow for further exceptions to online federal prescribing restrictions so that telehealth can be further used to prescribe controlled substances through creation of a registry, but the DEA has yet to do so – however, in 2021 they made a comment in an unrelated matter that they intend to do so soon.[27] As far as privacy, OCR's enforcement discretion to telehealth providers allowing them to utilize any non-public facing remote communication product, even if they don't fully comply with the requirements of HIPAA,[28] is also set to expire at the end of the PHE. Nevertheless, since this decision was made administratively, OCR technically has the ability to keep this policy or allow it to expire.

B. Ongoing Research Efforts: Policymaker Concerns & Desire for Data-Driven Policies

It is possible a number of recent telehealth studies and ongoing research efforts will impact long-term telehealth policy adoption and guide the future connected healthcare landscape. Not only have states commissioned studies into telehealth utilization and inequities, but Congress has as well. Therefore, it is important to note general findings and hope that policymakers take all studies into context as a whole before rushing to any conclusions that result in policy negatively impacting access to care.

> *Currently, emergency federal prescribing and privacy flexibilities are slated to end post-PHE*

1. Inequity Concerns

Focus on the relationship between telehealth and disparities in access to care continues to be a main focus of research and has resulted in new studies examining pandemic era data and the use of telehealth among disadvantaged populations. While policymakers and studies often try to put findings into two groups, whether telehealth increases or decreases inequities, to determine whether to expand or restrict coverage long-term, research shows that the study framework used and considerations made may impact outcomes more so than telehealth itself. For instance, in May of this year, a study was published in *Health Affairs* that found that as a result of emergency federal telemedicine coverage expansions, access increased for all Medicare populations, including those in the most disadvantaged areas.[29] The study was framed to examine the impact of expanded telehealth coverage policies on different populations, rather than looking at access generally where inequities have unfortunately always

[23] Center for Connected Health Policy, Maryland Medicaid Email, Phone, & Fax, (Jan. 25, 2022), https://www.cchpca.org/maryland/?category=medicaid-medicare&topic=email-phone-fax.

[24] Center for Connected Health Policy, Minnesota Medicaid Email, Phone, and Fax, (March 28, 2022), 2 https://www.cchpca.org/minnesota/?category=medicaid-medicare&topic=email-phone-fax.

[25] Center for Connected Health Policy, Connecticut Medicaid Email, Phone, and Fax, (Feb. 7, 2022), https://www.cchpca.org/connecticut/?category=medicaid-medicare&topic=email-phone-fax.

[26] Center for Connected Health Policy, California Medicaid Email, Phone, and Fax, (Jan. 17, 2022), https://www.cchpca.org/california/?-category=medicaid-medicare&topic=miscellaneous-medicaid-medicare.

[27] Final Rule, Drug Enforcement Administration, *Registration Requirements for Narcotic Treatment Programs with Mobile Components*, (June 28, 2021), https://www.federalregister.gov/documents/2021/06/28/2021-13519/registration-requirements-for-narcotic-treatment-programs-with-mobile-components.

[28] Office for Civil Rights, *supra* note 5.

[29] Sanuja Bose et. al., *Medicare Beneficiaries In Disadvantaged Neighborhoods Increased Telemedicine Use During The COVID-19 Pandemic*, HEALTH AFFAIRS, (May 2022), https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2021.01706?utm_campaign=may2022issue&_gl=1*1qy93rn*_ga*MTUyNzI2MDk2NC4xNjUxNjk0MTI4*_ga_PVWVB9KDNZ*MTY1MTY5NDEyOC4xLjAuMTY1MTY5NDEyOC42MA..&utm_medium=press&utm_content=bose&utm_source=mediaadvisory&journalCode=hlthaff.

existed. Comparing pre-COVID temporary waiver data with post-waiver implementation data, the authors discovered that the highest odds of utilization were among those in disadvantaged and metropolitan areas. As reported in a *Managed Healthcare Executive* article on the study, the Johns Hopkins researchers concluded that the results suggest that increased Medicare telemedicine coverage policies improve access to underserved populations without worsening disparities.[30]

An additional study published this year in *Telemedicine Journal and e-Health* showed that a virtual care program at Penn Medicine is reducing barriers to access specifically for Black patients and eliminating historic disparities. The authors looked at approximately one million appointments per year in both 2019 and 2020 for Philadelphia area patients and found that Black patients used telehealth more than non-Black patients and that appointment completion gaps between Black and non-Black patients closed.[31]

Another recent study, *Policy Considerations to Ensure Telemedicine Equity*, looked at various factors that must be taken into account to allow telehealth to increase equitable access to care.[32] The author clarifies that equity is a matter beyond telehealth and is related to patient-level barriers that include family, community, and general health care delivery level factors, such as issues related to the digital divide. In addition, the article cautions against policies focusing on increased utilization concerns, stating that increased use may mean that patients are finally attaining the care they need, in addition to the fact that increased access may reduce overall health care costs. Therefore, policies seeking to reduce reimbursement or limit audio-only modalities to address utilization and cost concerns may instead primarily reduce clinicians' willingness to offer telehealth and modalities that mitigate access barriers for historically excluded groups. The article also highlights how varying payer policies, such as those that allow reimbursement for telehealth visits with new patients versus those that do not, creates inequities, and that differing medical licensing and/or prescribing regulations by states can create inequitable access issues on top of differing coverage policies. These policy considerations are key to ensuring telemedicine mitigates inequities rather than exacerbates them.

While the pandemic generally has highlighted and exacerbated existing inequities, it has also provided the information necessary to show telehealth's ability to address disparities and increase equitable access to care. It is important that policymakers take such findings and opportunities from studies on telehealth equity into account when looking to potentially make pandemic policies permanent in order to properly preserve telehealth's positive impacts. It is also important that the framework used in the study be placed in context to help explain why some research speaks to telehealth disparities, or health care disparities, versus how telehealth is decreasing health care disparities. As shown in the aforementioned studies and articles, the difference in framing showcases that telehealth in and of itself does not create or exacerbate disparities, rather it is a tool that can be utilized to decrease disparities in access to care.

> “*Another recent study, Policy Considerations to Ensure Telemedicine Equity, looked at various factors that must be taken into account to allow telehealth to increase equitable access to care*

The tool has to be allowed to be effective, however, and that is where the role of public policy comes in. Policies must support broadband and telehealth infrastructure and promote the use of technology to deliver care equal to the delivery of in-person care. For instance, Medicaid policies that limit when telehealth can be used and/or certain allowable modalities can create inequities in comparison to more expansive commercial policies that guarantee better telehealth access to non-Medicaid patients. Therefore, policymakers must recognize that regulatory restrictions around telehealth cannot prevent already existing general access disparities, rather it is often the regulatory restrictions around telehealth that lead to exacerbating disparities. It becomes vital that research be put into context so that subsequent policies are implemented that allow telehealth to reach its full potential to reduce disparities.

[30] Peter Wehrwein, *Pandemic Surge in Telehealth Did Not Worsen Healthcare Disparity: Johns Hopkins researchers*, MANAGED HEALTHCARE EXECUTIVE, (May 13, 2022), https://www.managedhealthcareexecutive.com/view/pandemic-surge-in-telehealth-did-not-worsen-healthcare-disparity-johns-hopkins-researchers.

[31] Rebecca E. Anastos-Wallen et. al., *Primary Care Appointment Completion Rates and Telemedicine Utilization Among Black and Non-Black Patients from 2019 to 2020*, TELEMED J E HEALTH, (May 2, 2022), https://pubmed.ncbi.nlm.nih.gov/35501950/.

[32] Elaine C. Khoong, *Policy Considerations to Ensure Telemedicine Equity*, HEALTH AFFAIRS, (May 2022), https://www.healthaffairs.org/doi/abs/10.1377/hlthaff.2022.00300.

2. Utilization, Cost, and Fraud Concerns

State and federal policymakers often speak to inequity concerns connected to telehealth policy expansions, but many comments focus on utilization concerns as well, which is often connected to the perception that policies allowing for the increased use of telehealth will increase utilization, spending, and ultimately healthcare costs. For instance, a report released by the Committee for a Responsible Federal Budget in April of this year details fiscal considerations in relation to the continuation of telehealth flexibilities afforded during the COVID-19 emergency. The article argues that while telehealth has potential for improvements in timely and effective access to care, it also can result in increased utilization and misaligned provider payment incentives, fraud, and abuse. The authors point out that the Congressional Budget Office ("CBO") estimated that a permanent expansion in telehealth could cost Medicare $25 billion over ten years. As such, they urge caution in how telehealth is approached in the realms of utilization, provider incentives and fraud and abuse. The authors ultimately suggest continuing to take a measured and temporary approach to the telehealth flexibilities, suggesting that they be extended for a maximum of two additional years in order to provide time for evaluation and adjustments before policies are made permanent.[33]

> *The tool has to be allowed to be effective, however, and that is where the role of public policy comes in*

Nevertheless, the actual data doesn't generally support that telehealth policy expansions will increase overall utilization or costs. For instance, in a recently posted analysis conducted by researchers at the University of Michigan, Medicare claims data showed a slow decline in telehealth use for evaluation and management ("E&M") codes between its peak in 2020 through the end of 2021.[34] In fact, telehealth made up 50.7 percent of E&M codes in April 2020, and by the end of 2021 it plateaued between 8.5-9.5 percent. Additionally, total number of E&M services were lower in 2020 and in 2021 compared to 2019 indicating that increased use of telehealth did not increase overall claims volume as many feared it would. These results should help mitigate concerns regarding telehealth's impact on overall healthcare utilization as well as worries that it will be over-utilized by providers given the relatively small percent of claims that were received by the end of 2021 for telehealth.

Attention to the potential for fraud connected to expanded telehealth policies has also gained steam over the course of the pandemic. Multiple investigations and studies by the Inspector General for the Department of Health and Human Services ("HHS-OIG") in particular have been of focus to policymakers. Late last year, as part of the nomination of Christi Grimm as Inspector General, the U.S. Senate Committee on Finance asked a number of questions to which HHS-OIG provided official responses for the record ("QFRs"), showcasing not only policymaker concerns and confusion related to telehealth fraud, but the important role of HHS-OIG in terms of the future of telehealth policy. Many of the questions focused on the potential for telehealth fraud, providing an opportunity for HHS-OIG to articulate their existing enforcement work and overarching telehealth oversight strategy, and again clarify the difference between telemarketing fraud or "telefraud" and telehealth fraud.

The QFRs clearly state that in most HHS-OIG telefraud cases to date, the criminals are not engaging in telehealth fraud. Instead, the main target for these schemes is the medically unnecessary ordering of durable medical equipment ("DME"), laboratory tests, and prescriptions. While HHS-OIG says it is aware of allegations of telehealth fraud – billing for a telehealth service that does not occur or upcoding telehealth claims – those are only a small portion of their work. The majority of their enforcement remains around telefraud – aggressive telemarketing scams where bad actors conduct "cold calls" to Medicare beneficiaries to connect them with fraudulent provider orders. In terms of addressing the potential for fraud generally within the system, HHS-OIG suggested the need to increase telehealth literacy amongst patients and disseminating additional compliance and billing materials for providers.[35] It is important that policymakers understand these nuances in relation to telehealth fraud, as its potential in connection to telehealth policy expansions is not as significant as some appear to think.

[33] Committee for a Responsible Federal Budget, *Fiscal Considerations for the Future of Telehealth*, (April 21, 2022), https://www.crfb.org/papers/fiscal-considerations-future-telehealth.

[34] Chad Ellimoottil, *Trends in Telehealth Use by Medicare Fee-For-Service Beneficiaries and Its Impacts on Overall Volume of Healthcare Services,* medRxiv, (June 21, 2022), https://www.medrxiv.org/content/10.1101/2022.06.15.22276468v1.full.

[35] U.S. Senate Committee on Finance, *Official Responses to Questions for the Record in connection with The Senate Committee on Finance's Consideration of the Nomination of Christi A. Grimm to be Inspector General, Department of Health and Human Services*, (September 2021), https://www.finance.senate.gov/imo/media/doc/Official%20Responses%20to%20Questions%20for%20the%20Record%20-%20Nomination%20of%20Christi%20A%20Grimm%20-%20Senate%20Committee%20on%20Finance1.pdf.

C. Policymaker Interests, Privacy, and Abortion Decision Impacts

Some of the main indicators regarding potential long-term telehealth policy and the future of connected care regulation can be found in policymaker interests and comments, as well as the latest current events related to abortion considerations connected to both telehealth and privacy policy. Attention and support from prominent policymakers for making telehealth expansions permanent has been expressed, and generally, the issue of privacy is always a hot topic, with developments and interest in that area further increasing as of late in connection to health privacy policy. The recent Supreme Court ruling overturning *Roe v. Wade* has many looking to telehealth as a potential solution for those seeking abortion care and the federal government has also acted to increase telehealth access and address privacy concerns in that regard.

> ***The QFRs clearly state that in most HHS-OIG telefraud cases to date, the criminals are not engaging in telehealth fraud.***

1. <u>Bipartisan Telehealth Support and Policymaker Privacy Focus</u>

Hundreds of bills exist at both the state and federal levels regarding telehealth. Despite many being unlikely to pass, their introduction by legislators on both sides of the isle showcases there is a large amount of interest and bipartisan support surrounding long-term policies allowing access to care via telehealth. At the federal level, over 200 pieces of telehealth legislation exist[36] not to mention bills that impact connected health, broadband, and privacy issues more broadly. In addition, the Secretary of HHS, Xavier Becerra has been quoted expressing support for telehealth multiple times – even despite CBO estimates that telehealth expansion would increase federal budget costs.[37] A *Politico* article, sent via their email newsletter (subscription required) quoted him as pointing out that wearables can provide cost savings, and that "*the Congressional Budget Office sometimes gets in the way because what they see as a savings may not be what you and I agree [are] a savings… there are some things that on a bipartisan basis we can do that will reduce cost, not just mask the cost.*" In addition, earlier this year, a bipartisan group of 36 Senators and 7 members of the House sent a letter to Congressional leadership supporting permanent telehealth expansions.[38]

In June of this year, a bipartisan group of federal legislators introduced the American Data Privacy and Protection Act, which creates a national standard regarding the collection of consumer data by online companies, giving consumers more rights of the use of their data.[39] According to a House Committee on Energy and Commerce press release on the bill, given its bipartisan and bicameral nature, it is being represented as "the best opportunity to pass a federal data privacy law in decades."[40] The bill does include health information, as well as some exceptions for entities covered by and in compliance with other privacy laws, including HIPAA,[41] but it may still have some ability to overlap with and further complicate similar state laws.

In addition, last year the Federal Trade Commission ("FTC") signaled a focus on further regulating health apps similar to health providers with its statement that apps and connect-

[36] Center for Connected Health Policy, United States Pending Legislation & Regulation, https://www.cchpca.org/federal/pending-legislation/.

[37] Congressional Budget Office, Cost Estimate H.R. 5201, Telemental Health Expansion Act of 2020, (December 4, 2020), https://www.cbo.gov/system/files/2020-12/hr5201.pdf.

[38] United States Senator Brian Schatz et. al., Letter to Congressional Leadership, (January 28, 2022), https://www.feinstein.senate.gov/public/_cache/files/b/6/b6dc8608-24a4-4f7e-bdd9-4d63e143d8d8/C854D318465A3F370874F8F6C96A6388.telehealth-extension-letter.pdf.

[39] *American Data Privacy and Protection Act*, United States House Committee on Energy & Commerce Bill Discussion Draft, https://www.commerce.senate.gov/services/files/6CB3B500-3DB4-4FCC-BB15-9E6A52738B6C.

[40] Press Release, United States House Committee on Energy & Commerce, House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill, (June 3, 2022), https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.

[41] *American Data Privacy and Protection Act, supra* note 38.

ed device companies that collect health information must comply with the FTC's Health Breach Notification Rule.[42] Thereby, while such companies are not directly subject to HIPAA as they are not providers, they may still be regulated as a provider under similar health rules.

> *While such companies are not directly subject to HIPAA as they are not providers, they may still be regulated as a provider under similar health rules*

2. *Dobbs v. Jackson* - Abortion Decision Impact on Telehealth & Privacy

Given the recent *Dobbs v. Jackson* decision by the Supreme Court overrunning *Roe v. Wade*,[43] many are now looking to telehealth as a means to help ease the burden of individuals seeking abortions in states where it may now be illegal. This has further raised concerns related to privacy of information, especially for telehealth companies and providers, as well as patients, that fear personal health information could be tracked through telehealth applications, including whether or not patients have sought an abortion across state lines. Mailing abortion medications only became possible last year due to the easing of FDA medication requirements as a result of the COVID-19 pandemic. According to research from the Guttmacher Institute, even prior to the recent decision, 19 states already prohibited medication abortions by requiring an in-person visit for abortion medication to be prescribed and dispensed.[44]

Post-*Dobbs,* additional states may take similar action. While telemedicine allows individuals in states where abortion is banned to access physicians in states where it is allowed, it is important to note that the place of service is considered to be the physical location of the patient. Therefore, it would be the laws and regulations of the state the patient is physically located in that would apply, including any abortion ban. According to Politico, many physicians are planning to provide abortion services to out-of-state patients if they can.[45] In addition to privacy, this will draw increased focus on state licensure policies and exceptions.

In response, we've already seen related federal policy actions. On June 29th the HHS OCR updated their HIPAA Privacy Rule and Disclosure of Information online guidance for reproductive health. The guidance stresses that, without the individual's express permission, PHI can only be shared in specific situations outlined in law, including when it is required by law, is a disclosure for law enforcement purposes, or is a disclosure to avert a serious threat to health or safety.[46] In all these circumstances, HIPAA permits but does not require a provider to report an individuals' PHI (including abortion status if that is what is being requested). On the same day, OCR also updated online guidance related to privacy and security of health information stored on personal cell phones and tablets, clarifying again that HIPAA rules generally do not protect health information when it is accessed through or stored on a personal cell phone or device, unless the app is provided by a covered HIPAA entity or business associate.[47]

The *Dobbs* decision could lead conservative-leaning states to further restrict telehealth policies related to reimbursement, prescribing, and licensing, not to mention privacy policy impacts. The same may be seen in more progressive states in regard to adopting policies that further increase reproductive access via telehealth as well as privacy protections and potentially licensing flexibilities. Overall, given policymaker investment into promoting telehealth and privacy issues, pushes for additional policy changes appear inevitable at both the federal and state levels.

[42] United States Federal Trade Commission, *State of the Commission On Breaches by Health Apps and Other Connected Devices*, (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[43] *Dobbs v. Jackson*, 945 F.3d 265 (5th Cir. 2019), https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf.

[44] Rachel K. Jones, et. al., *Medication Abortion Now Accounts for More than Half of All US Abortions*, GUTTMACHER INSTITUTE, (February 2022), https://www.guttmacher.org/article/2022/02/medication-abortion-now-accounts-more-half-all-us-abortions.

[45] Ben Leonard, *What's Next for Virtual Abortions Post-Roe*, POLITICO, (June 24, 2022), https://www.politico.com/news/2022/06/24/whats-next-for-virtual-abortions-post-roe-00038085.

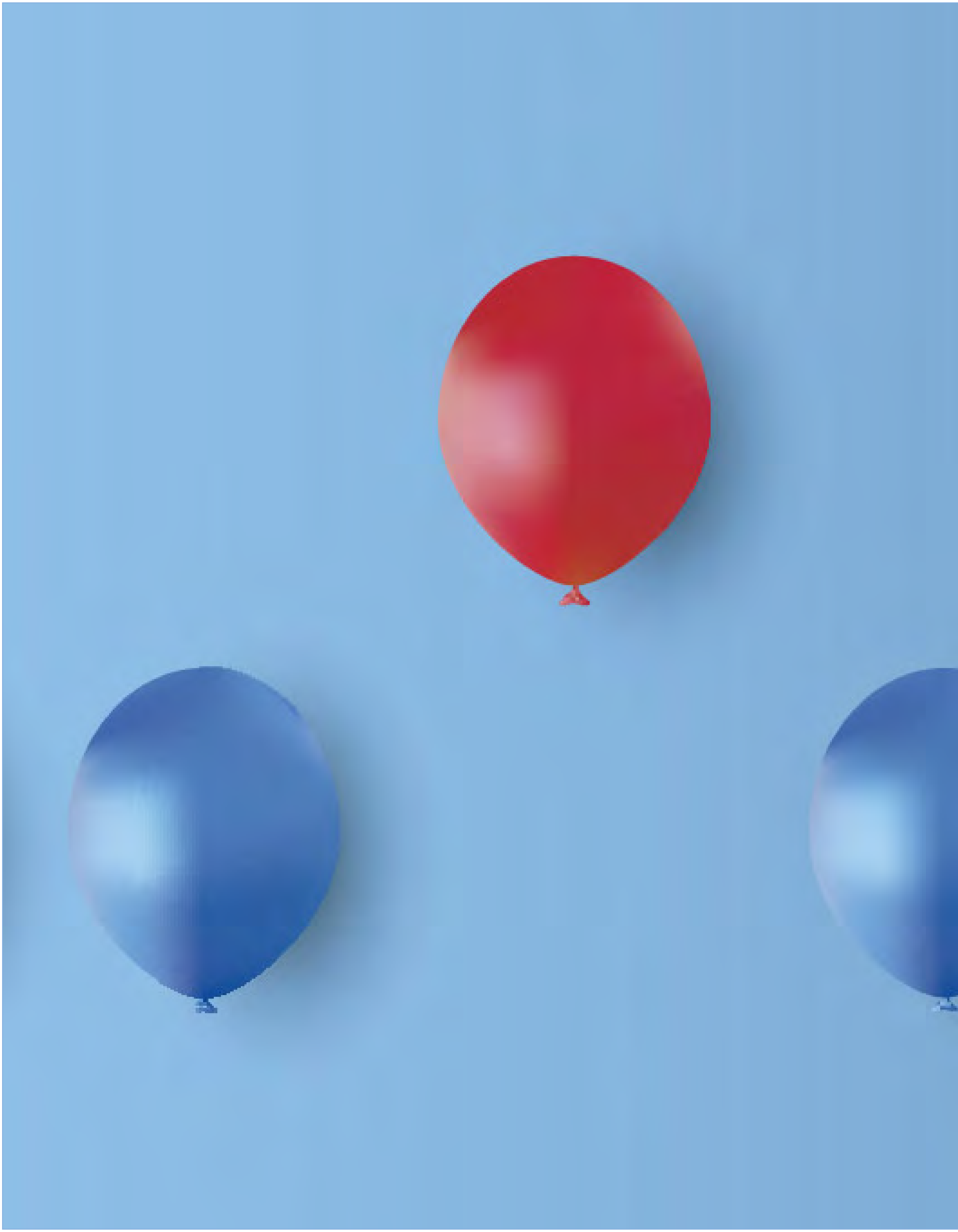
[46] U.S. Department of Health & Human Services, *HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html?source=email.

[47] U.S. Department of Health & Human Services, *Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html?source=email.

03 CONCLUSION

While connected health policies have never been as complicated and subject to change, the ability for telehealth and connected health technologies to improve access and decrease inequities has also never appeared stronger. It remains important to track regulatory efforts and perceptions that contribute to telehealth policy development, including privacy and broadband initiatives, as each is an integral component in ensuring practitioners and patients can provide and receive quality access to care. Moving forward, healthcare stakeholders and policymakers should continue to work together to understand and address remaining barriers while improving communication around available resources to providers and patients. In examining and committing to improve access to connected care long-term, policies could also help usher in some much-needed stability within the country's post-PHE healthcare system. ■

> “*In most cases, this hindrance of competition due to the conduct of any given firm is unlikely to amount to an antitrust contravention*



APPLE HEALTH'S APPROACH TO PATIENT SELF-REPORTED DATA – **A GAME CHANGER OR JUST MORE NOISE?**

BY

DAVID VORAN

Associate Professor, Department(s) of Community and Family Medicine, University of Missouri-Kansas City.

01 INTRODUCTION

Apple's native iPhone Health app is a personal health record enabling a user to passively collect and aggregate data from an ever-expanding number of tracking apps and connected devices into one source for the user to review. Since 2018, the health app has been able to connect with healthcare systems and reference laboratories to pull in clinical information, labs, test results, and office-based measurements. The only requirement was the patient had an active portal account with the source and the healthcare system had enabled the download capability, which over a thousand had done so in the United States. User satisfaction with this capability was quite high in at least one report.

With iOS 15 and higher, people could now begin sharing select data in their Health App to share with other people and their physicians. Some feel this may be the sleeper hit of iOS 15.[2] Simultaneously, Apple released application programing interfaces ("APIs") that enabled providers in healthcare organizations to open a Physician's Dashboard to view the patient's self-reported information found in the Health app. The current version includes three views of the patient: a summary of data over the last year (Figure 1); a more detailed wellness view (Figure 2); and a lab view (Figure 3).

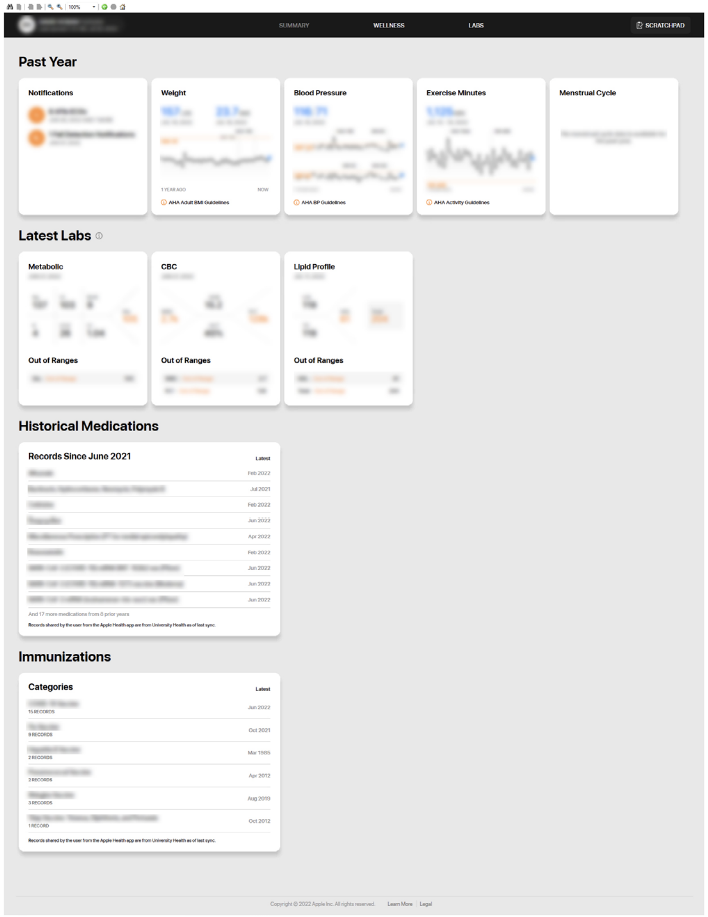


Figure 1. iOS 15.x Summary View in the Physician Dashboard

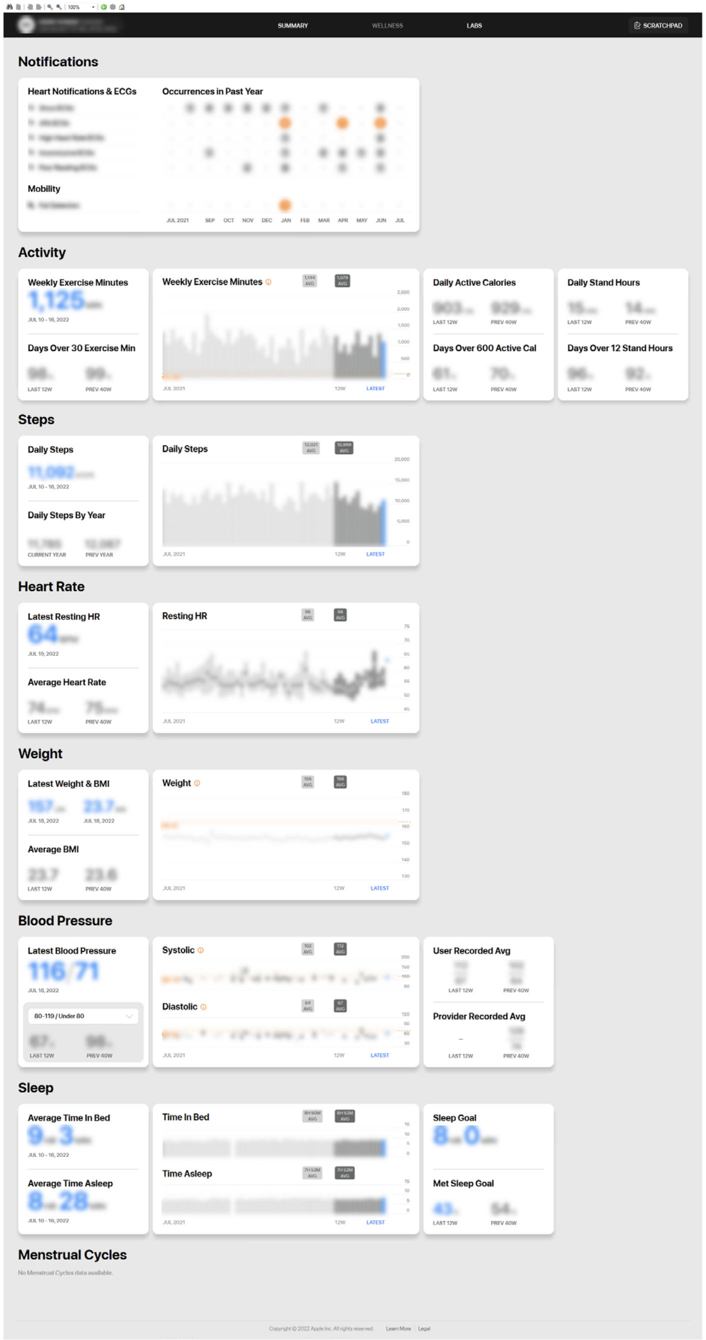
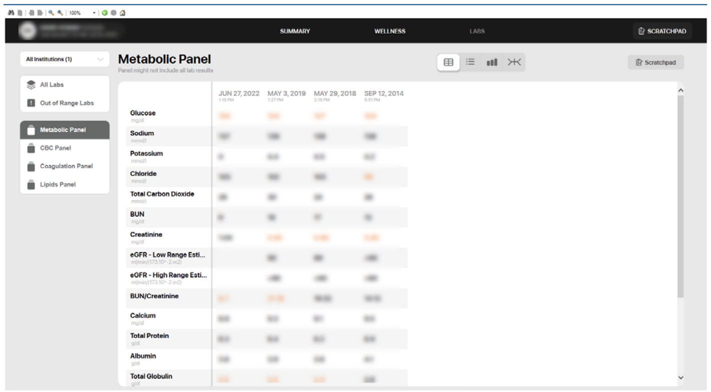


Figure 2. iOS 15.x Wellness View in the Physician's Dashboard

[2] Fitzpatrick A. Why Apple's Health App Could Be the Sleeper Hit of iOS 15. *Time.com*. September 2021:N.PAG. Accessed July 21, 2022.

Figure 3. iOS 15.x Lab View in the Physician's Dashboard

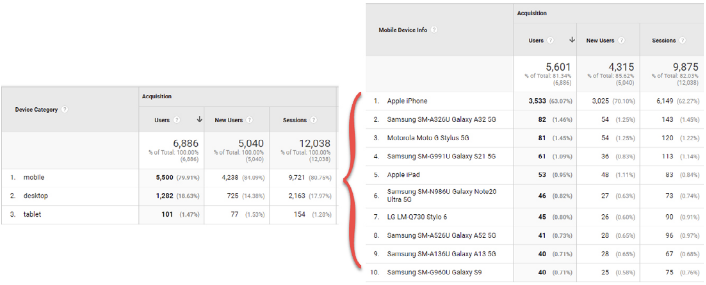


The summary view provides a high-level view what's happened to the patient over the last year and has tiles that contain notifications, most recent labs, historical medications, and immunizations if the connected person chooses to share those items with their physicians. The Wellness section contains notifications, activity, steps, heart rate, weight, blood pressures, sleep, and menstrual cycles. Finally, there's a lab section that will show all labs the person has received from any healthcare system or reference lab into which they have an active, connected portal account. This information can be very useful in helping patients with their chronic conditions since most chronic conditions have a large lifestyle component and many patients with chronic conditions receive medical care from disparate healthcare systems, physicians, and reference labs dependent on their insurance plans.

Surprisingly, this capability has not been widely advertised and many patients and physicians are totally unaware of this type of connectivity. This is true even for organizations, like the one I work in, where most physicians do not even thing to look or select an item called "Self-Reported Data" when reviewing a chart in preparation for a patient visit. Every physician sees a growing number of iPhone patients are using many lifestyle and activity related apps and even wearing devices and have devices at home that track a variety of activities, record weights, blood pressures, blood sugars, and sleeping patterns that would be extremely useful in managing their patient's chronic diseases but are often totally blind to the type of devices their patients are seen using in the exam rooms. Likewise, very few iPhone using patients are aware of the native Health app, let alone its ability to connect with their physician's healthcare system.

Smart phones are the predominant connectivity device most patients use. This is especially true at University Health Kansas City, one of Missouri's safety net hospitals serving both the Kansas City inner core and eastern Jackson County. A large percentage of our patients are underserved on several levels and nearly half of our patients either have no insurance or covered by Medicaid. Yet very few patients we see do not carry with them a smart phone. Seventy-six percent (67 percent) of University Health Kansas City's active portal accounts are reached using mobile devices and 50 percent of those users are using Apple's iPhones with the remainder using one of many types of devices running one of several Android software versions. (Figure 4)[3] We have also seen a growing number of patients wearing Apple watches that significantly enhance the data available in the Health App for sharing.

Figure 4. Google Analytics for University Health Kansas City



Device Category	Acquisition		
	Users	New Users	Sessions
	6,886 % of Total: 100.00% (6,886)	5,040 % of Total: 100.00% (5,040)	12,038 % of Total: 100.00% (12,038)
1. mobile	5,500 (79.91%)	4,238 (84.09%)	9,721 (80.75%)
2. desktop	1,282 (18.63%)	725 (14.38%)	2,163 (17.97%)
3. tablet	101 (1.47%)	77 (1.53%)	154 (1.28%)

Mobile Device Info	Acquisition		
	Users	New Users	Sessions
	5,601 % of Total: 81.34% (6,886)	4,315 % of Total: 85.62% (5,040)	9,875 % of Total: 82.03% (12,038)
1. Apple iPhone	3,533 (63.07%)	3,025 (70.10%)	6,149 (62.27%)
2. Samsung SM-A326U Galaxy A32 5G	82 (1.46%)	54 (1.25%)	143 (1.45%)
3. Motorola Moto G Stylus 5G	81 (1.45%)	54 (1.25%)	120 (1.22%)
4. Samsung SM-G991U Galaxy S21 5G	61 (1.09%)	36 (0.83%)	113 (1.14%)
5. Apple iPad	53 (0.95%)	48 (1.11%)	83 (0.84%)
6. Samsung SM-N986U Galaxy Note20 Ultra 5G	46 (0.82%)	27 (0.63%)	73 (0.74%)
7. LG LM-Q730 Stylo 6	45 (0.80%)	26 (0.60%)	90 (0.91%)
8. Samsung SM-A526U Galaxy A52 5G	41 (0.73%)	28 (0.65%)	96 (0.97%)
9. Samsung SM-A136U Galaxy A13 5G	40 (0.71%)	28 (0.65%)	67 (0.68%)
10. Samsung SM-G960U Galaxy S9	40 (0.71%)	25 (0.58%)	75 (0.76%)

Over the last year we have introduced many patients to the Physician's Dashboard and the sharing capabilities of the Health App. It's not unusual for most patients to say they were neither aware of the app, nor its ability to get daily feeds from their healthcare providers. Many also were not aware this app, a native iOS app on all iPhones, could be configured to communicate with many other applications and devices they were using including fitness trackers, watches, scales, thermometers, home blood pressure monitors, and other consumer devices. Often, when these applications were installed, the default setting was to connect with the Health app and were already populating the Health app with data. Most patients that could turn on the sharing feature of the Health app (i.e. those with active portal accounts) were pleasantly surprised at how much information they could see without having to do any further customization.

Additionally, most of the patients, even some that were using the app were not taking advantage of its ability to download a host of information from over thousands of hospitals, clinics, and labs if the user has an active patient portal that has been connected to Apple Health. They usually express surprise and relief at not having to log into their portal accounts in order to review their most recent labs.

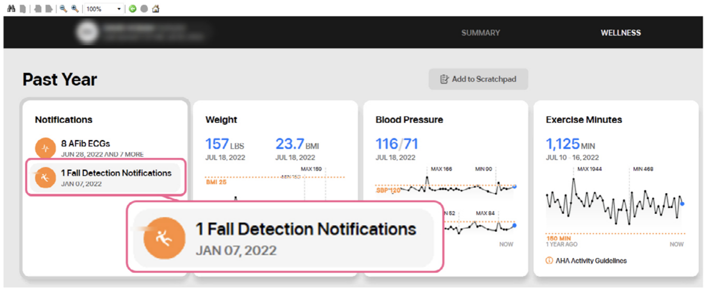
This lack of knowledge on both the patients and the physicians contributes to the inefficient and time-consuming interactions that are crammed into ever decreasing office visit schedules.

[3] Google Analytics for University Health Kansas City, accessed 7/20/2022.

Over the last year most iPhone touting patients introduced to this capability have turned this feature on. For those with existing active portal accounts, this process takes just a few minutes and then enables the physician and the patient to look at a very simple dashboard that has the potential to greatly enhance the office visit experience. This has led to some very interesting anecdotes.

For example, recently, a normally healthy patient presented to the clinic complaining of vague headaches and mild disorientation and came to us for diagnosis. Fortunately, this patient had turned on sharing and had religiously worn his Apple Watch. The Physician Dashboard was brought up on the examination room computer. Immediately both the patient and physician noticed a fall notification that correlated with the onset of a headache which the patient had totally forgotten (Figure 5).

Figure 5. Fall detection



This led to a quick diagnosis of post-concussion syndrome that otherwise might have been missed. Additionally, the physician's dashboard showed other life-style changes including a change in sleeping patterns and activity following this episode including one episode of atrial fibrillation that changed the follow-up of this patient with potential optimizations of future care.

First, accuracy and integrity. The majority of tracking apps, sleep monitors, and other sundry devices that can be connected to the Health app do not fall into any of the 3 FDA health monitoring classes with only 10 percent of monitoring equipment achieving the most stringent Class 3 approval.[4] Many consumer devices do not even attempt to obtain FDA approval yet will connect and send data to the Health app. Some of these, like wrist or finger-based blood pressure cuffs have a much larger variation in results than upper arm cuffs. The same can be said for temperature monitors, many of which are contactless. These variations are offset by the ease at which many measurements can be taken so volume of data does mitigate some errors in individual measurements.

Secondly, lack of monitoring. The Health app and Physician Dashboard is not designed to provide remote monitoring services, where there is a monitoring agency that alerts clinicians to abnormal values requiring interventions. There is no Apple provided list of patients who have enabled sharing. Even when lists of patients are created, there is no guarantee the patient will not turn off sharing. In fact, this has been the case among my own patients. I did maintain a list of patients that had at one time or another turned on sharing. I stopped maintaining this list of more than 20 patients when nearly a 3rd had already turned off sharing after a few months. Does even having access to this information at the patient level increase a physician's liability? Are patients fully instructed and reminded this data is not being monitored? Or will they assume that since their information appears in the chart there is some type of monitoring? Should we be obtaining consent forms from patients who share their information?

Third, while Apple is known for its data privacy, this cannot be assumed for the many apps a patient may use to feed the Health app. This elevates a person's privacy risk and has been documented for some time now.[5] Misappropriation of a person's health data and lack of access has also been constant issue, even though the Health app may mitigate some of the person's lack of access to their own data.[6]

Fourth, financial stability. Unlike physician-ordered Remote Patient Monitoring, physicians cannot charge for reviewing this data under most regulations. The 2021 Medicare Physician Fee Schedule expanded time-based billing for patient visits that allows time spent reviewing patient-derived information, but only on the day of the visit.[7] Unlike Remote Patient Monitoring or Chronic Condition Management, the current regulations are not clear about billing for time spent reviewing and responding to this information between encounters, even though this treasure trove of data is much

[4] PR Newswire. Wearable Consumer-Grade Health Monitors May Work, Yet Diagnostic FDA Approved Devices Still Gold Standard for Heart Arrhythmia Diagnosis. *PR Newswire US*. August 25, 2021. Accessed July 21, 2022. https://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=bwh&AN=202108250905PR.NEWS.USPR.UN85793&site=eds-live&scope=site.

[5] Owen Trip. Risks of Mobile Health Apps. Benefits Magazine, March 2015

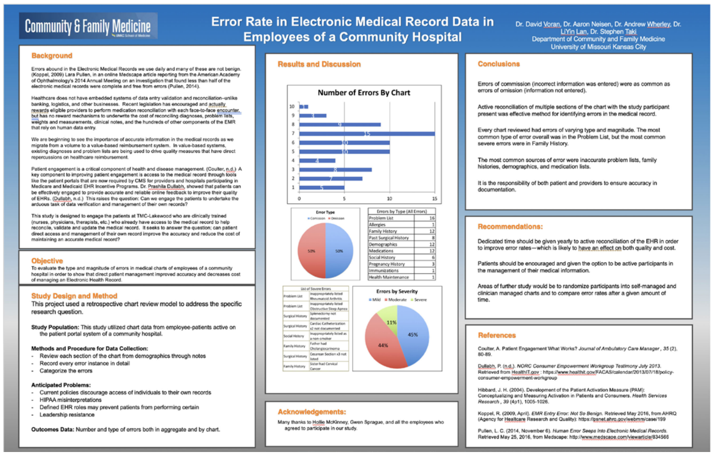
[6] Choe EK(1), Kim Y(2), Lee B(3). Investigating data accessibility of personal health apps. *Journal of the American Medical Informatics Association*. 26(5):412-419. doi:10.1093/jamia/ocz003.

[7] https://www.cms.gov/medicaremedicare-fee-service-paymentphysicianfeeschedpfs-federal-regulation-notices/cms-1734-f last accessed 7/21/2022.

more robust and comprehensive than most Remote Patient Monitoring services. Will the availability and upcoming enhancements to the Health app sharing undermine current Remote Patient Monitoring and Chronic Condition Management services that, at least for Medicare Beneficiaries, are reimbursed at financially sustainable levels?

Fifth, time. The electronic medical record used by most physicians contains an overwhelming amount of information on patients that should be reviewed and reconciled on each visit according to standard best practice recommendations. But this task, done properly, would exceed the time allocated to office visits. Even medication reconciliation can be very time-consuming and complicated, particular when the patient is being seen by multiple physicians and also consuming over-the-counter medications. Nearly 100 percent of charts contain errors; 50 percent of which are errors of omission and equal 50 percent errors of commission. (Figure 6)[8]

Figure 6. Poster on Error Rates in the EHR



Community & Family Medicine

UMKC School of Medicine

Error Rate in Electronic Medical Record Data in Employees of a Community Hospital

Dr. David Voran, Dr. Aaron Neisen, Dr. Andrew Wherley, Dr. LiYin Lan, Dr. Stephen Taki
Department of Community and Family Medicine
University of Missouri Kansas City

Background

Errors abound in the Electronic Medical Records we use daily and many of these are not benign. (Koppel, 2009) Lara Pullen, in an online Medscape article reporting from the American Academy of Ophthalmology's 2014 Annual Meeting on an investigation that found less than half of the electronic medical records were complete and free from errors (Pullen, 2014).

Healthcare does not have embedded systems of data entry validation and reconciliation–unlike banking, logistics, and other businesses. Recent legislation has encouraged and actually rewards eligible providers to perform medication reconciliation with each face-to-face encounter, but has no reward mechanisms to underwrite the cost of reconciling diagnoses, problem lists, weights and measurements, clinical notes, and the hundreds of other components of the EMR that rely on human data entry.

We are beginning to see the importance of accurate information in the medical records as we migrate from a volume to a value-based reimbursement system. In value-based systems, existing diagnoses and problem lists are being used to drive quality measures that have direct repercussions on healthcare reimbursement.

Patient engagement is a critical component of health and disease management. (Coulter, n.d.) A key component to improving patient engagement is access to the medical record through tools like the patient portals that are now required by CMS for providers and hospitals participating in Medicare and Medicaid EHR Incentive Programs. Dr. Prashila Dullabh, showed that patients can be effectively engaged to provide accurate and reliable online feedback to improve their quality of EHRs. (Dullabh, n.d.) This raises the question: Can we engage the patients to undertake the arduous task of data verification and management of their own records?

This study is designed to engage the patients at TMC-Lakewood who are clinically trained (nurses, physicians, therapists, etc.) who already have access to the medical record to help reconcile, validate and update the medical record. It seeks to answer the question; can patient direct access and management of their own record improve the accuracy and reduce the cost of maintaining an accurate medical record?

Objective

To evaluate the type and magnitude of errors in medical charts of employees of a community hospital in order to show that direct patient management improved accuracy and decreases cost of managing an Electronic Health Record.

Study Design and Method

This project used a retrospective chart review model to address the specific research question.

Study Population: This study utilized chart data from employee-patients active on the patient portal system of a community hospital.

Methods and Procedure for Data Collection:
- Review each section of the chart from demographics through notes
- Record every error instance in detail
- Categorize the errors

Anticipated Problems:
- Current policies discourage access of individuals to their own records
- HIPAA misinterpretations
- Defined EHR roles may prevent patients from performing certain
- Leadership resistance

Outcomes Data: Number and type of errors both in aggregate and by chart.

Results and Discussion

Errors by Type (All Errors)	
Problem List	16
Allergies	1
Family History	12
Past Surgical History	8
Demographics	12
Medications	12
Social History	6
Pregnancy History	3
Immunizations	1
Health Maintenance	1

List of Severe Errors	
Problem List	Inappropriately listed Rheumatoid Arthritis
Problem List	Inappropriately listed Obstructive Sleep Apnea
Surgical History	Splenectomy not documented
Surgical History	Cardiac Catheterization x2 not documented
Social History	Inappropriately listed as a non-smoker
Family History	Father had Cholangiocarinoma
Surgical History	Cesarean Section x3 not listed
Family History	Sister had Cervical Cancer

Acknowledgements:

Many thanks to Hollie McKinney, Gwen Sprague, and all the employees who agreed to participate in our study.

Conclusions

Errors of commission (incorrect information was entered) were as common as errors of omission (information not entered).

Active reconciliation of multiple sections of the chart with the study participant present was effective method for identifying errors in the medical record.

Every chart reviewed had errors of varying type and magnitude. The most common type of error overall was in the Problem List, but the most common severe errors were in Family History.

The most common sources of error were inaccurate problem lists, family histories, demographics, and medication lists.

It is the responsibility of both patient and providers to ensure accuracy in documentation.

Recommendations:

Dedicated time should be given yearly to active reconciliation of the EHR in order to improve error rates—which is likely to have an effect on both quality and cost.

Patients should be encouraged and given the option to be active participants in the management of their medical information.

Areas of further study would be to randomize participants into self-managed and clinician managed charts and to compare error rates after a given amount of time.

References

Coulter, A. Patient Engagement What Works? *Journal of Ambulatory Care Manager* , *35* (2), 80-89.

Dullabh, P. (n.d.). *NORC Consumer Empowerment Workgroup Testimony July 2013.* Retrieved from HealthIT.gov : https://www.healthit.gov/FACAS/calendar/2013/07/18/policy-consumer-empowerment-workgroup

Hibbard, J. H. (2004). Development of the Patient Activation Measure (PAM): Conceptualizing and Measuring Activation in Patients and Consumers. *Health Services Research* , *39* (4p1), 1005-1026.

Koppel, R. (2009, April). *EMR Entry Error: Not So Benign.* Retrieved May 2016, from AHRQ (Agency for Healtcare Research and Quality): https://psnet.ahrq.gov/webmm/case/199

Pullen, L. C. (2014, November 6). *Human Error Seeps Into Electronic Medical Records.* Retrieved May 25, 2016, from Medscape: http://www.medscape.com/viewarticle/834566

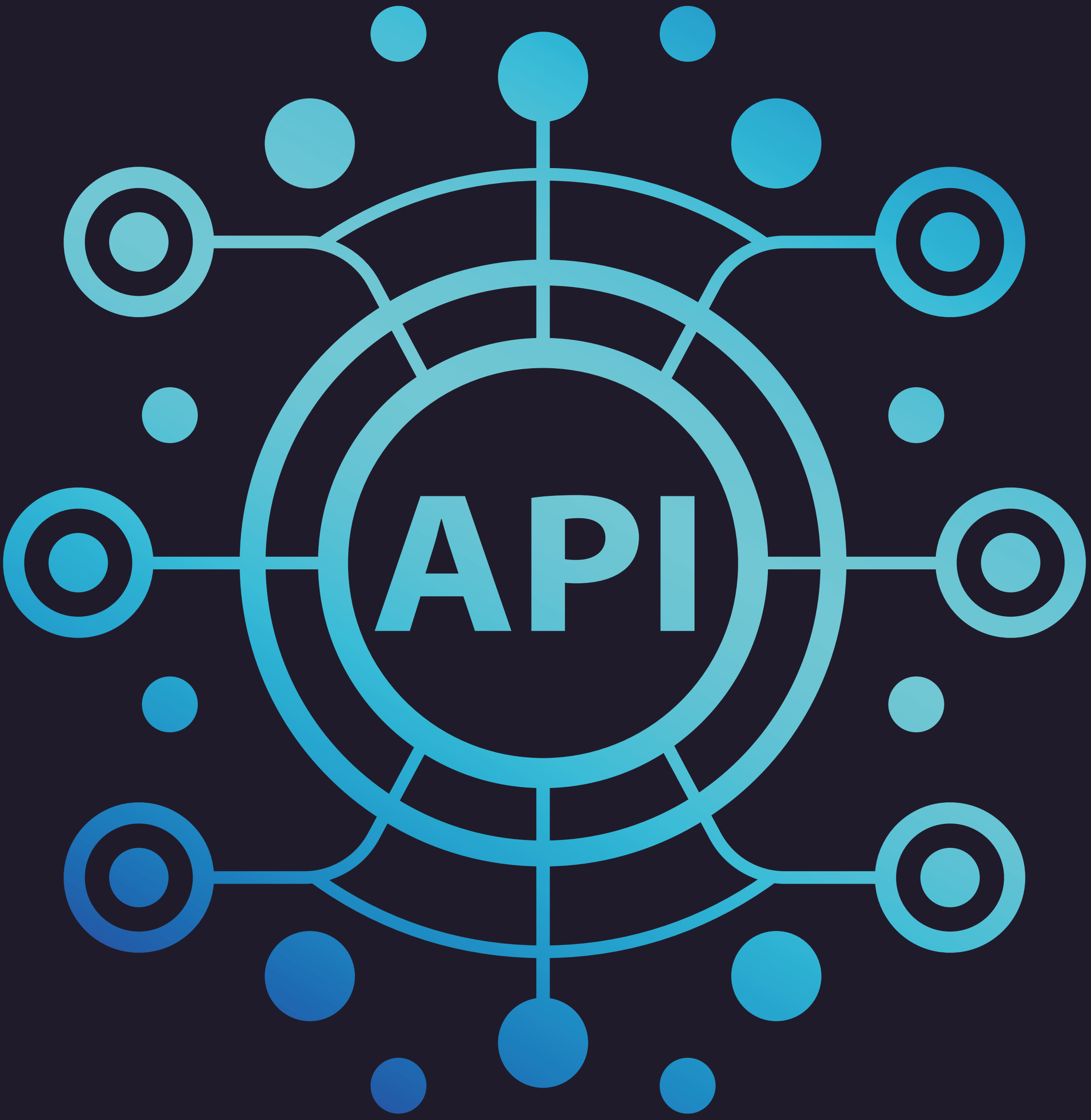
Correcting these errors is very time-consuming and, for the most part, can only be done with the physician and patient together. Will adding access to another whole layer of data that may open up a Pandora's Box of new sources of error add to the inaccuracies that already exist in the record due to the lack of time to review, manage, and reconcile this data?

Physicians experience a wide scope of training that enables them to see and treat most conditions patients present. We Physicians are life-long learners and are well trained to locate and learn from the scientific literature. What we are not trained to do is extract information from our EHRs and haven't embraced using social media "big data" to enhance our ability to answer questions our patients may have. We are even less aware of nor have been trained to utilize an ever-expanding source of information derived from apps, trackers, other wearables, and even data from the patient's beds. The ability to do so is in the hands of patients in the Apple ecosystem but will certainly advance to all platforms and may wind up being one of the more important resources available to us. In addition to paying very close attention to patients during our exams, it is also important that we pay attention to the types of devices a patient is wearing and using. They may be one of the most potent tools in our diagnostic armament soon. However, this type of patient-controlled information has the potential to overwhelm physicians, even more than they are now and raises many concerns.

Will this wind up being a game changer providing information that can be used to educate, motivate, and instruct patients to improve their management of their health and of their chronic conditions? Or will this but tool but one more layer of complexity that winds up being flotsam in the wake of our lives? ■

> ***"Correcting these errors is very time-consuming and, for the most part, can only be done with the physician and patient together***

[8] Aaron Neison, Andrew Wherley, LiYin Lan, Stephen Taki & David Voran. Error Rate in Electronic Medical Record Data in Employees of a Community Hospital. Poster presented at the Annual Scientific Exhibit, 2019.


API

CONNECTING THE MODERN WORLD OF APIs TO LEGACY HEALTHCARE INFRASTRUCTURE

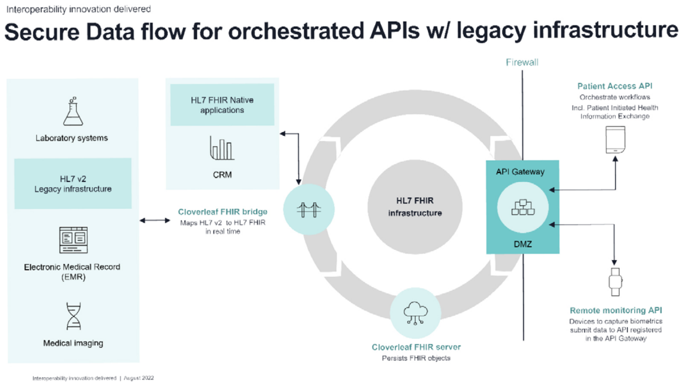
BY

HEINZ JOERG SCHWARZ

Professor Joerg Schwarz is currently Senior Director for Healthcare Interoperability Solutions and Strategy at Infor with over 25 years of experience in the Healthcare Industry and in the interoperability space specifically.

01 INTRODUCTION

The meaning of "Connected Healthcare" is constantly evolving. In the late 1980s and early 1990s, when Health Level Seven ("HL7") was launched, connected healthcare essentially meant that essential patient information could be exchanged between the patient registration system and the laboratory and radiology system. Fast forward to 2022, and we are still using primarily HL7 v2, a standard that was first published in 1988, to transact over 90 percent of healthcare data transactions among hundreds of applications in thousands of organizations worldwide. In an environment where value-based care gains momentum elevating the value of data higher and higher, connected healthcare now means not only connecting all the essential information systems inside of an organization, but beyond those organizational boundaries across different providers of healthcare and social services (Social Determinants of Health). This article will highlight how the legacy HL7 v2 infrastructure still predominant today can be utilized as the foundation for the next generation of connected healthcare, which includes remote patient monitoring for Hospital@Home programs and even a modern digital healthcare shopping experience for consumers. Essential for these modern services are HL7 Fast Healthcare Interoperability Resources ("FHIR") translations and API orchestration that work seamlessly in conjunction with the extant legacy infrastructure. The good news is that this evolution is very doable, and disruptive and costly rip-and-replace can be avoided in most cases.


Interoperability innovation delivered

Secure Data flow for orchestrated APIs w/ legacy infrastructure

Interoperability innovation delivered | August 2022

02

CONNECTING LEGACY INFRASTRUCTURE TO MEET THE DEMANDS OF TODAY

Hundreds of millions of health care data transactions are today still transacted in HL7 v2, a text based, delimited, data exchange standard developed in the 1980s and 1990s to connect laboratory and medical imaging systems to the patient registration systems of the time. The standard is relatively simple and allows transactions via file transfer relatively easily. Many organizations have scalable and reliable infrastructure in place to connect hundreds of applications using an HL7 integration engine, such as Infor's Cloverleaf as the #1 installed solution in the U.S and internationally.

However, HL7 v2 is not appropriate for the needs of contemporary healthcare systems anymore. While the structure of HL7 messages is well defined, the payload of HL7 messages can vary from organization to organization, so when someone needs to aggregate data that originates from multiple sites, it gets tricky very quickly. Is gender coded as a binary value (0 or 1, 1 or 2, F or M), or are there even more options? This variability is not good for data analytics. HL7 v2 is also not a good standard for responsive web-services. Instead of pinging an information source for a particular piece of information, the information sending systems sends out messages that then are forwarded. A modern, responsive webservice would require that the recipients ping the source for a piece of information and then receive a response with that exact information (or a message that the information is not available). This all can be accomplished with HL7 FHIR, a modern standard first published in 2012.

03

CONNECTING HL7 FHIR WITH LEGACY SYSTEMS

Many healthcare organizations intent to build user responsive, consumer centric web interfaces that allow potential patients to interact, submit information, schedule appointments, upload data and even conduct televisits through the Internet. This set of functionalities became especially popular during the COVID-19 pandemic and is often termed "Digital Front-Door." Patients like this type of consumer style engagement and it will remain a requirement long after the pandemic. As described before, HL7 v2 is not the best infrastructure to build this responsive consumer interaction, and the Electronic Health Record System ("EHR") neither has all the data, nor all the functionality to provide this front-end, either. Organizations often utilize CRM systems to keep track of patients with chronic conditions, they utilize advanced medical imaging procedures, and they want to support patients at home with remote monitoring devices. All of this can be accomplished by combining the new HL7 FHIR infrastructure with the existing legacy infrastructure.

Key components to make this seamless integration possible are an API Gateway,[2] a FHIR Server,[3] and a FHIR Bridge.[4] The API Gateway is installed in a DMZ that shields outside access from the network that connects all internal systems. APIs that allow for example triaging consumers requests for appropriate follow up in chat bots, or APIs that collect Internet of things ("IOT") data from patients are registered with the API Gateway and are isolated in isolated network environments that allow access to only limited resources. If either of these applications need information about a patient, that information request is routed as a FHIR resource request to the FHIR server, which can respond in real time – essential for applications with user interaction. The FHIR server stores all data received from the interface engine, originally formatted in HL7 v2 and translated by the FHIR Bridge into FHIR resources. A good, full featured FHIR Server will also support subscriptions, which means as soon as updated information becomes available, existing FHIR resources are updated. The FHIR server therefore has the most current data available to respond to requests from APIs interactively and in near real time. Conversely, if the API submits data, it can be persisted in the FHIR server. This is very important for APIs that collect user data, for example from patient monitoring devices. As much of the data will be noise, it requires applications with machine-learning trained algorithms to separate noise from relevant data. Once relevant data is detected, the API can push that data – but not the noise – into the EHR, where care providers can evaluate the data and take further action.

04 REVIEWING USE CASES FOR MODERN CONNECTED HEALTHCARE

A. IOT Devices and Remote Monitoring

IOT devices that can measure a variety of biometric data have become ubiquitous and make remote patient monitoring cost effective. The challenge is to collect the data and integrate it into the existing infrastructure for professional examination and billing. A variety of companies have developed applications that evaluate the incoming data for early detection of potential problems.

One such example is Vironix.ai,[5] which uses data from inexpensive at-home devices to detect pulmonary and cardiac problems that, if left untreated, could lead to severe health escalations. Another example is Medtronic, one of the world's largest medical device manufacturers, which launched Pacemakers[6] that can communicate with the Patient's smart phone to transmit data – but the data needs to be moved from the phone onto the desk of a physician if it is relevant for clinical decision making, and that requires further integration.

> *"IOT devices that can measure a variety of biometric data have become ubiquitous and make remote patient monitoring cost effective*

In value-based care environments it makes sense for care providers, such as Accountable Care Organizations ("ACO") to utilize remote monitoring to capture data from selected cohorts of patients, especially those with elevated risk, to keep them from worsening conditions that might require hospitalization. While remote monitoring is a cost-effective way to collect useful data, the patient can't be the endpoint – the endpoint of this data should be a care provider that can evaluate the data and initiate necessary corrections if and when required.

B. Social Services Integration

It is well understood that social determinants of health ("SoDH") such as housing, transportation, and nutrition have a large impact on health outcomes.[7] Connected Healthcare therefore also requires exchanging information with social services and consideration and mitigation of such factors.

[2] Infor API Gateway: https://www.infor.com/resources/cloverleaf-api-gateway.

[3] Infor FHIR Server: https://www.infor.com/resources/cloverleaf-fhir-server.

[4] Infor Cloverleaf FHIR Bridge: https://www.infor.com/resources/infor-fhir-bridge.

[5] More info on Vironix.ai can be found here: https://www.vironix.ai/.

[6] More info here: https://www.medtronic.com/us-en/mobileapps/patient-caregiver/mycarelink-heart-app-connected-heart-devices.html.

[7] Social Determinants of Health primer: https://www.kff.org/racial-equity-and-health-policy/issue-brief/beyond-health-care-the-role-of-social-determinants-in-promoting-health-and-health-equity/.

One of these factors could be transportation, and one of the integrative actions could be to integrate APIs for transportation providers such as Uber or Lyft, so that care providers can not only schedule an appointment for a patient, but also orchestrate that the patient will be picked up at home for an appointment and brought back home after the appointment. Since these services are in certain cases reimbursable, the integration would not only provide patient address and pickup time to the transportation provider, but also collect the information necessary to file for reimbursement from the insurance carrier.

C. Interactive Payer Integration

The 21st Century Cures Act does not only require providers to share clinical data with patients and other providers: it also requires Payers to exchange data among each other and with the patient. Connected Healthcare can modernize the ancient billing process, usually many months delayed after the clinical episode and transacted in X12, with modern, interactive HL7 FHIR workflows. Rightfully termed "Burden Reduction," a FHIR based dialogue between the provider and the payer can automate the prior authorization workflow that currently requires much manual intervention and communication both on the provider and the payer side.

> *One of these factors could be transportation, and one of the integrative actions could be to integrate APIs for transportation providers such as Uber or Lyft*

In this workflow, a provider that decides a patient requires a follow-up intervention submits a prior-authorization request to a payer, customized for the requirements of the payer for the type of requested procedure. This might require supporting documentation, which can be retrieved from the FHIR Server. The payer system that responds to the pre-authorization request can then not only confirm eligibility, but also check if all required documentation is provided. If something is missing, it can request this information is real time, while the care provider is still inside the patient workflow. On the payer side, the FHIR resources can be mapped into X12, the standard mandated by HIPPA to transact medical claims. All in all, a fully FHIR enabled workflow that interacts on the provider side interactively with the existing HL7 v2 infrastructure and on the Payer side with the existing X12 infrastructure creates a much streamlined process with time and cost savings for both payers and providers.

D. Hospital@Home

Gaining popularity even prior to COVID-19, Hospital@Home concepts have gained momentum in times when Hospitals struggled to keep capacity during the pandemic. The value is that patients who can be monitored and cared for in their own home don't occupy a hospital bed and still can receive hospital quality level care. Remote monitoring is essential in this concept, as are care providers that are able and equipped to travel to various home sites.

Hospital@Home represents a challenge for Connected Healthcare because the network infrastructure of the home is out of the control of the hospital, yet the data that flows from the home needs to end up in the same electronic medical record used inside the hospital. This can be accomplished by installing home hubs that collect and transmit data through mobile hotspots. Utilizing technologies such as the Cloverleaf Secure Courier,[8] intelligent agents that collect and encrypt the data remotely, transmit it to a central collection point on encrypted transmission lines where it can interface with the hospital integration engine, are available to enable this integration both securely and seamlessly.

It should also be mentioned that the scheduling systems and the supply chain system need to support Hospital@Home care delivery models with schedules that consider driving times and supplies that are in mobile units.

05 CONCLUSION

Connected Care is continuously evolving. From its humble beginnings, when the definition of connected care was restricted to connecting the laboratory system to the patient registration system inside a hospital, to today, when it involves collecting data from the patient and their IOT devices, exchanging data with payers in real time, providing hospital-level care at the patient's home, and including social services and social determinants of health, both technology and use cases keep adapting to new paradigms and business models. With the increasing importance of value-based care, the focus has shifted from acute care to prevention, enabled by modern telecommu-

[8] More Information can be found here: https://www.infor.com/resources/infor-cloverleaf-secure-courier.

nications infrastructure and IOT devices. The comforting news is that we have the technology to bridge between the legacy infrastructure built for the older Connected Healthcare paradigm and the modern infrastructure required for contemporary requirements without a costly rip-and-replace. ■

> “*Connected Care is continuously evolving*

TOWARD A SUSTAINABLE HEALTH ECOSYSTEM **FIXED ON THE DEEPEST PROFESSIONAL VALUES**

BY
GABRIËLLE SPEIJER

&
PETER WALGEMOED

Respectively, Radiation-Oncologist, Haga Teaching Hospital; and MBA, Founder CatalyzIT, NL and Founder Carelliance, NL. Thought leaders in health and Information Technology & Communication, sharing the ambition to make the necessary change for an inclusive and democratic society with heart and soul.

01

NEW TECHNOLOGY: DRIVEN BY HUMAN VALUES

Patients and healthcare professionals need to take the lead in technology as digital innovation starts to interfere with human values and needs. It is crucial that they organize together and not leave crucial decisions to other stakeholders, such as the tech industry or governments. All of these stakeholders should adhere to the same values, namely to contribute to health and care, in particular the Hippocratic

Oath. It is getting harder to follow the Hippocratic Oath in the absence of orchestration principles to place human values at the center of information technology and communications ("IT&C") design globally.

02

THE HIPPOCRATIC OATH

The deepest professional value for a doctor is the Hippocratic Oath.[2] In short, it comes down to the promise to entrust the patient and society to the best care and health in confidentiality. Given the technological developments and possibilities in contemporary society, the Hippocratic Oath could look like this:

As a Data Driven Doctor, I will:

- Make health information valuable
- Make health information available for my patient and the knowledge network of colleagues.
- Treat health information confidentially
- Define and Lead Technology & its development

Aiming at the best care and health for my patient and society.

03

CONTEMPORARY CHALLENGES IN HEALTHCARE

In clinical practice globally, the shift from paper was done quite literally: patient records, processes, and workflows suitable for the traditional organizational structures were simply digitized. In retrospect, rethinking the organizational structure in terms of what technology and its advances could offer us as a community seemed not to be a priority. Since technology influences processes, interactions and behavior, it can also freeze them with far-reaching consequences. Problem solving in the day-to-day treadmill of existence instead of back casting and imagining what we really want technology and its expected development to bring us in future has a high cost. As a matter of fact, we have lost sight of the translation of our societal values (including the Hippocratic Oath) into principles for IT&C design. This fundamental aspect of IT&C design is still lacking today, leading to significant challenges in healthcare.

A. Digitiz-ed: Increasing Risk for Health Safety

1. Digitized Paper

In clinical practice it takes the healthcare professional a lot of administrative time and effort to get insight into the health situation of their patient, as clinical information is stored in legacy documentation systems in files, folders, subfolders containing letters, PDFs, notes, workflows, to-do lists, etc. Moreover, the average professional must go through various documentation systems in different clinical practices, hospitals, or other care organizations to gather all the necessary information. To maintain an overview, all of these documents are copied manually into the systema of each healthcare professional and organization. This is an unnecessary, error-prone process leading to potential harms to patient safety, the reliability of healthcare professionals, and energy inefficiency,[3] as well as the need to put in place protection and governance measures to maintain robust resilience concerning cybersecurity.[4]

> "We're building virtual healthcare without foundation, solving today's problems technically, locking healthcare in the past."

2. Digitized Bricks and Mortar

A complete timeline of all records including the essential metadata (e.g. information about the place, the type of diagnostic or treatment machine or tool, the responsible care team members) of a patient's health path is not recorded since when digitizing some decades ago the 'old organization' was simple enough. With growing mobility, patients are visiting more and more clinical practices and with big advances in healthcare like expanding diagnostic

[2] World Medical Association. *The Modern Hippocratic Oath*. (2022). https://www.wma.net/what-we-do/medical-ethics/declaration-of-geneva/.

[3] Robie McKie et. al., *Chaos after heat crashes computers at leading london hospitals*, THE GUARDIAN (Aug 7, 2022), https://amp-theguardian-com.cdn.ampproject.org/c/s/amp.theguardian.com/environment/2022/aug/07/chaos-after-heat-crashes-computers-at-leading-london-hospitals.

[4] R. Quinn, Potential dangers of using technology in healthcare, SOCIETY OF HOSPITAL MANAGEMENT. (Mar 17, 2016), https://www.the-hospitalist.org/hospitalist/article/121825/potential-dangers-using-technology-healthcare.

applications, treatment modalities and superspecialization of healthcare professionals, the complexity of healthcare has increased a lot. The need for a complete timeline of all records will rise further with demand for telehealthcare. Strangely enough, it seems there is a widely held belief ‘the healthcare system’ is taking care of this complete timeline, while in reality there is no governance over this process. As a result, healthcare professionals struggle daily to get the right information on a timely basis. Also, information is difficult to track or may even be hidden away, despite best efforts.

3. Digitized Consent Concerning Access to Information

Considering the approach of how consent on access to information has been managed it simply became a e-translation from paper in recent times. As the world wide web facilitated the spread of information to anyone anywhere, it became a business model for companies. Besides the primary model based on development of services; advertising is still a big part of the revenue. In the meantime, privacy legislations like “HIPAA” (Health Insurance Portability and Accountability Act),[5] “CCPA” (California Consumer Privacy Act),[6] “GDPR” (General Data Protection Regulation)[7] and “PIPL” (Personal Information Protection Law)[8] have been introduced in the U.S., Europe, and China.

As a result, in the consumer market, we see “EULA” (End User License Agreements) of unreasonable sizes and understandability. Applying this to the field of healthcare one might discuss whether ethical to make people sign such agreements in a vulnerable (mental) state. In the healthcare sector we see a twofold reaction. Ignorance of the potential consequences of the importance of personal data protection especially for our professional relationship with the patient. On the other side of the spectrum, we see a reluctance giving access to data when crucial for continuity or advancement of care.

> *Considering the approach of how consent on access to information has been managed it simply became a e-translation from paper in recent times*

Lacking a seamless integration of consent concerning access to data, all sorts of data breaches that can currently be identified: from failure to deliver (on time), loss, unauthorized inspection, to use or misuse for purposes other than primarily providing care without consent, including technology, pharma or market research companies getting access to these sensitive data. Services, drugs, or marketing tools, with or without consent can now be developed in return for services or payment to the healthcare organization or healthcare professional. For Data Protection Authorities (“DPAs”) like the Dutch AP — the independent public authorities applying the GDPR — it is practically impossible to oversee the fundamental right to the protection of personal data.[9] In conclusion, the GDPR is not currently construed according to its intent, which leads to an increasing risk for health safety.

B. No State-of-the-art Technology: No Insight into Overall Health Situation

In healthcare, mainly financial administrative processes are supported digitally, much less the patient characteristics, which determine healthcare professionals' actions and outcomes with their patients. Purchasing of technology in clinical setting is often done after long-term trajectories of (public) procurement processes. These involve risks and uncertainties for suppliers of whom a limited number can survive and finally sign long-term contracts with hospital

[5] Health Insurance Portability and Accountability Act of 1996. https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[6] California Consumer Privacy Act, Cal. Civ. Codes § 1798.199.10, § 1798.199.10(a), § 1798.185(d), § 1798.199.10(a), § 1798.199.15(a), § 1798.155(a), § 1798.199.45(a). https://privacyrights.org/resources/california-privacy-rights-act-overview.

[7] General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (*Apr 26, 2016), https://gdpr.eu/.

[8] Personal Information Protection law. Nov 2020. https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

[9] Dutch Data Protection Authority, *necessary AP growth to protect citizens in digitizing Netherlands,* P356 (Nov 11,2020), https://www.privacy365.eu/en/by-the-dutch-data-protection-authority-necessary-ap-growth-to-protect-citizens-in-digitising-netherlands/.

management, receiving a privileged status.[10] As regulatory requirements become more intense, such as "MDR" (Medical Device Regulation), CE / FDA certification, and the EU AI Act,[11] they tend to slow down innovation even further when applied within these existing and cumbersome organizations.

> "Today technology imposes thresholds, it's about putting the thresholds on the right places in the system so that we can live up to our values and work together in this."

Since fundamental decisions on the functionality of the technology already have been made in the very beginning of its development, the people who deliver and receive care through it will face the resulting limitations and their clinical consequences. Even with deep knowledge in the field of medical informatics it turns out to be very hard to see through beautiful promises, let alone to foresee the implications of what has been offered and its clinical consequences over time as insight in the deeper layers is lacking before signing agreements.

> *In healthcare, mainly financial administrative processes are supported digitally, much less the patient characteristics, which determine healthcare professionals' actions and outcomes with their patients*

For example, an EHR vendor can claim integrated international standards for semantic interoperability like SNOMED International. Taking a deeper look this can turn out to be a low-value implementation of a limited list of codes for diagnoses and some treatments while eliminating the rich hierarchical structures representing its added value. On the other hand, this co-creative process with continuous input from the clinical side, discussion on what's possible and appropriate from a technical standpoint is crucial to support care safely over time. Standards, certifications, and other regulations are extremely important to deliver safe care, but they can't live up to clinical guidance and continuous validation!

As technology in the consumer market is developing exponentially, the domain of health and leisure applications is growing alongside it. While delivering care with legacy technology in the clinical setting as it shapes up to increasing regulations, these applications are mainly developed outside clinical practices. This means healthcare professionals generally lack information on most of their patients' health characteristics. Consultations still take a central role in healthcare today because it is impossible to harness the power of technology considering all variables like exposome, social graph, genome, microbiome, transcriptome, and metabolome. In short, we are unable to create a continuous insight into the overall health situation of a patient.[12]

> "In the design of the health ecosystem, the patient, who is of course central, is left all alone if we don't orchestrate the doctor with its Hippocratic Oath."

Even more concerning is the emergence of a parallel landscape able to expand driven by advertising and profit, and *not* necessarily following the core value of the Hippocratic Oath or other values like inclusion, justice, equality, solidarity, non-discrimination, or democracy. This holds a potential risk of harm to entire populations. For example, social media platforms can say that they support people with mental problems but may make profit on insights shared by their users. Seriously ill and vulnerable people may miss out on routine care, making them tempting prey for sinister treatments outside the scope of regular licensed and heavily regulated practices. This is a paradoxical situation.

> "The Hippocratic Oath should be deployed across the entire health ecosystem, why should it only apply to doctors, when we share the same purpose?"

C. No Support from Connective Technology: No Learning Health System

Making information available is not digitally supported in the current systems, either among colleagues from the same discipline or across medical disciplines, let alone at the institutional level. Consequently, healthcare professionals are using workarounds to get the information to the right place on time. This is done by phone calls, additional meetings,

[10] KPMG, authority consumer markets (ACM), *The market for EHR systems has been further concentrated in the past ten years; there is little movement due to a limited offer in combination with high transition costs, (2021),* https://www.acm.nl/sites/default/files/documents/market-survey-into-information-systems-and-digital-data-exchange-in-the-hospital-sector.pdf.

[11] Regulation of the European Parliament and of the Council, *Harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts,* SEC (2021) 167 final, SWD (2021) 84 final, SWD (2021) 85 final, (Apr 21, 2021), https://artificialintelligenceact.eu/.

[12] Eric J. Topol, I*ndividualized medicine from prewomb to tomb,* Cell Vol 157, Issue 1, p241-253, 2014, https://www.cell.com/cell/fulltext/S0092-8674%2814%2900204-9.

emails, direct messaging etc. To keep oversight in clinical settings, correspondence is still used (like when working on paper) and archived in all these systems. This leads to unnecessary risks for patient safety, and creates extra administrative work for the physician who would rather spend time with the patient.[13] Moreover, the ability to learn from data is lacking because information can become blocked in certain systems.[14]

D. No Proper Archiving: No Value Creation and Undesired Bias

Every organization and clinical practice have its own processes in place to store patient health information (irrespective of its value) for a period subject to statutory data retention periods until simply deleting it. Data curation, the process in the clinical setting where communication, clinical evaluation, and decision-making take place, determines the value of data. This includes data for its primary use (i.e. its clinical purpose) and for its secondary use (scientific research, the development of services, or pharma, quality, financial or safety analysis).

Efforts made separately from clinical processes, like data cleaning, checks by clinicians on non-current data in individual platforms, and systems or standard data entry forms and boxes for clinicians and patients, can lead to the following issues. First, loss of context over time leads to lower data quality. Second, standardization of data entry forms can lead to selection for information already known, therefore enlarging potential biases in clinical decision making, research, service-, product development and missing potential crucial factors to improve quality, finance, safety, security, energy efficiency, and much more.

E. No Joint Focus on (Cyber)security: Potential Profound Implications for Societal Health

The cybercriminal also seemed to plunge into healthcare recently. Healthcare had the highest number of data breaches of all sectors in 2020. Based on the 2021 Identity Breach Report, the healthcare sector experienced a 51 percent increase in the total volume of records exposed when compared with 2019.[15] Healthcare is threatened by the cybercriminal who operates in a purely financially driven way. The most important areas appeared to be ransomware and disinformation in the era of digital everything, which puts healthcare at great risk. Joint efforts throughout the entire sector to protect from this (new) type of global health threat has never been more urgent. A crucial step in this is collaboration among healthcare professionals making it part of their work ethic.

04

SOLUTION TO SUSTAINABLE HEALTH ECOSYSTEM: A NEW ROADMAP

As described above, big challenges are threatening safe and sustainable health(care) globally while tackling problems in the workspace by fitting in technology seems to even get us further away from what health(care) should and could be. In the early days of the world wide web there was a shared vision of a huge potential to connect everyone's computer anywhere in the world, a democratic model to build up knowledge globally. In the following years, it escaped the attention of the broader public what digital development would imply when you leave it to some parties. From the start of the world wide web (Web 1.0), platforms (Web 2.0) developed. Web 2.0 brought so many conveniences (either for free or in exchange for a subscription fee) that we as a society got used to. We seem not to make a big deal out of the way data should be handled. Data about ourselves, our activities and what we consider as valuable to keep regardless the range of technological applications over time. During the COVID-19 pandemic, we have seen healthcare professionals working longer hours, risking their own health to help patients, while in society there has been a growing trend towards healthcare consumerism and lack of trust. Insight into the expectations and experiences of society and healthcare professionals toward and with each other will be required in order to bridge this gap in the near future.

> "The virtual space for healthcare: fixed on the deepest professional value, the Hippocratic oath and super flexible in all other dimensions."[16]

[13] Atul Gawande. *Why doctors hate their computers*, Annals of Medicine Nov 12, 2018, https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers.

[14] Keneth D Mandell, *Scalable Collaborative Infrastructure for a Learning Healthcare System (SCILHS): Architecture*, J Am Med Inform Assoc. 2014 Jul; 21(4): 615 620, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4078286/.

[15] Constella, 2020 Identity Breach Report, *Weaponized Data Breaches Fueling Identity-based Attacks Across the Globe,* (May 2020), https://info.constellaintelligence.com/2020-identity-breach-report?hsLang=en.

[16] G. Speijer. *What will metaverse offer physicians and patients in the future?* ICT & health International, Jun 28,2022, https://ictandhealth.com/what-will-metaverse-offer-physicians-and-patients-in-the-future/news/.

A. Mindset

Globally, there is a growing awareness of the fact that technological development has such a societal impact.[17] Recently, the European Parliament discussed defending European values, democracy, and fundamental rights in terms of how the Digital Services Act could set the global benchmark for regulating online platforms in the future.[18] [19] European frameworks and legislation are important, and the GDPR provides crucial rights supporting confidentiality in the doctor-patient relationship.

However, a broader sense and understanding of what is necessary and urgent to find a fundamental solution is ahead of us now. While releasing more legislation and regulation it is key to acknowledge there is a window of opportunity now as technology for Web 3.0 is reaching readiness levels allowing us to collectively translate our human values into the design principles for IT&C.[20] This will facilitate the process to keep up with the speed of technological developments and to create frameworks and laws around.[21] In healthcare we must be aware of this crossroads in history as our health is at stake globally now.[22]

Sustainable care is about orchestration of people, processes, and technology. The essence is to be able to provide the best care in confidentiality. This implies the freedom for patients and healthcare professionals to match with each other flexibly, supported with the available insights in order to build upon that trusted connection by knowing about their expectations and experiences with each other. It also means the ability to stack knowledge and insights openly and transparently.

> *However, a broader sense and understanding of what is necessary and urgent to find a fundamental solution is ahead of us now*

This requires a shift in focus from *return on investment* to *return on data* aiming at *return on health*. A learning health system where we can learn from every single patient starts with the mindset of being aware of the societal value of data and the underlying value of the Hippocratic Oath when contributing to the health and care space.

B. Cooperation with Mission

By applying Ostrom's principles for self-governance of communities,[23] [24] and common property, data can gain their genuine value when curated within communities with a shared goal (Commons Based Peer Production[25]) or more solid mission driven communities sharing a long-term purpose (data-driven health lab co-operative)[26] demonstrating that approach equating data to oil is a false, deceptive as-

[17] World Economic Forum, *Responsible use of technology*, Aug 2019, https://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf.

[18] News European Parliament, *Facebook whistle blower testifies in European Parliament*, Nov 9, 2021, https://www.europarl.europa.eu/news/en/headlines/society/20211028STO16120/facebook-whistleblower-testifies-in-european-parliament.

[19] News European Parliament, *Discussion with Frances Haugen on the global impact of digital services act.* May 16, 2022. https://www.europarl.europa.eu/news/en/press-room/20220516IPR29638/discussion-with-frances-haugen-on-the-global-impact-of-the-digital-services-act.

[20] Digital Assembly, Future of the Internet: *The Metaverse and Web3*, (Jun 21-22, 2022) https://digitalassembly2022.captag.events/J4RMT4/#/d/v5qgubZRA8zY3KyrtJqPXdDaEGvXBlMq6WEKb2UcKEM.

[21] Dirk Helbing et. al. *Will Democracy Survive Big Data and Artificial Intelligence?* Feb 25, 2017, https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence.

[22] G. Speijer, *Digital Preparedness of the healthcare sector.* Ch15 p122 Natascha van Duuren, Victor de Pous. Multidisciplinary aspects of COVID-19 apps. KNVI, 2021, 978-90-9034977-0. ffhal-03547444

[23] Beyond Markets and States: Polycentric Governance of Complex Economic Systems, American Econ. Review 100 (June 2010): 641-67 https://web.augsburg.edu/sabo/BeyondMarketsandStatesPolycentricGovernanceofComplexEconomicSystems.pdf.

[24] David Rozas, When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance, Mar 26, 2021, https://journals.sagepub.com/doi/full/10.1177/21582440211002526.

[25] Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press. Online at: https://cyber.harvard.edu/wealth_of_networks/Download_PDFs_of_the_book.

[26] Paul Cerrato & John Halamka, The Digital Reconstruction of Healthcare Transitioning from Brick and Mortar to Virtual Care p120, 2022.

sumption.[27] If data would be treated as oil, it becomes a rival product in a highly profitable and under-regulated data economy, without equal health and fair wealth distribution. It won't automatically match the shared values of our society and specifically the Hippocratic Oath. Similarly to the provisions we have made socially for pure drinking water for all, we will have to orchestrate analogous to how our society takes control when it comes to data and technology in the current technological revolution.[28]

> *This requires a shift in focus from return on investment to return on data aiming at return on health*

Therefore, a more appropriate definition in healthcare might see data equivalent to blood.[29] This would be proper from a moral perspective. However, from a value perspective the definition is incorrect. Because like oil, blood is a finite resource, whereas data are characteristic for their *anti-rivalrous* property, which means opposed to non-rival goods that are not reduced in case of consumption, data even increase. For example, with the same high quality, context-, device and expert-traceable curated dataset a range of diagnoses can be made. For example, with a combination of this and other curated datasets development of drugs or applications like computational models can be done, while a selected dataset can be used to control quality, finance, and process flow. Most valuable data are curated within a cooperative that's driven by a shared long-term mission co-creating and representing stakeholders from the different communities with the right to these data: the citizens (or patients) as *consent holders*, the healthcare professionals and researchers as *knowledge contributors*, the technology developers as *technology orchestrators* and the *data curators* (or *Rentmeester*s).

C. IT&C Principles Empower Right Mindset

Speijer & *Walgemoed* are concretizing these principles toward a sustainable health ecosystem. All principles are needed to design its foundation.

1. Data Rentmeesterschap

The requirement for data curation by design in the orchestration of IT&C is first described as data Rentmeesterschap.[30] This encompasses taking care of data, maintaining, and making it accessible to the stakeholders and future generations on behalf of (healthcare) professionals, researchers and citizen including patients.

The first step starts at the moment of data creation: the consultation or knowledge contribution of the healthcare professional and context of the patient. To provide qualitative data, this needs to be open and therefore highly confidential. This cyber-physical moment of interaction determines the quality of data. In order to turn these data into valuable data it needs to be done in agreement with top performing colleagues in the specific domains of expertise; seamlessly and instantly.

The second step encompasses archiving data for now and later, as an asset on behalf of the team of the healthcare professional and patient with consent of both. This process is highly confidential between the healthcare professional and patient, with them deciding on the level of transparency for primary and secondary use together. This is the foundation for a learning health system: the patient with healthcare professional (data driven doctor) as *trusted link*, both committed to lead with their right to data for health of the individual patient and benefit of society, supported by their trust expert network.

Data curation as described above forms the prerequisite for quality, reliability, provenance, and integrity of data. This process is determining the safety and outcome of care, research, and drug and technology development.

2. Dynamic Informed Consent

Dynamic informed consent is an understandable form that describes what happens to the consent holder's data, its connected technology processors and knowledge contributors using that combination.

3. Data Application Independence and Freedom of Applications

Applications process data. Data is made available independent from the application. In this way data can move freely

[27] World Economic Forum, You may have heard data is the new oil. It's not. Jan 10, 2018, https://www.weforum.org/agenda/2018/01/data-is-not-the-new-oil/.

[28] G. Speijer, our values as a society are reflected in digital developments for me, Data, Cybersecurity and Privacy, Feb 14, 2022, https://www.dcsp.nl/our-values-as-a-society-are-reflected-in-digital-developments-for-me-the-hippocratic-oath/.

[29] Eric Perakslis & Andrea Coravos, Is healthcare data the new blood? The Lancet Digital, Vol 1 issue 1, E8-9, May 1, 2019, https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30001-9/fulltext.

[30] P. Walgemoed, Datarentmeester column, CC-BY 2004, https://datarentmeester.org/staging/index.php/2022/04/28/datarentmeester-welcome/.

across applications and can be curated sustainable. Applications now by design can be exchanged by new and better applications, this drives innovation.

4. Timeline

Recording of all curated data with their metadata and relations over time provide the context. Because knowledge is added during a specific period in time, time traveling shows what happened when and with new developed insights. One can go back in time to see whether these could give you new insights. It now becomes possible to forecast different scenarios. In addition, artificial intelligence can then drive the support on a bigger level. This forms the technical foundation for the learning health system.

> ***The second step encompasses archiving data for now and later, as an asset on behalf of the team of the healthcare professional and patient with consent of both***

5. Translation Engine with Underlying Living Standards [31]

By connecting the knowledge contributors seamlessly and flexibly, international standards for semantic interoperability like SNOMED, RadLex, NANDA or LOINC supra mentioned can be integrated as underlying living standards facilitating them to curate data increasingly faster and better.

6. Self-Sovereign Identity ("SSI") with Verifiable Credentials

For seamless, flexible, and trusted connectivity between the patient and healthcare professional in the virtual space credentialing - showing provenance of the data- is required. Technology based on blockchain can help when interacting digitally in a secure and privacy by design way.

7. Personalized User Experience ("UX")

And since, all applications are processors (they don't keep or control data), the former 'one-size fits all' UX for every single application is now exchanged for a truly personalized virtual space for all processors optimizing over time.

8. Virtual Space

In this virtual environment stepping in and out is easy with freedom of choice as a prerequisite from both sides: the patient and the healthcare professional. Both aiming at the highest level of connectivity and trust. And therefore, health outcomes. Getting insight in the expectations and experiences with each other facilitates this process. Having access to, developing, and selecting the latest and best applications and algorithms. With the ability to specify, improve and kill applications when (potentially) dangerous for safe care delivery or compromising health.

[31] G. Speijer, S. van Sandijk & P. Volkert, *Covid laat belang en waarde SNOMED zien. Elkaar verstaan is de basis.* ICT&health nr 4, 2020 p 64-65.

05

SUSTAINABLE HEALTH ECOSYSTEM GLOBALLY

A prerequisite to develop the sustainable health ecosystem is healthcare professionals together with citizens taking the lead in technology as digital starts with human values and human needs. In this health ecosystem anti-trust law and legislation is embedded in its design. This is also the case for the shared human values and in particular the Hippocratic Oath as a professional value.

> *“Cooperatives with a shared long-term mission yielding curated data will be able to concretize the vision of Ostrom: revealing the anti-rival nature of data and their value for the entire society, instead of being financially beneficial for a small group and mainly being underexploited.”*

Bringing in the maximum potential of everyone’s qualities and insights, continuously. Performing on top of licenses, realizing breakthroughs. For many more people and our future generations to learn and create wisdom on it, exponentially. ■

> “*A prerequisite to develop the sustainable health ecosystem is healthcare professionals together with citizens taking the lead in technology as digital starts with human values and human needs*

PATENT LAW CONSIDERATIONS FOR DRUG DISCOVERY INNOVATIONS UTILIZING ARTIFICIAL INTELLIGENCE

BY
CARL
KUKKONEN

&
PATRICIA
CAMPBELL

&
GURNEET
SINGH

Mr. Kukkonen, Dr. Campbell, and Mr. Singh are intellectual property attorneys at Jones Day. Mr. Kukkonen resides in the San Diego office while Dr. Campbell and Mr. Singh reside in the Silicon Valley office.

01 DRUG DISCOVERY AND ARTIFICIAL INTELLIGENCE

In the pharmaceutical and biopharmaceutical industries, taking a drug to market is a tedious process. For example, to create a drug, scientists first predict one or more combinations of molecules that can be transformed into a drug. Next, scientists perform experiments on each molecular combination to test for efficacy, stability, safety, and other metrics. Many promising molecular combinations fail one or more metrics. This road of trial-and-error experimenting with different molecular combinations can take many years, and cost billions of dollars.

Artificial intelligence ("AI") tools have been proven to substantially reduce the time of trial-and-error experimenting with molecules by trimming the molecules that are not ideal based on historical data. Particularly, AI tools can sift quickly through stores of data and results from decades of laboratory experiments to suggest molecular combinations with the desired characteristics that are optimized for a specific medicinal task. Pharmaceutical companies can fast-track those suggested molecular combinations, also referred to as leads, for determining efficacy, stability, safety, and other metrics. This quickens the process and reduces the investment for finding effective, stable, and safe molecular combinations that can be developed into a drug. AI can help new drugs reach the clinical stage five times faster and cut industry costs by 30 percent.[2]

> *Artificial intelligence ("AI") tools have been proven to substantially reduce the time of trial-and-error experimenting with molecules by trimming the molecules that are not ideal based on historical data*

In addition, AI allows for expeditiously repurposing drugs (also referred to as drug repositioning, reprofiling, or retasking).[3] Drug repurposing is a strategy for identifying new uses for approved or investigational drugs that are outside the scope of the original medical indication.[4] Repurposing qualifies an existing drug directly for Phase II clinical trials, thereby reducing the time and investment otherwise required for drug development. For example, repurposing significantly diminishes expenditures because, for example, the cost of launching a new drug typically amounts to $41.3 million, while relaunching an existing drug typically amounts to only $8.4 million.[5]

For drug discovery and development,[6] AI has accelerated drug screening (including target identification and validation), design (through access to new biology or improved / novel chemistry), validation, and repurposing, among other uses. Drug screening includes prediction of bioactivity and toxicity. Bioactivity, as in the level of binding between a material and living tissue, is a critical factor in determining the effectiveness of a drug molecule. In order to deliver a therapeutic response, drugs must have adequate affinity for target proteins or receptors. Alternatively, a drug that interacts with unintended proteins or receptors can lead to toxicity. AI can measure the binding affinity of a drug based on features measuring similarity between the drug and a target, intended or unintended.[7]

For designing drug molecules, AI can be used to predict the three-dimensional protein structure and ensure the resulting drug is designed in accordance with the chemical environment of a target protein site.[8]

For clinical trial design and monitoring,[9] AI has been used to enroll or select subjects, and to facilitate patient compliance or dropout. Improper patient selection and patient dropout respectively contribute to 86 percent and 30 percent of clinical trial failures.[10] Given the substantial time (about 6 to 7 years) and financial investment dedicated to clinical trials, a clearance rate of only about 10 percent of drug candidates in trial represents a monumental loss to the pharmaceutical industry.[11] AI can improve the success rate by limiting the recruitment of the disease population to patients with the necessary drug targets. For patient dropout, AI has been used to monitor medication intake of schizophrenia patients in a Phase II

[2] http://www.pmlive.com/pharma_intelligence/Has_AI_been_the_key_to_tackling_the_COVID-19_pandemic_1346052.

[3] *Id*.

[4] https://www.nature.com/articles/nrd.2018.168#:~:text=Drug%20repurposing%20(also%20called%20drug,drug%20for%20a%20given%20indication.

[5] https://www.pmlive.com/pharma_intelligence/Has_AI_been_the_key_to_tackling_the_COVID-19_pandemic_1346052.

[6] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7577280/.

[7] *Id*.

[8] *Id*.

[9] *Id*.

[10] *Id*.

[11] *Id*.

trial, which increased the adherence rate of patients by 25 percent and ultimately led to the successful completion of the trial.

AI has also been employed in manufacturing by correlating manufacturing errors to set parameters and by performing various automation functions; in product management by evaluating market positioning criteria, performing market prediction and analysis, and determining product costs; and in quality assurance and quality control through understanding critical process parameters, guiding future production cycles, and regulating in-line quality.

02 PHARMACEUTICAL AND AI PARTNERSHIPS

Over the last five years, interest in and use of AI in several sectors of the pharmaceutical and biopharmaceutical industry has rapidly increased and continues to grow. By the end of 2022, AI-facilitated solutions in the pharmaceutical sector are projected to achieve a revenue of over $2 billion.[12]

The burgeoning interest in AI's applications in pharmaceuticals makes sense as AI can help new drugs reach the clinical stage five times faster and cut industry costs by 30 percent.[13] For example, AI can predict drug-target interactions, which allows for the repurposing of existing drugs.[14] Repurposing qualifies an existing drug directly for Phase II clinical trials. This qualification eliminates the time investment otherwise required for three major stages of drug development namely, drug discovery, the preclinical phase, and Phase I clinical trials. Further, repurposing significantly diminishes expenditures because the cost of launching a new drug typically amounts to $41.3 million, while relaunching an existing drug typically amounts to only $8.4 million.[15]

Traditionally, pharmaceutical companies and AI platform companies have been separate. To enhance speed and reduce cost during drug discovery and development, pharmaceutical-AI partnerships between several industry leaders in the pharmaceutical and AI spaces continue to emerge.

In late 2019, Novartis selected Microsoft as its AI partner in its research on cell and gene-based therapies with the collaboration seeking to speed the process of developing medicines from years to potentially weeks or even days.[16]

At the start of 2022, Sanofi agreed to pay $100 million upfront with a potential $5.2 billion in downstream milestones for rights to up to 15 oncology and immunology drugs to be identified by Exscientia's AI technology.[17] Sanofi also recently, in August 2022, invested in AI-powered drug discovery by inking a $1.2 billion biobucks research collaboration with San Francisco-based Atomwise.[18]

AstraZeneca, GlaxoSmithKline, Biogen, Bayer, and Novartis have similarly entered into deals with Ionis Pharmaceuticals, which has developed a drug discovery platform that targets RNA to create new antisense therapies.[19]

Biopharmaceutical and artificial intelligence partnerships have considerable potential for success and are expected to generate revenues of over $44.5 billion by 2026.[20]

[12] https://www.researchandmarkets.com/reports/4846380/growth-insight-role-of-ai-in-the-pharmaceutical.

[13] https://www.pmlive.com/pharma_intelligence/Has_AI_been_the_key_to_tackling_the_COVID-19_pandemic_1346052.

[14] *Id*.

[15] *Id*.

[16] https://news.microsoft.com/transform/novartis-empowers-scientists-ai-speed-discovery-development-breakthrough-medicines/.

[17] https://endpts.com/sanofi-exscientia-ink-the-next-ai-megadeal-signing-terms-on-a-100m-upfront-pact-with-up-to-15-drugs-on-the-line/.

[18] https://www.fiercebiotech.com/biotech/sanofi-signs-12b-pact-atomwise-latest-high-value-ai-drug-discovery-deal.

[19] https://www.fiercebiotech.com/special-report/top-10-m-a-targets-biotech-for-2022.

[20] https://www.prnewswire.com/news-releases/healthcare-artificial-intelligence-ai-market-size-to-reach-revenues-of-usd-44-5-billion-by-2026--arizton-301435270.html.

03

IMPLICATIONS FOR PATENT LAW

The confluence of AI and pharmaceuticals involve new inventions that can be protected using patent law, implications of which are discussed below.

A. Nonobviousness

One requirement for U.S. patent protection is for the invention to be nonobvious. 35 U.S.C. § 103. Whether an invention is obvious is analyzed through the eyes of a hypothetical person of ordinary skill in the art ("POSITA"). Essentially, if the differences between the invention seeking a patent and the prior art (any materials publicly disclosed prior to the patent's filing date) would have been obvious to a POSITA, the USPTO will not award a patent to the applicant. For example, using a new material like porcelain for a wooden doorknob would be "obvious" to a POSITA. *Hotchkiss v. Greenwood*, 52 U.S. 248 (1850). There must be proof of "more ingenuity and skill . . . than were possessed by an ordinary mechanic acquainted with the business."

In the context of AI-facilitated biopharmaceutical solutions, determining who is the POSITA is not always clear. AI systems require large interdisciplinary teams for programming, training, and perfecting code. Is the POSITA the AI programmer or the technician in the field of the invention? One issue, however, is settled. The Supreme Court has affirmed that the POSITA is not an automaton,[21] so there can be no "AI of ordinary skill in the art."[22]

There are also concerns over whether AI recalibrates the obviousness standard since AI increases what a POSITA has the capacity to recognize as obvious.[23] The American Intellectual Property Law Association posited that what seems nonobvious to a human "could be rather obvious to an artificial intelligence machine because it has the capability to crunch through a bunch of numbers in a very fast period of time and come up with an answer to a problem in minutes that would take a human being a lifetime." The SUNY Research Foundation considered accessibility issues and suspected that accounting for AI's capacity would make it "impossible for everyday inventors without access to artificial intelligence to make a patentable contribution to their respective, far-ranging fields."

B. Inventorship

Under U.S. patent law, inventorship determines patent ownership. There is widespread debate over whether artificial intelligence can be considered an inventor for purposes of securing a patent. A key area of the debate focuses on whether AI is simply a tool or something more. One of the essential criteria for inventorship is conception that goes beyond supplying abstract ideas or merely executing others' ideas.[24] Conception is about abstract thinking, an ability that even the world's most sophisticated forms of AI currently lack.

Computer scientist Stephen Thaler is the human inventor of DABUS, an AI machine that "invented" an improved beverage container and a device for search-and-rescue missions.[25] In 2019, Thaler filed patent applications listing DABUS as the sole inventor for these devices in over a dozen countries and the European Union. With these application, Thaler and his international legal team have argued around the world that AI should be considered an inventor for the purposes of receiving a patent with varying results.

On August 5, 2022, in *Thader v. Vidal*, the U.S. Court of Appeals for the Federal Circuit affirmed that patent inventors must be natural persons, rejecting a technologist's attempt to name an artificial intelligence as the sole inventor on patent applications. In this opinion, the Federal Circuit affirmed actions by lower courts and the U.S. Patent and Trademark Office, holding once again that patent inventors can only be natural persons. The Patent Act defines inventors as "the individual or . . . individuals collectively who invented." 35 U.S.C. § 100(f). As a result, whether "individual" could include non-persons such as an AI was a matter of statutory interpretation, and the analysis was a simple one. Because the Supreme Court has held that an "individual" generally means a human being absent some indication that Congress intended a different meaning, and because the Patent Act offers no such indication, the Federal Circuit held that the statute is unambiguous in restricting inventors to natural persons. Thus, according to the Court, no complicated inquiry into the nature of invention, or the rights of AI, was required.

[21] https://www.westlaw.com/Document/Ie2b011acf72211dbb92c924f6a2d2928/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[22] https://revistajuridica.uprrp.edu/inrev/index.php/2021/10/28/its-time-for-the-ai-patent-the-case-for-an-artificial-intelligence-patent-category/#easy-footnote-bottom-52-3257.

[23] https://news.bloomberglaw.com/ip-law/patents-and-artificial-intelligence-an-obvious-slippery-slope.

[24] https://academic.oup.com/grurint/article/71/4/295/6528412.

[25] *Id*.

In contrast to the U.S., a Federal Court of Australia judge agreed with Thaler,[26] finding that Australian patent provisions do not preclude AI systems from being treated as inventors and opining that failing to recognize AI inventorship would harm innovation. However, Australia's second highest judiciary body, the Federal Court of Australia's Court, realigned Australian patent law with the rest of the world and reversed the lower court's decision.[27] The court referenced language from Australia's highest court that repeatedly used "human action" to define patent eligible subject matter.

In the artificial intelligence and legal communities, the majority viewpoint is that AI techniques are merely tools in a human inventor's hands.[28] While the artificial intelligence community has expressed criticism of the anthropomorphization of AI, some have persuasively argued that AI is simply a tool when a human uses AI to facilitate the inventive process in the same way as one would use any other tool like a microscope.[29] There, the inventor would be the person using the AI, not the individual who developed the AI algorithm. In other words, patent law recognizes an inventor in the individual who engaged in thinking and decision-making to solve problems assisted by AI.[30] That individual would be the researcher or scientists screening, developing, and discovering drugs in the biopharmaceutical context. Not the one who developed the basic AI algorithm of a general-purpose nature. Additionally, if "mere implementation of instructions" would not suffice for a human inventor to be entitled to a patent, AI creating output from human input cannot be a standalone inventor either.

Even if inventorship were to be recognized in AI, the question of ownership would remain. In cases where the patent applicant is different from the inventor, the patent applicant must show it properly obtained ownership from the inventor. This was the case in Thaler's patent applications around the world, listing DABUS as the inventor. An AI machine like DABUS can neither hold title to an invention nor pass title to a patent applicant like Thaler under current U.S. patent law.

> “*Computer scientist Stephen Thaler is the human inventor of DABUS, an AI machine that "invented" an improved beverage container and a device for search-and-rescue missions*

Critics of the world's majority position of inventorship believe that this stance makes AI-facilitated inventions and discoveries unpatentable.[31] Some have suggested turning to trade secrets, which offers the advantages over patents of not requiring public disclosure and retaining protection for unlimited periods of time.[32] As long as an invention can be protected by employing reasonable measures to maintain it as a secret, the trade secret will offer protection. However, this is less appropriate in the pharmaceutical context, where securing FDA approval for a drug requires disclosure of its ingredients, what happened during the clinical trials, and its manufacturing, processing, and packaging, which makes trade secret protection unworkable.[33]

[26] https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2021/2021fca0879.

[27] https://www.law360.com/ip/articles/1483893/australian-appeals-court-says-ai-actually-can-t-get-patents.

[28] https://www.law360.com/ip/articles/1483893/australian-appeals-court-says-ai-actually-can-t-get-patents.

[29] https://www.twobirds.com/en/insights/2019/global/who-owns-an-ai-generated-invention.

[30] *Id*.

[31] https://montrealethics.ai/summoning-a-new-artificial-intelligence-patent-model-in-the-age-of-pandemic/.

[32] https://revistajuridica.uprrp.edu/inrev/index.php/2021/10/28/its-time-for-the-ai-patent-the-case-for-an-artificial-intelligence-patent-category/.

[33] https://www.fda.gov/drugs/types-applications/new-drug-application-nda.

04

ADDITIONAL RECOMMENDATIONS FOR PROTECTING TECHNOLOGICAL ASPECTS OF AI-PHARMA PARTNERSHIPS

Companies should consider the following when strategizing on protecting their AI by way of patents.

First, innovators should have a framework to harvest AI inventions for patenting. For example, it can be helpful to classify and harvest the inventions based on the stage in the AI process. Such stages include, for example:

- building a machine learning ("ML") model (e.g. identifying types of input and output of the ML model and specifying functions to be performed by the ML model),
- obtaining training data for the ML model (which can include training inputs fed into the ML model to train the model, and categories for such training inputs such that the ML model is trained to identify a training input as belonging to a respective category),
- training of the ML model (which is generally an iterative process that determines model weights to optimize some objective function that identifies a training input as belonging to a respective category),
- hosting the trained ML model and providing access to the trained ML model (e.g. hosting the ML model in a cloud and providing remote access to it on a user device),
- deploying the trained ML model to generate a predicted output (e.g. executing the trained ML model on real or live input to predict an output such as a category to which the input belongs), or
- application of the predicted output (e.g. system that takes, as input the predicted output generated by the ML model to perform some further processing).

Second, companies should consider whether their AI innovations are eligible for patenting. The U.S. Supreme Court's decision in *Alice* and subsequent decisions by the Federal Circuit, as well as guidance published by the U.S. Patent and Trademark Office (USPTO), have provided guidance on subject matter eligibility (SME) that applies to AI inventions. Based on this guidance, life-sciences companies should, in general, steer away from merely disclosing mathematic relationships or formulas, mere ideas that can reside within the mind of the inventors, or just ideas of organizing human activity, and should rather, or additionally, focus on technological or computational improvements offered by implementation of their AI innovations.

Third, even if their AI is patent-eligible, innovators should consider whether they should patent the AI or maintain it as a trade secret. To make this determination, companies can consider factors including tenure of protection, public disclosure, investor value, damages, and SME. For tenure, patents have a limited life, which in the U.S. for utility patents is 20 years from the earliest filing date, whereas the trade secrets can be maintained for an indefinite time so long as the companies maintain secrecy. However, given the speed at which technology advances or modifies nowadays, the limits on the tenure do not deter patent protection. Public disclosure can be an important factor for sensitive cases because the patents disclosing AI inventions may become public at some point before the patent even issues. However, for patents being filed only in the U.S., patentees can delay the publication until issuance of the patent by filing a non-publication request. With respect to investor value, patents allow easier ways to analyze and quantify the value of the AI innovations, whereas it is generally more difficult to quantify the value of a trade secret. For damages, there can be high hurdles to prove and obtain patent damages, while monetary relief may be easier to obtain once trade secret misappropriation has been established. From the SME perspective, some AI aspects, such as training data used to train ML models, may not be patent-eligible by itself, and may be better protected by way of trade secrets.

Fourth, if companies pursue patent protection, it is important to consider when to file patents. There has generally been a "land rush" to file AI patents. Given this trend and the fact that most jurisdictions, including the U.S., have a first to file patent system, companies can benefit by filing sooner rather than later.

Fifth, innovators should decide on subject matter to be presented in the patent claims such that it's relatively easy to identify infringement. For example, a technique for training an ensemble of machine learning models for drug discovery purposes might be a candidate for treatment as a trade secret given the potential difficulty of identifying competitor infringement. In other cases, patent protection might be more appropriate if the innovation is consumer facing (e.g. a digital health platform, etc.), can be reverse engineered without much burden, competitors publish their activities, and there are few or no alternative approaches to practicing the invention.

05 CONCLUSION

Artificial intelligence has many valuable applications that can accelerate and reduce the cost of discovery in the biopharmaceutical industry. Upholding patent protections for new AI-facilitated inventions will advance threaten life-saving discoveries and innovation. So long as human ingenuity continues to lead biopharmaceutical development and discovery, with AI as a tool rather than as a replacement for human creativity, patent protection will remain viable and should be pursued strategically. ■

> *Innovators should decide on subject matter to be presented in the patent claims such that it's relatively easy to identify infringement*

WHAT'S **NEXT**

For October 2022, we will feature a TechREG Chronicle focused on issues related to **Behavioral Economics**.

ANNOUNCEMENTS

CPI TechREG CHRONICLES November 2022

For November 2022, we will feature a TechREG Chronicle focused on issues related to **Interoperability**.

Contributions to the TechREG Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI TechREG Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "TechREG Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers in any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

ABOUT **US**

Since 2006, **Competition Policy International** ("CPI") has provided comprehensive resources and continuing education for the global antitrust and competition policy community. Created and managed by leaders in the competition policy community, CPI and CPI TV deliver timely commentary and analysis on antitrust and global competition policy matters through a variety of events, media, and applications.

As of October 2021, CPI forms part of **What's Next Media & Analytics Company** and has teamed up with **PYMNTS**, a global leader for data, news, and insights on innovation in payments and the platforms powering the connected economy.

This partnership will reinforce both CPI's and PYMNTS' coverage of technology regulation, as jurisdictions worldwide tackle the regulation of digital businesses across the connected economy, including questions pertaining to BigTech, FinTech, crypto, healthcare, social media, AI, privacy, and more.

Our partnership is timely. The antitrust world is evolving, and new, specific rules are being developed to regulate the so-called "digital economy." A new wave of regulation will increasingly displace traditional antitrust laws insofar as they apply to certain classes of businesses, including payments, online commerce, and the management of social media and search.

This insight is reflected in the launch of the **TechREG** Chronicle, which brings all these aspects together — combining the strengths and expertise of both CPI and PYMNTS.

Continue reading CPI as we expand the scope of analysis and discussions beyond antitrust-related issues to include Tech Reg news and information, and we are excited for you, our readers, to join us on this journey.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.