



# Increasing access to care: telehealth during COVID-19

David A. Hoffman\*

Corresponding author. E-mail: avid.hoffman@duke.edu

## ABSTRACT<sup>1</sup>

The coronavirus disease 2019 (COVID-19) public health emergency has amplified both the potential value and the challenges with healthcare providers deploying telehealth solutions. As people across the country find ways to stay at home, telehealth preserves an opportunity to obtain necessary healthcare services. Further, telehealth can help individuals avoid COVID-19 infection, free up hospital beds and other resources for those patients most in need, and prevent infected individuals from spreading that infection. Federal and state regulators have recognized this potential of telehealth and have quickly changed a variety of laws and regulations to enable healthcare providers to deploy solutions quickly. These changes can provide lasting benefits for the use of telehealth well after the current crisis. However, to best realize telehealth's benefits, further legal and regulatory actions are necessary. Specifically, lawmakers and regulators should focus on six areas: reimbursement, privacy/cybersecurity, liability, licensure, technology access, and artificial intelligence.

**KEYWORDS:** telehealth, privacy, cybersecurity, COVID, artificial intelligence, telemedicine

## THE GREAT NEED FOR TELEHEALTH

Healthcare providers, academics, and technology developers have advocated for increased use of telehealth for decades. As internet and communications technology has advanced, regulators have incrementally made changes to enable the use of

\* Steed Family Professor of the Practice of cybersecurity policy at Duke University Sanford School of Public Policy, and Associate General Counsel and Global Privacy Officer at Intel Corporation.

1 Many thanks to Nick Galvez, Bonnie Britton, Nita Farahany, Matt Perault, Christina Silcox, Courtney Van Houtven, Jackie Medeck, Ari Schwartz, John Banghart, Justin Sherman, Micalyn Struble, and Alexander Hoffman for reviewing and providing feedback on this paper.

telehealth solutions. The unique impacts of the coronavirus disease 2019 (COVID-19) public health emergency have created an unprecedented amount of regulatory changes for telehealth. These changes should help address the current crisis and provide an opportunity for much needed longer-term evolution of US healthcare delivery to improve health outcomes and lower costs. This paper provides an overview of recent regulatory changes that enable telehealth and proposes additional modifications that will be particularly helpful in the battle against COVID-19 and the future development of telehealth services.

Across the USA as we encourage everyone to stay home, telehealth provides an opportunity to reduce the visits to doctors' offices and hospitals. These reduced visits protect against COVID-19 patients infecting others (particularly healthcare workers) and help protect patients with other medical issues from infection. In addition, telehealth services create the potential to release patients earlier from the hospital and to avoid new hospital visits, which potentially frees up hospital beds and equipment for those patients who most need them.

As we increasingly see outbreaks of infection in post-acute congruent living facilities such as assisted living centers and retirement communities, telehealth can and should be used to protect their elderly and other high-risk residents.<sup>2</sup> Another benefit of telemedicine, the need for which has increased during this emergency, is to provide healthcare for communities, which have limited access to needed services. These communities often include rural and underserved urban areas that may have limited internet broadband service and whose residents may have less access to other telehealth technologies such as a smartphone.<sup>3</sup> These underserved communities may often need to rely on voice-only telehealth services.

Telehealth is at least as old as the invention of the radio and the telephone.<sup>4</sup> Medicare has actually reimbursed for some telehealth services for over 20 years. There have been periods of healthcare providers advancing use of these services, but always followed by a waning period due to the lack of proper incentives and challenges with interoperability.<sup>5</sup> Recent advances in broadband internet access, internet of things devices, electronic health records, and advanced data analytics have created a surge in both the capability, and the cost efficiency of telehealth services. The current public health emergency necessitates a detailed look at the federal and state telehealth regulations to determine what changes will properly incentivize rapid adoption of the technology while also mitigating concerns related to safety, privacy, cybersecurity, and how best to assist underserved communities and people.

Telehealth is a broad set of services that includes telemedicine delivery of clinical care as well as other nonclinical activities, such as provider training, administrative meetings, and continuing medical education.<sup>6</sup> The American Telemedicine Associa-

---

2 <https://www.cdc.gov/coronavirus/2019-ncov/hcp/long-term-care.html> (accessed May 25, 2020).

3 <https://www.fcc.gov/reports-research/reports/broadband-progress-reports/eighth-broadband-progress-report>; <https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/> (accessed May 25, 2020).

4 <https://blog.evisit.com/history-telemedicine-infographic> (accessed May 25, 2020).

5 <https://revcycleintelligence.com/news/medicare-reimbursement-rules-limit-telehealth-adoption> (accessed May 25, 2020).

6 <https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine> (accessed May 25, 2020).

tion (the ATA) defines the subset of telehealth referred to as telemedicine as ‘a health care provider’s provision of services to a patient using telecommunications technology, where the patient and provider are in different locations’. One particularly important category of telehealth services, which is often treated separately by regulators, is remote patient monitoring (RPM). The ATA defines RPM as ‘including home telehealth, uses devices to remotely collect and send data to a home health agency or a remote diagnostic testing facility (RDTF) for interpretation. Such applications might include a specific vital sign, such as blood glucose or heart ECG, or a variety of indicators for homebound consumers. Such services can be used to supplement the use of visiting nurses.’<sup>7</sup>

Telehealth services are often divided into three separate categories: synchronous, asynchronous, and RPM.<sup>8</sup> Synchronous services allow for direct engagement between a healthcare provider and the patient using phone, video, or data transmission such as texting. Asynchronous services allow patients and healthcare providers to store information and forward it to the other party with an expectation that they will hear back at some point in the future. The delivery of photos for examination is particularly effective in asynchronous services. RPM allows for a mix of both synchronous and asynchronous communication to allow healthcare providers to evaluate a patient’s progress over time. The Department of Health and Human Services (HHS) conducted a study that demonstrated that healthcare providers across many specialties were using these services even before the current crisis.<sup>9</sup>

Telehealth, and especially RPM, has the potential to increase the number of healthcare providers by recruiting retired doctors and nurses who may have valid reasons not to want to work face to face with a patient (a compromised immune system or an injury that prevents the physical work that a hospital often requires), but who would like to put their skills and experience to use. In addition, the data that telehealth implementations create can be of tremendous value to public health agencies and health researchers.

Federal and state governments have recently removed many telehealth implementation barriers for the duration of the current emergency. The Food and Drug Administration (FDA), the Office of Civil Rights (OCR) at the Department of Health and Human Services, the Centers for Medicare and Medicaid Services (CMS) at the HHS, the Substance Abuse and Mental Health Services Administration (SAMHSA) at the HHS, the Drug Enforcement Administration at the Department of Justice, and state health and human services agencies all have done remarkable work to enable telehealth. This crisis can provide the USA with an opportunity to assess the role telehealth can play in our healthcare system and what regulations are necessary to increase its use and value while also protecting patients from risks created by the remote delivery of services. To assist with the US learning what we can during the emergency, the following provides a summary of some of the recent regulatory changes and recommendations for additional actions:

---

7 <https://www.americantelemed.org/resource/why-telemedicine/> (accessed May 25, 2020).

8 Michael A. Dowell, *Federally Qualified Health Center and Rural Health Center Telemedicine Compliance and Legal Issues*, 21 J. HEALTH CARE COMPLIANCE 5, 6 (2019).

9 Annette M. Totten et al., *Telehealth: Mapping the Evidence for Patient Outcomes from Systematic Reviews*, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, June 2016, at 22.

## BARRIERS, RECENT ACTIVITY TO REMOVE THEM, AND PROPOSALS FOR ADDITIONAL ACTION

This paper focuses on six categories of public policy barriers to the implementation of telehealth: reimbursement, privacy/cybersecurity, liability, licensure, technology access, and artificial intelligence (AI).

### Reimbursement

One of the most impactful barriers to the implementation of telehealth solutions has been whether the amount allowed for payment is enough to create an economic incentive for doctors (especially given the current demands on doctors' and their staff's time), and for system integrators and device manufacturers to develop the technology. CMS has made great progress in recent months in providing for greater reimbursement for Medicare patients by making a number of changes that apply for the duration of the current emergency.<sup>10</sup>

These changes allow healthcare providers to now bill for the following telehealth services:

- initial and subsequent observation and observation discharge day management;
- audio-only telephone services for certain services;
- initial hospital care and hospital discharge day management;
- initial nursing facility visits, all levels (low, moderate, and high complexity) and nursing facility discharge day management;
- critical care services;
- domiciliary, rest home, or custodial care services, new and established patients;
- home visits, new and established patient, all levels;
- inpatient neonatal and pediatric critical care, initial and subsequent;
- initial and continuing intensive care services;
- care planning for patients with cognitive impairment;
- psychological and neuropsychological testing;
- therapy services, physical and occupational therapy, all levels;
- radiation treatment management services;
- licensed clinical social worker services, clinical psychologist services, physical therapy services, occupational therapist services, and speech-language pathology services can be paid for as Medicare telehealth services

Taken together, these reimbursement changes allow for provider compensation for a broad set of telehealth services potentially at lower cost than in-person care. The experience in other countries supports the conclusion that reimbursement changes can significantly increase the potential of healthcare providers investing in the tools, processes, and training necessary to effectively provide services during the current crisis. For example, when France changed its reimbursement policies, they originally

---

10 <https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes> (accessed May 25, 2020).

expected 1.2 million virtual care consultations for 2020, but recent data suggest they may see in excess of 5 million visits by the end of the year.<sup>11</sup>

CMS will also now provide for reimbursement for RPM services for acute conditions as well as chronic, and that expansion will extend beyond the public health emergency.<sup>12</sup> This change can enable remote monitoring of those exhibiting symptoms of COVID-19 and has potential to allow for earlier release from the hospital for patients freeing up beds for those who have more serious needs.

Healthcare providers can now perform RPM services when the caregiver is not located in the same physical location as the doctor. This change allows for new business models employing nurses and other healthcare providers who may have concerns or challenges with working in the doctor's office. Other significant CMS changes include permitting RPM services for new as well as existing patients, and that RPM providers will only need to obtain patient consent once per year.<sup>13</sup>

### Reimbursement Proposals

Although CMS has made many changes to Medicare reimbursement to encourage the use of telehealth during the public health emergency, there are further changes that can be made, especially in the area of RPM. Even with the recent changes, there are still low limits to the amount of time allowed for RPM and the amount allowed to be billed. These limits will discourage providers from offering services that could greatly assist patients, reduce risk during the crisis, and over time lower healthcare costs.<sup>14</sup>

Recent CMS changes only allow for two 20-minute RPM sessions to be billed per month at a national average of \$54. To effectively allow for RPM management of COVID-19 symptoms (particularly pulse oximeter readings), CMS should allow for a greater amount of monthly time and an increased billing rate. Also, currently, only a primary care physician or a specialist is allowed to bill for RPM in any particular month. Coverage should be expanded to allow for the primary care physician and multiple specialists to each bill as they may be monitoring different illnesses, such as diabetes and COVID-19. CMS should also allow for reimbursement for the cost of the devices that need to be used by the patient for RPM.

There are restrictions on RPM services that do not allow certain organizations to bill Medicare. CMS should immediately allow Federally Qualified Health Centers (FQHC), rural health centers, and home health agencies to bill for RPM services. Also, given the current issues of COVID-19 infection in congruent living facilities such as nursing homes and rehabilitation centers, CMS should follow up on the expansion of Medicare coverage for RPM from chronic to acute and further expand it to post-acute care. Billing should be allowed for multiple RPM sessions a day for post-acute care. This change for post-acute RPM services will assist patients to return to their homes earlier and reduce risks to themselves and others. To aid in that goal, CMS should allow for

11 <https://hitconsultant.net/2020/05/14/covid-19-global-impact-primary-care-virtual-consultations/#.Xr6w7WhKhPY> (accessed May 25, 2020).

12 <https://mhealthintelligence.com/news/cms-affirms-payment-parity-for-telehealth-adds-more-covered-services> (accessed May 25, 2020).

13 <https://www.cms.gov/files/document/covid-final-ifc.pdf> (accessed May 25, 2020).

14 <https://news.careinnovations.com/blog/how-rpm-helps-achieve-the-triple-aim-of-healthcare> (accessed May 25, 2020).

reimbursement for provider telehealth visits with family caregivers. If these changes are collectively made, it will allow families to better care for their loved ones in their homes.

HHS should also explore changes that will assist patients and providers to better use the technology and to navigate the often-difficult billing codes and processes. HHS should provide operational guidance to Medicare Administrative Contractors for claims processing/billing requirements for expanded telehealth services. This should include guidance for Rural Health Clinics and FQHCs. Also, many telehealth services still require video for CMS to provide for reimbursement.<sup>15</sup> This video requirement may substantially limit the use of these services by underserved populations who do not have access to a smartphone or broadband internet. CMS should look to expand reimbursement coverage for telehealth audio-only services. Audio-only services will allow individuals who are most comfortable with talking on the phone to have meaningful discussions with their providers and to reduce the need for broadband internet access. This change will be particularly helpful during the current crisis, as it will reduce logistical challenges of sending new devices to patients and educating them on how to use the technology.

The current emergency also should encourage CMS to look at reimbursing for new healthcare services that hospitals are currently struggling to provide. Specifically, Medicare beneficiaries should be able to access respiratory therapy services necessary for their recovery via telehealth and remote monitoring solutions.<sup>16</sup> These services should not be limited just to COVID-19 patients.

### Privacy/Cybersecurity

Telehealth creates new cybersecurity and privacy risks, as the patient's home may not have the same protections in place as a provider's office.<sup>17</sup> Telehealth also creates new opportunities for health information sharing that have privacy and security implications. Understanding what further cybersecurity and privacy regulatory changes need to be made requires an overview of the current regulatory environment.

The USA has a long-established regulatory framework for protecting the privacy and cybersecurity of health data. That framework is primarily composed of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA Privacy Rule, and the HIPAA Security Rule.<sup>18</sup> In 2016, Congress passed the 21st Century Cures Act to promote the interoperability of electronic health records and to allow the patient to control the sharing of their personal health information.<sup>19</sup> On March 9, 2020, the Office of the National Coordinator for Health Information Technology (ONC) published the Cures Act Final Rule, which implements the interoperability provisions of the 21st Century Cures Act to promote patient control over their own

---

15 <https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet> (accessed May 25, 2020).

16 <https://www.latimes.com/california/story/2020-04-07/coronavirus-respiratory-therapists-ventilators-shortage> (accessed May 25, 2020).

17 <https://www.nccoe.nist.gov/sites/default/files/library/fact-sheets/hit-th-fact-sheet.pdf> (accessed May 25, 2020).

18 <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (accessed May 25, 2020).

19 <https://www.healthit.gov/curesrule/overview/about-oncs-cures-act-final-rule> (accessed May 25, 2020).

health information while protecting privacy and cybersecurity.<sup>20</sup> This rule makes many needed changes and has potential to greatly increase patient access to their health records, and HHS now needs to take steps to increase the speed of implementation.

Within HHS, OCR enforces the security and privacy rules. OCR has provided a number of useful clarifications and changes to increase the use of telehealth during the emergency. These following clarifications to encourage greater health information sharing specifically will be important to further the adoption of telehealth services that often require multiple providers, tools, and business associates.<sup>21</sup>

### *Interoperability*

Although the Cures Act Final Rule was just published on March 9, CMS quickly determined that the deadline for compliance of January 2, 2021, maybe unreasonable given the COVID-19 resource strain. Interoperability presents practical systems development challenges that if addressed poorly can create significant cybersecurity and privacy issues. As a result, CMS and ONC delayed the requirement for compliance with many of the requirements of the Rule.<sup>22</sup>

### *Patient Consent*

OCR reiterated that HIPAA was intended to allow for the sharing of information without the consent of the patient as necessary to treat the patient or another patient.<sup>23</sup> For the current crisis, the sharing of clinical information may be impactful for the treatment of other patients. To mitigate privacy concerns, it is important to educate providers and the public that this form of health information sharing is necessary. The California Consumer Privacy Act has brought considerable attention to the concept that individuals should be able to control their personal data, even while exempting HIPAA covered Protected Health Information (PHI) from its requirements.<sup>24</sup> At the same time, many privacy experts argue in the favor of moving away from an exclusive focus on consent to enable the sharing of information that is better for the individual and society.<sup>25</sup> As COVID-19 contact tracing efforts bring more attention to privacy,<sup>26</sup> it will be important to avoid a public backlash against health information sharing by HHS communicating to the public the importance of the exceptions to consent requirements.

HHS has also gone further to give providers latitude for information sharing during the crisis. On March 15, 2020, HHS made a waiver for up to 72 hours from the

---

20 [https://www.healthit.gov/sites/default/files/cures/2020-03/ONC\\_Cures\\_Act\\_Final\\_Rule\\_03092020.pdf](https://www.healthit.gov/sites/default/files/cures/2020-03/ONC_Cures_Act_Final_Rule_03092020.pdf) (accessed May 25, 2020).

21 <https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2013.0997> (accessed May 25, 2020).

22 <https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index> (accessed May 25, 2020).

23 <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf> (accessed May 25, 2020).

24 <https://www.brookings.edu/blog/techtank/2019/04/29/a-federal-privacy-law-could-do-better-than-californias/> (accessed May 25, 2020).

25 <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/> (accessed May 25, 2020).

26 <https://www.washingtonpost.com/politics/2020/04/28/contact-tracing-apps-can-help-stop-coronaviruses-they-can-hurt-privacy/> (accessed May 25, 2020).



time the hospital implements its disaster protocol that covered hospitals would not be sanctioned for failure to comply with five provisions of the HIPAA Privacy Rule: (i) obtaining a patient's agreement to speak with family members or friends involved in the patient's care, (ii) honoring a request to opt out of the facility directory, (iii) distributing a notice of privacy practices, (iv) complying with a patient's request for privacy restrictions, and (v) complying with the patient's right to request confidential communications.<sup>27</sup>

*Sharing with Public Health Authorities, Law Enforcement, and First Responders*

OCR made clear that the HIPAA Privacy Rule allows Covered Entities to share information without patient consent with public health authorities, first responders, and law enforcement,<sup>28</sup> at the discretion of public health authorities, a foreign government agency,<sup>29</sup> and persons at risk of contracting or spreading a disease or condition.<sup>30</sup> These disclosures may only transfer the minimum necessary information to accomplish the purpose.<sup>31</sup>

*Telemedicine Cybersecurity*

Physicians have restricted the technology they have used for telehealth to remain compliant the HIPAA Security Rule. OCR's February of 2020 notification states that Covered Entities and Business Associates need to continue to comply with obligations to properly provide cybersecurity protections for PHI. The notification says: 'In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.'<sup>32</sup>

However, in March 30, 2020, notification OCR stated: 'During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules. OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately'. This added flexibility is not limited to just COVID-19

---

27 <https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf> (accessed May 25, 2020).

28 45 CFR §§ 164.501 45 CFR 164.512(b)(1)(iv), 45 CFR; 164.512(k)(5), 45 CFR 164.512(j)(1) and 164.512(b)(1)(i).

29 45 CFR 164.512(b)(1)(i).

30 45 CFR 164.512(b)(1)(iv).

31 45 CFR 164.502(b).

32 <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf> (accessed May 25, 2020).



patients and should provide physicians the ability to use common technologies like texting to greatly increase their communications with patients.

OCR goes on in the March 30 notice to distinguish between public-facing communications technologies, which are not covered, and those that allow for private communication. They provide a nonexhaustive list of these covered private communication technologies: ‘Under this Notice, covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency. Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.’<sup>33</sup> As OCR allows for a greater selection of devices for telehealth, there will be an increased need to educate providers on how to increase their level of cybersecurity. One project that will help with this is the National Institute of Technology and Standards’ (NIST) effort to increase cybersecurity in telehealth. NIST’s National Cybersecurity Center of Excellence is conducting the Securing Telehealth Remote Patient Monitoring Ecosystem project,<sup>34</sup> which will use the NIST Cybersecurity Framework<sup>35</sup> to apply a risk assessment methodology to develop a specific telehealth NIST Cybersecurity Practice Guide.

#### *Business Associate Information Sharing*

Telehealth experts have expressed concern that provisions of HIPAA may restrict entities that fall under the ‘Business Associate’ definition from sharing information with public health authorities, first responders, and law enforcement.<sup>36</sup> As many telehealth providers may fall under this definition, there was a need to remove this regulatory concern. On April 2, OCR provided notice that it will exercise its enforcement ‘discretion and will not impose penalties for violations of certain provisions of the HIPAA Privacy Rule against health care providers or their business associates for the good faith uses and disclosures of PHI by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.’<sup>37</sup>

#### **Privacy/Cybersecurity Proposals**

Allowing broadly used technologies for telehealth is an important way to ramp the use of these services during the emergency. After the US moves beyond the emergency, it will be important to study the privacy and cybersecurity risks of using these general commercial platforms for telehealth. For example, Congress, HHS, and state regulators should fund the study of how health data obtained by the companies providing these

33 <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html> (accessed May 25, 2020).

34 <https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth> (accessed May 25, 2020).

35 <https://www.nist.gov/cyberframework> (accessed May 25, 2020).

36 <https://www.mwe.com/insights/ocr-waives-penalties-for-certain-phi-use-disclosure-by-business-associates-during-covid-19-emergency/> (accessed May 25, 2020).

37 <https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-hipaa.pdf> (accessed May 25, 2020).

platforms may have been commercialized and or transferred to other entities such as data brokers and online advertising providers. Also, Congress should provide increased funding for NIST's Securing Telehealth Remote Patient Monitoring Ecosystem project and other methods to increase the use of the NIST Cybersecurity Framework by telehealth providers.

The use of new telehealth technologies and services does create the potential for increased privacy and cybersecurity risks, as it expands the footprint for cybersecurity attack to the use of new hardware and software, and outside of the providers information technology network.<sup>38</sup> However, some of the existing restrictions that are intended to protect against these risks do not make sense in the current environment. For example, although OCR removed the risk of enforcement for sharing Business Associate information with public health authorities, there are still concerns that the contracts between HIPAA Covered Entities and their Business Associates may restrict the sharing of this information. Congress should put in place a legislative change to make these contract provisions unenforceable, and to create an obligation for sharing with public health authorities and approved researchers. This legislative change should also require the approved researchers to put measures in place to make certain the data is only used for healthcare research and not for data mining or other commercialization of the information.

Given that the ONC Interoperability Rule under the 21st Century Cures Act Final Rule was just published in March it is not surprising that there is still considerable work to be done to realize the interoperability of electronic health records.<sup>39</sup> The ONC rule calls for providers and medical device developers to promote patient data access using third-party apps and application programming interfaces (APIs) to share information between providers and among the different electronic health record vendors. Improved sharing of electronic health records has the potential to greatly benefit telehealth, and specifically RPM. OCR should fund a study for how to best incentivize the implementation of the APIs and for how patients can most efficiently decide to share telehealth information with new healthcare providers.

Telehealth also involves the use and sharing of information by entities that will not fall under HIPAA's scope.<sup>40</sup> The processing of that data will then be covered by Section 5 of the US Federal Trade Commission (FTC) Act's language regulating unfair or deceptive trade practices. State consumer protection and privacy laws may also apply to these uses of data. Many privacy commentators, including me,<sup>41</sup> have described this patchwork of FTC and state enforcement as confusing and inadequate.<sup>42</sup> To better foster trust in the use of telehealth, Congress should pass a strong comprehensive privacy law that provides the FTC with rule-making authority and substantially increased resources.

---

38 <https://www.healthcareitnews.com/news/nist-mitre-offer-cybersecurity-tips-telehealth-deployments> (accessed May 25, 2020).

39 <https://ehrintelligence.com/news/how-the-coronavirus-could-push-health-it-to-ehr-interoperability> (accessed May 25, 2020).

40 <https://thehealthcareblog.com/blog/2020/02/10/healthcare-in-the-national-privacy-law-debate/> (accessed May 25, 2020).

41 <https://blogs.intel.com/policy/2019/05/27/the-u-s-must-have-strong-enforcement-for-a-successful-privacy-regime/> (accessed May 25, 2020).

42 <https://www.privacyforamerica.com/> (accessed May 25, 2020).

### Liability

Malpractice liability remains a concern for providers of telehealth services. These concerns include a lack of a clear understanding of how the standard of care applies in telehealth, questions of whether existing malpractice insurance policies cover these services, and which state's law applies if the patient and the provider are located in different areas of the country.<sup>43</sup> There are concerns that telehealth services do not allow for certain medical practices that have been considered standard for treating patients with respiratory issues, such as being able to listen to the lungs with a stethoscope. It is unclear whether telehealth's inability to allow a healthcare professional to perform these time-tested approaches will impact their potential malpractice liability if there is an incorrect diagnosis.<sup>44</sup> Some states are taking action in this area. Hawaii has passed a law requiring malpractice insurance carriers to provide coverage for telehealth services.<sup>45</sup> Other states like New York have temporarily created exemptions from malpractice liability except in situations of gross negligence.<sup>46</sup> It is unclear whether concerns about when these temporary exemptions will expire will discourage healthcare providers from substantially investing in telehealth infrastructure due to fear of longer-term malpractice liability.<sup>47</sup>

### Liability Proposals

There is continued uncertainty about the extent to which malpractice insurance carriers cover claims arising from telehealth services.<sup>48</sup> States should expand their telehealth parity laws to require insurance carriers to include malpractice coverage for telehealth services on par with how they cover face-to-face services and for coverage of services outside the geographic area where the doctor is licensed. Also, given the possibility that telehealth may increase, or at least present new, cybersecurity risks providers also need to understand the extent to which their policies cover cybersecurity and the exemptions to coverage such as attacks by foreign nation-states.<sup>49</sup> Congress should fund the development of education materials for doctors to check with their malpractice insurance carriers to make certain the terms of insurance policies will cover all telehealth services they are planning to provide.

### Licensure

Many of the healthcare workers who are needed to address the current public health crisis are regulated by state professional licensure requirements that limit work across state lines. These workers include doctors, nurses, nurse practitioners, and nurses'

---

43 <https://www.natlawreview.com/article/doctor-medical-malpractice-issues-age-telemedicine> (accessed May 25, 2020).

44 <https://www.kff.org/womens-health-policy/issue-brief/opportunities-and-barriers-for-telemedicine-in-the-u-s-during-the-covid-19-emergency-and-beyond/> (accessed May 25, 2020).

45 HI Rev. Stat. § 671.7(a) (2019); Center for Connected Health Policy, 'State Telehealth Law & Reimbursement Policies: A Comprehensive Scan of the 50 States & the District of Columbia' (Fall 2019).

46 Executive Order, New York: No. 202.10 at 2, <https://www.governor.ny.gov/news/no-20210-continuing-temporary-suspension-and-modification-laws-relating-disaster-emergency> (accessed May 25, 2020).

47 <https://www.law360.com/insurance/articles/1272579/11-post-pandemic-predictions-for-telehealth-regulation> (accessed May 25, 2020).

48 <https://www.cchpca.org/telehealth-policy/malpractice> (accessed May 25, 2020).

49 <https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html> (accessed May 25, 2020).

aides. Telehealth and RPM can best realize their potential to address COVID-19 if they allow for healthcare workers in states that are not experiencing large infection rates to provide services to those states that are currently in crisis. This is especially true in certain practice areas where some states may have limited numbers of specialists.<sup>50</sup>

There is an existing system that 17 states and the District of Columbia have enacted to deal with emergency needs for healthcare providers. Those states have enacted versions of the Uniform Emergency Volunteer Health Practitioner Act (UEVHPA), which is model legislation developed in 2006 by the Uniform Law Commission.<sup>51</sup> When enacted by a state, the system allows for the emergency recognition of out-of-state healthcare licenses.

Along with emergency declarations, there are also longer-term reciprocity frameworks to recognize out-of-state healthcare licenses. An example of this type of framework is the Enhanced Nurse Licensure Compact (eNLC). The eNLC provides for automatic recognition of nursing licenses from over 30 states that participate in the agreement.<sup>52</sup>

Many states are also amending their licensure requirements in more targeted ways.<sup>53</sup> For example, Alaska, Missouri, and Tennessee have implemented reciprocity policies. Also, New Jersey took action to expedite approval for out-of-state-doctors applying for licensure.<sup>54</sup> Connecticut is an example of a state that took more specific licensure action to enable telehealth. The state suspended the licensure/certification/registration requirements to allow telehealth services by out-of-state professionals.<sup>55</sup>

### Licensure Proposals

Shortages of healthcare workers in communities with high numbers of COVID-19 patients are a significant concern.<sup>56</sup> Additional changes are necessary so that telehealth can allow doctors and nurses in other states to help even out those local shortages. States that have not passed a UEVHPA law should do so quickly. Also, states that are currently not participating should join the eNLC. All states should amend necessary legislation to allow for the provision of telehealth services by individuals physically located outside of the state. HHS should work with state governors to put in place executive orders that allow for the creation of Emergency Management Assistance Compacts (EMACs). EMACs can allow for mutual recognition of doctors between states. More information on EMACs, including a template executive order, is available at <https://www.emacweb>.

---

50 <https://www.ruralhealthinfo.org/toolkits/telehealth/2/care-delivery/specialty-care> (accessed May 25, 2020).

51 <https://www.uniformlaws.org/committees/community-home?CommunityKey=&#x003D;565933ce-965f-4d3c-9c90-b00246f30f2d> (accessed May 25, 2020).

52 <https://nurse.org/articles/enhanced-compact-multi-state-license-eNLC/> (accessed May 25, 2020).

53 <https://www.fsmb.org/siteassets/advocacy/pdf/states-waiving-licensure-requirements-for-telehealth-in-response-to-covid-19.pdf> (accessed May 25, 2020).

54 <https://www.astho.org/StatePublicHealth/States-Leverage-Telehealth-to-Respond-to-COVID-19/04-08-20/> (accessed May 25, 2020).

55 <https://www.natlawreview.com/article/connecticut-governor-lamont-expands-access-to-telehealth-services-response-to-covid> (accessed May 25, 2020).

56 <https://www.healthcarediver.com/news/covid19-respiratory-therapists-staffing/575033/> (accessed May 25, 2020).

org/. All states should explore making permanent reciprocity for out-of-state telehealth professionals.

### Technology Access

To realize the benefits of telehealth, providers will need to deploy the technology to communities that currently lack broadband internet access and the use of smartphones. This broad use of the technology will create more diverse data that will over-time produce better telehealth implementations. The focus on increasing use of the technology will also help extend healthcare services to rural areas and undeserved urban communities. Communities that are underserved with healthcare services may also be those that have limited access to reliable broadband internet service and/or the understanding of how to deploy telehealth technology.

Regulators have worked to broaden the list of available technologies to use with telehealth services, including those that can be deployed on smartphones. In addition, HHS has funded the creation of a national network of telehealth resource centers, which focus on training telemedicine providers.<sup>57</sup>

### Technology Access Proposals

Doctors and patients have to figure out how to use new technologies and incorporate the tools into their lives and work. Outreach to doctors and patients to provide assistance on how to implement telehealth technology is necessary, including providing easy to understand education materials. To increase telehealth technology access and further the creation of diverse telehealth data for analysis, regulators should promote telehealth access across the country. HHS should increase the funding for the national network of telehealth resource centers with a specific focus on rural areas and underserved urban areas. These resource centers are important ways to help doctors and other providers understand how to offer telehealth services.

### Artificial Intelligence

The broadened set of new telehealth technologies (especially end point RPM technologies like Bluetooth-enabled thermometers and pulse oximeters) will create more data that can be useful to train AI algorithms. Because COVID-19 is so new, there are little data to use to train analytical algorithms and AI solutions to determine how best to spot COVID-19 infection, to determine which patients are at increased risk of acute illness, and to develop a more effective treatment.<sup>58</sup>

New algorithms deployed in telemedicine require a lengthy FDA premarket assessment process. Although there are many of the current proposals for the use of AI in hospital-based care, there are a number of use cases where the technology can be useful in telehealth.<sup>59</sup> Technology providers are pushing AI algorithms to ‘the edge’, meaning that they will run on the end point devices used by patients such as scales, ther-

---

57 <https://www.telehealthresourcecenter.org/> (accessed May 25, 2020).

58 <https://towardsdatascience.com/artificial-intelligence-against-covid-19-an-early-review-92a8360edaba> (accessed May 25, 2020).

59 <https://www.forbes.com/sites/cognitiveworld/2020/04/16/edge-ai-is-the-future-intel-and-udacity-are-teaming-up-to-train-developers/#6b3cf92768f2> (accessed May 25, 2020).

mometers, and pulse oximeters.<sup>60</sup> The FDA’s traditional approach to medical device review was not designed for adaptive AI and machine learning (ML) technologies. Under the FDA’s current approach to software modifications, the FDA anticipates that many AI software updates will need a premarket review. Such a review process would substantially limit the benefits that can come from quickly updating software based on AI learning.

The FDA has recently proposed modifications to this assessment process that have potential to increase the speed of the implementation of software changes created by ML and other AI tools.<sup>61</sup> The FDA proposal is based on the following four principles: (i) Establish clear expectations on quality systems and good ML practices, (ii) this proposed regulatory approach would apply to only those AI/ML-based software as a medical device that requires premarket submission and not those that are exempt from requiring premarket review, (iii) expect manufacturers to monitor the AI/ML device and incorporate a risk management approach, and (iv) enable increased transparency to users and the FDA using post-market real-world performance reporting for maintaining continued assurance of safety and effectiveness.<sup>62</sup>

The FDA is also making changes that will allow AI to be more useful with RPM technologies. In March of 2020, the FDA provided a notification of enforcement policy to provide flexibility in the use of a number of noninvasive RPM technologies. The policy document states: ‘FDA does not intend to object to limited modifications to the indications, claims, functionality, or hardware or software of FDA cleared non-invasive remote monitoring devices that are used to support patient monitoring (hereinafter referred to as “subject devices”) during the declared public health emergency, as described in more detail below, without prior submission of a premarket notification under section 510(k) of the FD&C Act and 21 CFR 807.81.5’.

The FDA policy document included examples of permissible modifications, such as ‘the inclusion of monitoring statements related to patients with COVID-19 or co-existing conditions (such as hypertension or heart failure); for subject devices previously cleared only for use in hospitals or other health care facilities, a change to the indications or claims regarding use in the home setting; and hardware or software changes to allow for increased remote monitoring capability.’<sup>63</sup> These allowed modifications pave the way for the FDA to learn more about how these technologies function in practice during the emergency, and what level of review will be necessary once the crisis subsides.

### AI Proposals

Once providers are using telehealth solutions more broadly, there will be opportunities to gain value from the data those implementations create. Two policy priorities can then make better use of that data. First, Congress should require electronic health record vendors and healthcare providers to share data with health researchers using

---

60 <https://mhealthintelligence.com/news/at-the-cutting-edge-of-healthcare-iot-data-in-preventative-care> (accessed May 25, 2020).

61 <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device> (accessed May 25, 2020).

62 <https://www.fda.gov/media/122535/download> (accessed May 25, 2020).

63 <https://www.fda.gov/media/136290/download> (accessed May 25, 2020).



federated homomorphic encryption solutions.<sup>64</sup> These encryption solutions can allow for important research using telehealth data while still preserving the privacy and cybersecurity of the underlying personal health information.<sup>65</sup>

HHS should encourage health researchers to use the increased data provided by telehealth services to train AI software that can further improve not only the telehealth services, but also other clinical care, healthcare operations, and research. Also, CMS should create emergency reimbursement codes for the use of narrow AI solutions such as methods to triage patients (either for the first step in a telemedicine appointment with a doctor, or as part of an automated RPM application like a daily set of questions asked by a smartphone application or through a digital assistant with voice recognition like the Amazon Echo or the Apple HomePod).

To help enable this ecosystem of the use of telehealth data to improve AI healthcare algorithms, the FDA should move quickly forward with its proposed new AI assessment process.<sup>66</sup> Concurrently, the FDA should create a streamlined assessment pathway for critical AI uses in addressing COVID-19, such as allowing rapid retraining of known cleared AI applications toward other uses and further expansion of them for those new uses. An example of this type of expansion for a new purpose could be the use of algorithms that have been used in radiology to assist a doctor in spotting lung cancer to now also detect COVID-19 respiratory infection. Data from telehealth could provide substantial assistance in augmenting existing training data with an understanding of how patients progress over time.

## CONCLUSION

The FDA, HHS, and state regulators have done tremendous work in a short period of time to remove regulatory barriers and create incentives to enable the use of telehealth, and specifically RPM services, during the COVID-19 public health emergency. There are still actions that need to be taken in the areas of reimbursement, privacy/cybersecurity, liability, licensure, technology access, and AI. As we move past the crisis, regulators should examine how companies are using personal health information that is transmitted using telehealth technologies, and whether additional restrictions on the use of the data are necessary.

Further, this emergency will likely introduce millions of Americans to using telehealth services, providing substantial benefits to patients including, but not limited to, those who live in rural areas with limited access to healthcare. Regulators should make use of the data on the use of these services during this emergency. Collecting data and allowing for its analysis by researchers can assist Congress, HHS, and state regulators to determine which of the regulatory changes to make permanent. This data analysis can also help determine what further changes are necessary to properly incentivize providers to fully utilize these services, technology companies to continue to innovate in this area, and for insurers to adequately reimburse and cover malpractice claims.

---

64 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5961814/> (accessed May 25, 2020).

65 <https://venturebeat.com/2020/01/16/meet-the-new-twist-on-data-encryption-that-promises-better-privacy-and-security-for-ai/> (accessed May 25, 2020).

66 <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device> (accessed May 25, 2020).