MERCATUS CENTER
George Mason University

TESTIMONY

TESTIMONY TO THE MASSACHUSETTS HOUSE OF REPRESENTATIVES ON TELEMEDICINE AND CYBERSECURITY

Jared Rhoads
Visiting Research Fellow, Mercatus Center at George Mason University
Lecturer, Dartmouth Institute for Health Policy & Clinical Practice

Massachusetts House of Representatives, Committee on Technology and Intergovernmental Affairs

July 18, 2019

Good morning, Chairman Angelo Puppolo, Vice Chair Aaron Vega, Ranking Minority Member Marc Lombardo, and distinguished members of the Massachusetts House of Representatives Committee on Technology and Intergovernmental Affairs.

My name is Jared Rhoads. I am a visiting research fellow at the Mercatus Center at George Mason University and a researcher and lecturer at the Dartmouth Institute for Health Policy and Clinical Practice. I teach health policy with a focus on technology and innovation. Before working for Mercatus and Dartmouth, I worked for nine years as a healthcare research specialist for CSC Healthcare, a large technology services and consulting firm, where I tracked and analyzed emerging issues in both telemedicine and cybersecurity. I thank you for the opportunity to speak here today.

The advice I respectfully submit for the consideration of this committee can be summarized as follows:

- Consider the benefits of telemedicine, not just the risks. Overemphasizing security risks can eclipse the large existing and potential benefits of telemedicine for the people of Massachusetts.
- Beware of naming particular technologies in new regulation. In the fast-changing environment of the technology industry, regulation anchored to a specific technology is likely to become irrelevant in time or be circumvented by alternative technologies.
- When regulation sets a minimum security standard, that standard can become a ceiling, as market actors will have little incentive to invest in higher levels of security beyond the standard.
- Beware of special interests and firms seeking to erect barriers to entry to the market. Regulations, while well intended, often have the unintended effect of protecting market incumbents against the competition of future entrants.

TELEMEDICINE DEFINITION AND OVERVIEW

I would like to start by making sure that we all have a common understanding of what telemedicine is. Telemedicine is typically defined as the provision of medical care or services at a distance, involving the

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

use of information technologies or electronic communications.[1] That is a good, general definition that can guide our discussion.

Within that general definition of telemedicine, there are two main subtypes. They are (1) provider-to-provider telemedicine and (2) patient-to-provider telemedicine. Provider-to-provider telemedicine is the older and more prevalent type of telemedicine. It refers to physicians and other practitioners using communications technologies such as a telephone or a videoconferencing platform to share information about patients and come to decisions about diagnoses and treatments. This type of telemedicine need not be delivered in real time. For instance, a nurse who uses a digital camera to photograph a patient's wound or rash and then sends that photo a dermatologist for later evaluation is using telemedicine, even though there is no real-time communication going on.

Patient-to-provider telemedicine is somewhat newer. It refers to patients communicating directly with clinicians. The electronic visit (or e-visit) is an example of patient-to-provider telemedicine. In an e-visit, the patient and the clinician are in two different locations, but through videoconferencing are having the equivalent of a face-to-face conversation. In general, this mode of telemedicine is newer because it was not until the past 10 years or so that consumer electronics and consumer home internet bandwidth were powerful enough to have high-quality interactions and prevalent enough for hospitals and physicians to be interested in offering them as a regular service.

THE BENEFITS OF TELEMEDICINE

The academic literature on telemedicine consists largely of studies of new uses of telemedicine conducted by health services researchers. Here are four main benefits:

1. *Greater access to specialists*. Some physicians have such narrow specialties that there are not enough cases (patients) in a given region for it to make sense to have them on the staff of a practice, clinic, or hospital. Not every rural town in America needs a neurologist—until a patient shows up who needs a neurologist. Telemedicine can enable physicians in rural settings to consult with specialists hundreds or thousands of miles away. For example, telestroke services can extend stroke-care expertise into remote or underserved areas. One telestroke system in Georgia called Remote Evaluation of Acute Ischemic Stroke (REACH) enables emergency room physicians to get the specialist consultation necessary to determine whether to administer critical clot-dissolving medications (which need to be administered within three hours of stroke onset). By increasing access to stroke specialists, the telestroke service eliminates travel time, speeds time to treatment, and reduces death and disability.[2]
2. *Enhanced convenience and satisfaction for patients*. When patients can see their doctors without the time, expense, and hassle of traveling to a hospital or doctor's office, there are clear gains in terms of convenience and time saved. (Rural patients are perhaps the most obvious beneficiaries, but busy parents, busy employees, and urban patients who have to deal with dense traffic can save on travel time too.) Telemedicine removes geographic barriers for everyone. A related point is that patient satisfaction with telemedicine is generally very high, and for some teleservices patient satisfaction can even be higher than for traditional face-to-face services.[3] For example, in pediatric telepsychiatry, many young patients report feeling "a greater sense of safety and control when dealing with an unfamiliar adult . . . and greater sense

[1] Office of the National Coordinator for Health Information Technology "Telemedicine and Telehealth," September 28, 2017, https://www.healthit.gov/topic/health-it-initiatives/telemedicine-and-telehealth; John Craig and Victor Patterson, "Introduction to the Practice of Telemedicine," *Journal of Telemedicine and Telecare* 11, no. 1 (2005): 3–9.

[2] David C. Hess et al. "Telestroke: Extending Stroke Expertise into Underserved Areas," *The Lancet: Neurology* 5, no. 30 (2006): 275–78.

[3] Frances Mair and Pamela Whitten, "Systematic Review of Studies of Patient Satisfaction with Telemedicine," BMJ: British Medical Journal 320, no. 7248 (2000): 1517–20.

of personal space."[4] Those pediatric patients also miss less school when treated via telepsychiatry, compared to traditional office-based psychiatry.

3. *Improved patient outcomes*. Telemedicine is not an outright replacement for traditional medicine. Rather, telemedicine has been used where it successfully supplements or augments existing services or where it achieves something that previously was not possible. In other words, it tends to be used where it makes patients better off. Various telemedicine programs have shown improvements in clinical outcomes, including reduced readmissions, earlier diagnosis and treatment of conditions, and earlier detection of problems through closer monitoring. For example, in the Better Choices, Better Health diabetes self-management program tested by researchers at Stanford University, patients with diabetes achieved better self-management of their hemoglobin A1c levels, improved medication adherence, and other clinical benefits through a "virtual coach," a type of telemedicine that uses videoconferencing and messaging via a mobile device to connect patients with clinicians.[5]
4. *Reduced healthcare costs*. Although it can be hard to fully measure and evaluate the effect of telemedicine on the cost of care owing to the heterogeneity of telemedicine programs, objectives, and outcomes, a survey of the literature on cost effectiveness found that telemedicine can reduce costs for patients and providers.[6] Patients can see savings in the form of decreased travel, reduced waiting time, and reduced costs owing to reduced morbidity. Providers can see savings in the form of reduced hospital stays and avoided hospital readmissions. For example, patients with heart failure who use telemedicine services have reduced all-cause hospitalization, cardiac hospitalization, all-cause mortality, cardiac mortality, and length of stay.[7]

It would take many more pages of testimony to cover all of the diverse examples in the academic literature, let alone the self-reported experiences of hospitals and health systems that can be found in white papers, vendor case studies, and conference proceedings. What I have just covered is offered as merely an indication of the main benefits, with one example in each area from the academic literature.

SECURITY RISKS WITH TELEMEDICINE

Telemedicine, like all modern information-based technologies, is susceptible to security risks. All telemedicine technologies work by communicating health information over a computer network. Patients using digital home blood pressure readers to send readings to their primary care physicians do so over the internet. Patients sending photographs of skin conditions to their dermatologists do so over the internet. Physicians consulting with one another via videoconferencing do so over the internet. All of these transmissions run the risk of being intercepted, hacked, or compromised in some way, just as online banking information and other transactions over the internet are also susceptible.

The reason why health information is an attractive target owes to the rich personal identifiers that are present in a medical record. In a medical record, Social Security Numbers (SSNs) are linked with a birth date, an address, and other identifying information, and are of greater quality and reliability. Cybercriminals can use patient and provider identifiers to divert medical equipment or prescriptions, to

[4] David E. Roth, Ujjwal Ramtekkar, and Sofija Zeković-Roth, "Telepsychiatry: A New Treatment Venue for Pediatric Depression," *Child & Adolescent Psychiatric Clinics* 28, no. 3 (2019): 377–95.

[5] Kate Lorig et al., "A Diabetes Self-Management Program: 12-Month Outcome Sustainability from a Nonreinforced Pragmatic Trial," *Journal of Medical Internet Research* 18, no. 12 (2016): 1–11; Neesha Ramchandani, "Virtual Coaching to Enhance Diabetes Care," *Diabetes Technology & Therapeutics* 21, no. 2 (2019): S248–S251.

[6] Isabel de la Torre-Díez et al., "Cost-Utility and Cost-Effectiveness Studies of Telemedicine, Electronic, and Mobile Health Systems in the Literature: A Systematic Review," *Telemedicine and E-Health* 21, no. 2 (2015): 81–5.

[7] Ye Zhu, Xiang Gu, and Chao Xu, "Effectiveness of Telemedicine Systems for Adults with Heart Failure: A Meta-Analysis of Randomized Controlled Trials," *Heart Failure Reviews* (May 2019): 1–13.

file fake claims with insurers, and more. This is why, on the black market, a medical record is worth far more to identity thieves than an SSN or credit card number alone.[8]

Security risks and safeguards differ slightly based on the two subtypes of telemedicine that I described earlier (provider-to-provider telemedicine and patient-to-provider telemedicine).

In provider-to-provider telemedicine, the two parties are required by federal law, namely the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to implement "appropriate safeguards." The main risks here are that unencrypted transmissions are intercepted or that unauthorized users at either end inappropriately gain access. Appropriate safeguards include encrypting data so that it appears scrambled to anyone other the intended recipients, and authenticating users and devices so that only the intended parties can access the data in the first place.

In patient-to-provider telemedicine, the patient end of the transaction "falls outside the controlled and supervised environment of a HIPAA-regulated clinical care setting."[9] The main risks, again, are that unencrypted transmissions are intercepted, or that an unauthorized user at either end gains access to the computer or device. Another risk that is particularly pertinent to this type of telemedicine is that malware (i.e., malicious software) could become accidentally installed on the patient's device.

WEIGHING THE BENEFITS AND THE COSTS OF SECURITY REGULATION

For telemedicine to achieve its full potential and consistently deliver the aforementioned benefits, it is imperative that it be secure from cybercriminals. Without security, patients and providers will cease to trust telemedicine and will cease to use it.[10] However, it is possible for security requirements to be too strict or too limiting. The question is, how do we let telemedicine thrive while maintaining a reasonable level of security? My advice for the committee is this:

1. *Consider the benefits of telemedicine, not just the risks.* The only way to achieve total, guaranteed security in telemedicine (i.e., zero breaches) is to not use telemedicine at all or to restrict it to extremely limited situations. To do so, however, would be to forgo a major opportunity to obtain many great benefits, such as those we have heard today. The goal of new regulation in this area, if any is needed at all, should be to achieve as many of those benefits as possible, with a tolerable level of risk—not to attempt to bring the probability of a security incident to zero.
2. *Beware of naming particular technologies in new regulation.* An inherent challenge with coming up with regulation in this area is that this is a rapidly changing technological landscape. Regulation that is general and unspecific tends not to be helpful to organizations who are trying to ensure compliance. Regulation that is specific to particular technologies (such as two-factor authentication or a particular type of encryption) is apt to get eclipsed technologically and become irrelevant within a few years.
3. *When regulation sets a minimum standard, that standard can become a ceiling.* The trouble with setting a specific minimum security standard is that any actor who meets that standard can call himself "compliant" and in effect put himself on the same level as actors who have long surpassed or who would otherwise seek a higher level of security. A minimum standard may achieve some good in terms of motivating the security laggards, but it also creates a disincentive for anyone to go above and beyond that security standard. In a world with security standards written into state law, there is less reason to become a security leader because it is more difficult to differentiate oneself in the marketplace when everyone can say they are compliant.

[8] Mariya Yao, "Your Electronic Medical Records Could Be Worth $1000 to Hackers," *Forbes*, April 14, 2017.

[9] Joseph L. Hall and Deven McGraw, "For Telehealth to Succeed, Privacy and Security Risks Must Be Identified and Addressed," *Health Affairs* 33, no. 2 (2014): 216–21.

[10] Hall and McGraw, "For Telehealth to Succeed."

4. *Beware of special interests and firms seeking to erect barriers*. There are many reputable information technology (IT) security firms who provide immensely valuable services to their clients, and who compete fairly to do so. However, if the state were to embark on the crafting of new regulation, it would undoubtedly attract the attention and involvement of security vendors seeking to protect their interests. Vendors would likely push for regulation that is friendly to their products and services, and unfriendly to their competitors' products and services. We might even see hospitals and health systems push for regulations that they already meet or could easily meet, but that would serve as barriers to entry to their smaller competitors.

CONCLUSION

After years of slow growth and development, telemedicine is finally hitting its stride. Most of this progress owes to the rapid technological advances of the Internet and mobile device era that have driven the cost of telemedicine down and have given it a value proposition that is hard to ignore.

In provider-to-provider telemedicine, HIPAA mandates encryption. In patient-to-provider telemedicine, more and more teleservices now run on consumer devices such as smartphones and home computers that have increasingly sophisticated security features. These are the same devices and networks over which we do our online banking, our online shopping, and so forth.

It is hard to anticipate what further security regulations in this area would be helpful for the state of Massachusetts to adopt. I have offered four reasons why it is not clear that enacting additional security regulations or setting new higher standards would yield a net social benefit. Moving forward, this committee should consider whether security might best be left to the natural incentives of the physicians, patients, and organizations involved to adopt the technologies and practices that enable them to deliver the greatest benefit at a level of security that they are comfortable with.

That concludes my testimony. Thank you for your time.

Sincerely,

Jared Rhoads
Visiting Research Fellow, Mercatus Center at George Mason University
Lecturer, Dartmouth Institute for Health Policy & Clinical Practice