MERCATUS CENTER
George Mason University

TESTIMONY

# SECURITY, PRIVACY, AND INNOVATION IN THE FUTURE OF TELEMEDICINE

**Jennifer Huddleston**
*Research Fellow, The Fourth Branch Project, Mercatus Center at George Mason University*

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 Committee on Technology and Intergovernmental Affairs.

My name is Jennifer Huddleston, and I am a research fellow at the Mercatus Center at George Mason University, where my research focuses primarily on the intersection of law and technology. This includes issues surrounding data security and data privacy. Thank you for this opportunity to discuss such policy matters in relation to telemedicine.

Within this context I would like to focus on three key points:

1. Telemedicine and other technological innovations expand the debate over protected health information (PHI) privacy and security and may require an examination of existing laws to reflect the reality of such an expansion.
2. Policymakers should attempt to be as precise as possible when it comes to data security or data privacy to avoid unintended consequences that impede beneficial innovation, such as telemedicine.
3. Policymakers should account for and consider tradeoffs and consequences, including not only the need for sensitivity around PHI, but also what might be lost by focusing only on the need for privacy.

## TELEMEDICINE, INNOVATION, AND DATA AND EXISTING REGULATION

Like many other fields, healthcare has experienced a rapid pace of innovation. New technologies, including mobile fitness trackers and other internet of things (IoT) devices, health apps, direct-to-consumer testing, and telemedicine can empower consumers and provide additional choices in healthcare. However, in many cases, such technologies do not fit into traditional categories. Concerns about the privacy and security of sensitive information can arise, and innovation can be deterred when outdated policies prevent the development of technologies or do not adequately reflect the new concerns that arise.

The fact that such technology often outpaces traditional policy mechanisms is often referred to as the "pacing problem."[1] Particularly in sectors such as healthcare, that are both heavily regulated and

[1] Adam Thierer, "The Pacing Problem and the Future of Technology Regulation," *The Bridge*, August 8, 2018.

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

constantly experiencing innovation, regulations can quickly become outdated and either prevent the adoption of technologies or no longer address the actual concerns that arguably should be regulated. For example, the primary federal healthcare privacy law, the Health Insurance Portability and Accountability Act (HIPAA), was initially enacted in 1996, and its privacy rule's effective date was 2003. Even the more recent Health Information Technology for Economic and Clinical Health Act (HITECH Act), incentivizing the adoption and meaningful use of electronic health records (EHR) and outlining certain privacy and usage principles associated with such, is now a decade old. Similarly, most state laws also remain relatively static or struggle to keep up with these rapid changes. Massachusetts last updated its state law governing healthcare privacy and disclosure more than a decade ago, in 2008. Existing laws may have requirements that do not include recent new technologies such as telemedicine or create regulatory barriers to their deployment. They may also fail to deal with emerging technological changes that could contribute to retention, storage, or transfer of data in more secure ways like cloud computing and possibly, one day, blockchain.[2]

In some cases, the pacing problem can be a pacing benefit for innovation by allowing it to emerge faster than it can be regulated away;[3] but in other cases, outdated regulations may prevent innovations like telemedicine from becoming more widely adopted or deter innovators from pursuing certain opportunities or applications for promising technologies. In telemedicine, this can include limitations that prevent televisits with a provider who has not been previously seen or requiring a nurse to be present during televisits.[4] Such burdens can not only discourage the use of telemedicine, but also keep it from being available to any patient, anytime, anywhere.

Policymakers should consider whether additional security requirements are necessary for new health innovations, such as telemedicine. In fact, in some cases, rather than expanding existing regulations to new technologies, policymakers may want to consider whether the old regulations are necessary for currently regulated entities as well.[5] They should also consider how new and old requirements might be able to evolve along with the technology.

## THE IMPORTANCE OF PRECISE DEFINITIONS AND LIMITING UNINTENDED CONSEQUENCES

Most people consider health information, such as information about which medications they take, to be particularly sensitive information and would often be willing to pay a price or make tradeoffs to maintain the security and privacy of such information.[6] Health information is shared in burgeoning technologies, such as fitness apps, social media support groups, and telemedicine. In an environment where data is increasingly omnipresent, it is necessary to be precise about both data and covered entities. Such precision helps ensure that regulations do not frustrate consumer expectations or impede the intended purpose for sharing the information.[7]

In general, existing laws narrowly establish which entities are covered by regulatory requirements. In Massachusetts, for example, hospitals and medical offices are subject to the privacy requirements for PHI and EHR, but the privacy requirements do not apply to the doctors directly.[8] If expansion of these

---

[2] Bill Kleyman, "Approaching the Top 5 Healthcare Cloud Security Concerns," *Cloud News*, Health IT Security, May 21, 2018; Sony Salzman, "Electronic Medical Records: Holy Grail for Blockchain," *MedPage Today*, August 22, 2018.
[3] Adam Thierer, "The Pacing Problem, the Collingridge Dilemma & Technological Determinism," *Technology Liberation Front*, August 16, 2018.
[4] For a discussion of the impact of regulatory barriers on telemedicine, see Robert Graboyes and Jennifer Skees, "The Promise of Telemedicine in Mississippi," *Clarion Ledger*, August 4, 2018.
[5] Adam Thierer, "Converting Permissionless Innovation into Public Policy: 3 Reforms," *Plain Text*, November 29, 2017.
[6] Mary Madden, *Americans Consider Certain Kinds of Data to be More Sensitive than Others* (Washington, DC: Pew Research Center, 2014).
[7] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, March 2012, 47.
[8] Commonwealth of Massachusetts, "Guide on the Disclosure of Confidential Information: Health Care Information," accessed July 8, 2019, https://www.mass.gov/info-details/guide-on-the-disclosure-of-confidential-information-health-care-information.

covered entities is necessary to ensure parity in security and privacy for online providers, it should be done carefully and precisely to reflect those providers that are similarly situated.

Additionally, definitions of covered PHI data should distinguish between data that are deliberately collected and utilized and those which may be incidental or publicly shared by the patient. This approach would reflect a Obama-era 2012 Federal Trade Commission report recommending that when such data is collected or utilized, those doing so obtain a heightened level of consent and awareness from consumers when providing choices involving sensitive data.[9] This approach would minimize the effects of unintended consequences of broad definitions that could accidentally penalize benign or beneficial actions.[10] An overly broad definition of health information could include everything from physical descriptions to buying habits that indicate certain medical conditions or health-related habits.[11] When considering how to address technological changes, policymakers should be cautious in expanding definitions of health information.

A narrowly tailored approach could help ensure parity in security and privacy in online and offline medical visits, while limiting potential unintended consequences. It should not always be assumed that the appropriate policy answer is to expand definitions to regulate new digital technologies like telemedicine to the equivalent of their analog counterparts.[12] Broad definitions could have unintended consequences for a variety of patient choices and empowerment via technology, not just for telemedicine or electronic health records. Appropriately narrow definitions also provide greater clarity for both consumers and providers to hopefully limit either mistakes that wrongly allow information to be exposed or the frustration in being unable to obtain information they are entitled to while still providing the flexibility for innovation to evolve.

## CONSIDER POTENTIAL TRADEOFFS

Health information is often sensitive. Focusing on privacy presents tradeoffs among innovation, the different uses of data by different providers or entities, the need for access to information for legitimate purposes, or consumer choices. Placing restrictions to always favor privacy can at times cause harm.

While healthcare privacy is often incredibly important, it is also important to consider the impact of privacy requirements on access to information by the patient, next of kin, or another physician during an emergency. For example, families or emergency providers may encounter difficulties gaining access to records in a timely fashion owing to strict interpretations of regulations.[13] That is not to say that creating additional protections for sensitive information is inappropriate, but that valuing privacy is not without its own costs.

Classifications of data and technologies are not always clear, particularly when it comes to the growing array of technologically enabled tools for both patients and providers. For example, in addition to telemedicine, a growing number of apps allow individuals to track and even share health data from menstrual cycles to blood sugar to heartrate during fitness workouts. In some cases the creators of these apps have sought FDA approval,[14] but in many cases such approval is deemed unnecessary.[15] While the FDA and other regulators have recognized the value to both providers and patients of such

[9] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 47.
[10] Federal Trade Commission, 47.
[11] US Department of Health and Human Services, *Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*, December 13, 2017, 5–7.
[12] Thierer, "Converting Permissionless Innovation into Public Policy."
[13] Lisa Szabo, "Mental illness: Families Cut Out of Care," *USA Today*, February 26, 2016.
[14] For examples of FDA-approved medical apps, see CareCloud, "7 Best FDA Approved Health Apps," *Continuum*, n.d.
[15] Food and Drug Administration, "Mobile Medical Applications," September 4, 2019, https://www.fda.gov/medical-devices/digital-health/mobile-medical-applications.

innovations,[16] subjecting a direct-to-consumer app to the same requirements as a hospital when it comes to the information collected could deter such innovation. It also poorly reflects the purpose and nature of the data collected and the consumer and innovator assumptions about its purpose. Policymakers should consider how classifications of data could impact not only doctors and telemedicine, but a growing number of devices consumers may use to take control of their own health as well.

Creating additional regulations for the security and privacy around telemedicine could also limit investment or the number of eligible providers who can participate. For example, following the General Data Protection Rule (GDPR) in Europe, venture investment in startup and micro tech companies in the European Union has decreased in part owing to concerns about the difficulty and costs of compliance.[17] At a state level, additional regulatory requirements could create a patchwork that makes it difficult if not impossible for innovators to provide their services throughout the entire country.[18] This patchwork can undermine the advantages of borderless technologies such as telemedicine or prevent states from benefiting from new technologies.[19] For example, Illinois's restrictive biometric privacy laws have resulted in its residents being geofenced out of technologies that residents of many other states enjoy.[20]

In some cases, favoring privacy over innovation or choice may be a necessary tradeoff to ensure certain minimal standards in regulated industries such as healthcare, but if states institute too many contradictory requirements, the effect may be to undo the borderless benefits of new and developing technology.[21]

## CONCLUSION

Telemedicine and many other innovations in the healthcare marketplace have the potential to help solve many longstanding problems that patients and providers face. A regulatory approach should not only consider the potential risks and problems with issues such as data security and privacy for sensitive health information, but should also reflect the benefits new technologies can have in empowering patients and assisting providers. As technology often outpaces traditional policy tools, policymakers will need to exercise a degree of regulatory humility; this means precisely addressing specific problems while enabling flexibility in future innovation. In addition to thinking about whether any new regulatory requirements are necessary for data security and data privacy in telemedicine, policymakers should also consider whether existing requirements reflect current technology and best practices and how outdated regulations might prevent the benefits of new technologies.

[16] Food and Drug Administration, "Mobile Medical Applications."
[17] Leonid Bershidsky, "Europe's Privacy Rules Are Having Unintended Consequences," *Bloomberg*, November 14, 2018.
[18] For a discussion of such an issue in the context of data privacy more generally, see Jennifer Huddleston, "The Problem of Patchwork Privacy," *Technology Liberation Front*, August 15, 2018.
[19] Huddleston, "The Problem of Patchwork Privacy."
[20] For example, see Selena Larson, "Google's Face Match Feature Doesn't Work in Illinois and Texas," *CNN Business*, January 17, 2018.
[21] Huddleston, "The Problem of Patchwork Privacy"; Graboyes and Skees, "The Promise of Telemidicine in Mississippi."