Health Law and Policy Brief

Volume 13 | Issue 2 Article 2

2019

Telemedicine and Legal Disruption

Mark Andriola
Yale Law School

Telemedicine and Legal Disruption

*Mark Andriola**
Yale Law School

* Mark Andriola, Yale Law School Class of 2019. Mark is particularly thankful to Professor Mark Barnes for introducing him to the field of health law, and Professors Rebecca Crootof and BJ Ard for their thoughtful feedback. Finally, Mark would like to thank Susan Vari and Mary Elizabeth Guard for a lifelong lesson in the law of medicine.

I. INTRODUCTION

"'Science has eliminated distance,' Melquiades proclaimed. 'In a short time, man will be able to see what is happening in any place in the world without leaving his own house.'"[1]

The invention of the automobile had a profound effect on the health care industry. The automobile made many physicians feel "as if the day had forty-eight hours instead of twenty-four."[2] The car, along with the general urbanization of the United States, saved doctors and patients tremendous amounts of time and greatly expanded health care markets. Yet not all doctors appreciated the new technology. Transportation also increased competition among doctors by allowing patients to see physicians from different towns.[3] A common theme of new technologies held true for the automobile in its relationship to health care: there are winners and losers.

The growth of telemedicine has generated similarly mixed reactions from the medical community. To some, telemedicine represents a phenomenal opportunity to expand access for patients and decrease costs for doctors. One study of the Virtuwell system in Minnesota found that average cost decreased $88 per episode.[4] Another analysis indicated that Teladoc, a large telehealth company, increased access to patients who are not otherwise connected to providers.[5] The telemedicine market is expected to be worth over $34 billion by 2020, with North America accounting for more than 40% of that total.[6] In 2016 alone, forty-four states considered new legislation to regulate the growth of telemedicine.[7]

Some groups have been more resistant to the technology's development. Most notably, the Texas Medical Board issued new guidelines defining a proper physician-patient relationship as including a face-to-face meeting unless telemedicine consultations occurred at "distant site providers."[8] Texas may have relied on studies like the one found in *Journal of American Medicine* showing "significant variation in quality" across telemedicine providers in the management of acute illness.[9] While the jury is still out on

---

[1] Gabriel Garcia Marquez, One Hundred Years of Solitude 2 (trans. Gregory Rabassa, First Harper Perennial Modern Classics ed. 2006).

[2] Paul Starr, The Social Transformation of American Medicine 70 (1982). For another comparison of telemedicine to the introduction of automobile, see Alison M. Sulentic, *Crossing Borders: The Licensure of Interstate Telemedicine Practitioners*, 25 J. Legis. 1, 1 (1999).

[3] Starr, *supra* note 2, at 77.

[4] Patrick T. Courneya et al., *HealthPartners' Online Clinic For Simple Conditions Delivers Savings of $88 Per Episode and High Patient Approval*, 32 Health Aff. 385, 387 (2013).

[5] Lori Uscher-Pines & Ateev Mehrotra, *Analysis of Teladoc Use Seems to Indicate Expanded Access to Care for Patients Without Prior Connection to A Provider*, 33 Health Aff. 258, 263 (2014).

[6] Bernie Monegain, *Telemedicine Market to Soar Past $30B*, HealthcareITNews (Aug. 4, 2015), http://www.healthcareitnews.com/news/telemedicine-poised-grow-big-time.

[7] Michelle Apodaca & Neil Issar, *An Update on Telemedicine in Texas and Beyond*, Lexology (Feb. 9, 2017), http://www.lexology.com/library/detail.aspx?g=19709cf2-d5ab-4a1f-9273-c32650bcde45.

[8] *Telemedicine FAQs*, Tex. Med. Board, http://www.tmb.state.tx.us/page/laws-GC-FAQs-Licensees.

[9] Adam J. Schoenfeld et al., *Variation in Quality of Urgent Health Care Provided During Commercial Virtual Visits*, 176 JAMA Internal Med. 635, 636 (2016).

various particular uses of telemedicine, the industry is growing and creating new legal and practical questions.

This Article argues that telemedicine is not legally disruptive. As of now, the technology has not fundamentally altered the legal underpinnings of health law. Telemedicine is defined as the use of virtual audio-visual interactions to deliver clinical health services while a patient and physician are physically separated.[10] A meaningful number of health care interactions no longer require the joint presence of both patient and physician. The car allowed physicians to get around quicker, while telemedicine may remove the need to get around at all.

This Article considers three key areas of law and regulation to demonstrate that telemedicine is not legally disruptive. Part II provides further detail on the meaning and significance of legal disruption. Part III addresses the physician-patient relationship and whether the removal of physicality as a structurally necessary component of that relationship is disruptive.[11] Telemedicine arguably upends, or so Blum suggests, the "special human relationship" joining physicians and patients.[12] Yet the pillar on which the physician-patient relationship rests is one of contractual consent—physicians must agree to the establishment of the relationship—not physicality.[13] Moreover, these relationships have already been established without physical interaction via telephone and through consultations from doctors.[14]

Part IV assesses the effect of telemedicine on physician licensure, which currently operates through state-based licensing laws.[15] The state-based licensing system supposedly prevents the interstate practice of telemedicine, and many view licensing as the most significant burden to the widespread use of the technology.[16] The physical

---

[10] This definition stems from New York state law, which defines "telemedicine" as "use of synchronous, two-way electronic audio-visual communications to deliver clinical health care services, which shall include the assessment, diagnosis, and treatment of a patient, while such a patient is at the originating site and a telehealth provider is at a distant site." N.Y. Pub. Health Law § 2999-cc-5 (2019). This Article does not address the broader digitization of health care, including electronic health records and mobile health applications. For a thorough consideration of these issues, see Robert Wachter, The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age (2015). Telemedicine further stands in contrast to telehealth, which more generally includes the use of "electronic information communication technologies by telehealth providers." N.Y. Pub. Health § 2999-cc-4 (2019).

[11] *See infra* Part II.

[12] *See* Blum, *supra* note 50, at 413.

[13] *Compare* Williams v. United States, 242 F.3d 169 (5th Cir. 2001) (finding no obligation on Cherokee Indian Hospital to treat non-Indian suffering respiratory distress), *and* Esquivel v. Watters, 154 P.3d 1184 (Kan. Ct. App. 2007) (finding no relationship between patient and hospital where hospital only agreed to provide free gender determination and did not identify defect in pregnancy), *with* Ricks v. Budge, 64 P.2d 208 (Utah 1937) (finding a physician-patient relationship continued even when patient had unpaid bills).

[14] *See infra* Section III.B.

[15] *See infra* Part III.

[16] *See, e.g.*, Diane E. Hoffman &Virginia Rowthorn, *Legal Impediments to the Diffusion of Telemedicine*, 14 J. Health Care L. & Pol'y 1 (2011) ("As a foundational matter, Roundtable participants acknowledged that the historical model of state licensure is a constraint on the growing

separation of the physician from the patient does not prevent states from effectively regulating quality of care. Part V discusses the issue of data security, a primary concern for many health care experts in the age of digitization.[17] While telemedicine certainly creates new challenges for data protection, it is not legally disruptive on this issue. For one, the industry has already adopted and encouraged a massive expansion of electronic health records, and telemedicine does not meaningfully exacerbate this challenge.[18] The complications of data security can also be resolved through the existing framework that attempts to manage security issues while embracing the utility of digitization in health care. Existing rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[19] may require change, but these adjustments are not disruptive in nature. Part VI offers lessons learned from this analysis of telemedicine regarding how to generally assess whether a new technology is legally disruptive and concludes that the existing law for these three areas is amenable to telemedicine and can adjust through modifications.[20]

II. UNDERSTANDING LEGAL DISRUPTION

This Article contends with whether this development is legally disruptive.[21] Telemedicine is legally disruptive if it requires reconsideration and ultimate adjustment of the core legal and regulatory principles of health law. The use of "requires" is somewhat misleading, however, because introduction of a new technology rarely requires changes to existing law. Law can stubbornly remain antiquated in the face of new technology, though evidently not ideal. Put simply, a new technology is legally disruptive when it both cannot be accommodated through existing legal structures and should be accommodated for its social value.[22] There are two important factors to consider when applying this definition

---

field of telemedicine but agreed that any alternative must preserve the goals of licensure—to protect the public from incompetent physicians and sub-standard care.").

[17] *See infra* Part IV.

[18] *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. 111-5 (2009) (providing substantial incentives for adoption of electronic medical records); *see also* Howard Burde, *The HITECH Act: An Overview*, AMA JOURNAL OF ETHICS: HEALTH LAW (Mar. 2011), http://journalofethics.ama-assn.org/article/hitech-act-overview/2011-03.

[19] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[20] *See infra* Part VI.

[21] By legally disruptive, I do not mean to invoke Clayton Christensen's definition of disruption whereby smaller companies push out incumbents by moving downstream, offering more functional services at a lower price, and eventually moving up the food chain. *See* Clayton M. Christensen et al., *What is Disruptive Innovation?*, HARV. BUS. REV. 44-53 (2015). For one, while there is some evidence of this process in telemedicine, large incumbents are arguably best positioned to accrue the benefits of the new technology. New York Presbyterian, to some the most prestigious hospital and health system in New York City, recently announced the creation of Digital Urgent Care and Virtual Visit through their NYP OnDemand app. *See New York-Presbyterian Launches Digital Urgent Care and Virtual Visit with NYP OnDemand*, NY-Presbyterian (Nov. 7, 2016), http://www.nyp.org/news/NYP-Launches-Digital-Urgent-Care-and-Virtual-Visit. Like other forms of economically disruptive innovation, telemedicine will likely decrease costs and increase access to new customers.

[22] Ryan Calo offers a "moderate conception that holds technologies to be exceptional if the best reconciliation of societal values leads to systemic changes to law or institutions." *See* Ryan Calo,

of legal disruption. First, the extent to which a technology is legally disruptive will depend in part on how much the technology alters human capabilities.[23] It is likely that a technology modestly expanding human capabilities should be accommodated through the existing legal regime. Electronic car windows are not legally disruptive because they do not meaningfully expand human capabilities.[24] A car that can fly, or drive itself, alternatively, can be legally disruptive.

The second relevant factor is the flexibility of the underlying doctrine. Drones are an expansion of human capabilities but, perhaps more importantly to their legal disruptiveness, there are justifiably strict regulations surrounding the national airspace. This regulation is clearly structured around commercial airplanes and not unmanned aerial vehicles. Douglas Marshall has argued that the lack of an explicit statutory mandate for the Federal Aviation Administration to regulate drones has led to a "perilous journey" and messy administrative process for regulating unmanned aerial vehicles.[25] Alternatively, a very novel technology may not be legally disruptive if its role is in an already lax or flexible legal regime. While we accurately think of health care as a heavily regulated industry, many of the underlying legal doctrines are quite flexible. Much of the physician-patient relationship revolves around the contractual concept of consent, a doctrine highly amenable to telemedicine.[26] Health care is a constantly changing industry, and any legal doctrine must be responsive to new modes of delivery of care.

Though there is general acknowledgment that telemedicine may be a source of market disruption,[27] scholars have not explicitly considered the question of legal disruption. Many scholars have effectively applied traditional principles of health law to telemedicine when assessing its potential effect.[28] For example, Phyllis Forrester Granade, addressing telemedicine's effect on medical malpractice as early as 1997, recognized that "[t]elemedicine malpractice cases might be characterized

---

Robotics and the Lessons of Cyberlaw, 103 CALIF. L. REV. 513, 550 (2015). Calo's theory is a broad one of disruption, but I apply his logic to the narrower question of legal disruption. A normative judgment as to the value of a new technology is required to assess its potential for disruption.

[23] This is based upon Donald Schon's definition of technology as "any tool or technique, any product or process, any physical equipment or method of doing or making, by which human capability extended." Donald Schon, TECHNOLOGY AND CHANGE 1 (1967).

[24] Lyria Bennett Moses notes that "traffic rules would continue to apply to cars with electric windows." *See* Lyria Bennett Moses, *Why Have a Theory of Law and Technological Change?*, 8 MINN. J. L. SCI. & TECH. 589, 596 (2007).

[25] *See* Douglas Marshall, *What a Long Strange Trip It's Been: A Journey Through the FAA's Drone Policies & Regulations*, 65 DEPAUL L. REV. 123, 123 (2016).

[26] *See infra* Section II.A.

[27] Thomas R. McLean, *The Future of Telemedicine & Its Faustian Reliance on Regulatory Trade Barriers for Protection*, 16 HEALTH MATRIX: J. LAW-MEDICINE 443, 450 (2006) ("Telemedicine is an example of a 'disruptive innovation,' i.e. an innovation that allows a service to be provided cheaper and in a more convenient fashion than traditional medicine.").

[28] *See, e.g.*, John D. Blum, *Internet Medicine and the Evolving Status of the Physician-Patient Relationship*, 24 J. LEGAL MED. 413, 414 (2003); Phyllis Forrester Granade, *Medical Malpractice Issues Related to the Use of Telemedicine An Analysis of the Ways in Which Telecommunications Affects the Principles of Medical Malpractice*, 73 N.D. L. REV. 65, 90 (1997).

as the application of old law to new delivery mechanisms."[29] Similarly, John Blum demonstrated how traditional bases for the physician-patient relationship can be applied to telemedicine.[30] At the same time, these and other authors have used extraordinary language to describe the change brought on by telemedicine. Carl F. Ameringer, writing in the *Journal of Health Care Law and Policy,* states that "telemedicine's potential for altering the course of health care delivery is transcendent."[31] Blum himself notes that "unlike other changes . . . cybermedicine alters the core relationship between physician and patient by removing the once-constant element of physicality."[32] The existing scholarship regarding application of legal principles to telemedicine stands in sharp contrast to the exceptional language used to describe the potential change brought by telemedicine.

The question of legal disruption must be explicitly isolated from other forms of disruption. Lawrence Lessig identifies four modalities of regulation: law, market, norms, and architecture.[33] However, the four modalities do not exist in isolation; rather, "[c]hanges in any one will affect the regulation of the whole."[34] To contextualize within telemedicine, it is possible that new technology could disrupt the market sufficiently so as to make the concept of a hospital (and legal concepts like the corporate practice of medicine) unstable, thereby causing legal disruption. It is for precisely this reason that it is critical to specifically identify where legal disruption, as opposed to disruptions of norms or markets, occurs.

The potential for abuse of the language of disruption in telemedicine can be seen in other industries. Consider the disruption created by rideshare companies like Uber.[35] Legislators are unlikely to be concerned about potential harm to the taxi industry, presuming Uber's technology creates a better service for consumers.[36] Rather, the potentially convincing argument is that Uber unfairly classifies its drivers as independent contractors instead of employees, thereby avoiding labor regulations.[37] When the California Labor Commission held that certain Uber drivers are employees, the National

---

[29] Granade, *supra* note 28, at 90.

[30] Blum, *supra* note 28, at 414.

[31] Carl F. Ameringer, *State-Based Licensure of Telemedicine: The Need for Uniformity but Not a National Scheme*, 14 J. Health Care L. & Pol'y 55, 56 (2011).

[32] Blum, *supra* note 28, at 414.

[33] *See* Lawrence Lessig, Code: Version 2.0 123 (2006).

[34] *Id.*

[35] *See, e.g.*, Walter Isaacson, *How Uber and Airbnb Became Poster Children for the Disruption Economy*, N.Y. Times (June 19, 2017), http://www.nytimes.com/2017/06/19/books/review/wild-ride-adam-lashinsky-uber-airbnb.html; Arun Sundararajan, *Taxis, Hotels, What Industry Is Next To Be Disrupted by the New Economy*, The Wall St. J. (June 18, 2017), http://www.wsj.com/articles/taxis-hotels-what-industry-is-next-to-be-disrupted-by-the-new-economy-1497837840.

[36] Andre Andoyan, Note, *Independent Contractor or Employee: I'm Uber Confused! Why California Should Create an Exception for Uber Drivers and the 'On-Demand Economy'*, 47 Golden Gate U. L. Rev. 153, 155 (2017).

[37] *See id.*

Taxi Workers Alliance president celebrated that there finally exists "a set of laws Uber has not been allowed to violate or skirt."[38]

If those who stand to lose from telemedicine's potential market disruption are instead able to frame the issue as a threat to the legal underpinnings of health law, telemedicine's impact may be unfairly limited. Alternatively, if telemedicine proponents can falsely claim that detractors are actually masking their economic incentives despite legitimate potential for legal disruption, telemedicine will be adopted before legal structures can effectively adjust. As this Article demonstrates, however, the extent of regulation in health care does not translate into rigid legal doctrine. In fact, a theme of consent, either on behalf of the physician, state government, or patient, emerges across the issues. It is no surprise that various critical health law doctrines have already survived decades of pivotal changes to the industry. Though the removal of the physical component of the relationship with providers is significant, it does not diminish the fundamentally consensual nature of our health care system. As a result, telemedicine does not legally disrupt health law.

III. TELEMEDICINE AND THE PHYSICIAN-PATIENT RELATIONSHIP

A. Consent Is The Basis For The Physician-Patient Relationship

Telemedicine's most fundamental and tangible threat to the medical-legal framework is that it removes the physicality from the physician-patient relationship. John D. Blum suggests that the physician-patient dyad constitutes the basic structure of medicine historically, though we have certainly moved far from that with the introduction of hospitals, corporate practice of medicine, and managed care.[39] Blum further acknowledges that "[t]he element of physicality may be traditional, but it is not essential to the existence of the physician-patient relationship."[40] The basic foundation of the physician-patient relationship is contractual consent, and a physical meeting is simply one way of demonstrating consent. Telemedicine is not legally disruptive of the physician-patient relationship because consent to such a relationship can be established virtually.

The question of how the physician-patient relationship will be changed by telemedicine has been at the forefront of telemedicine literature for decades. Writing in 1997, Phyllis Forrester Granade identified five questions a court asks to determine if a physician-patient relationship exists:

> (1) [W]hether the consultant and the patient have met; (2) whether the consultant ever examined the patient; (3) whether the patient's records were ever viewed by the consultant; (4) whether the consulting physician knew the patient's

[38] *Taxi Workers Respond to California Labor Commission Game Changer Ruling: Uber Drivers Are Employees*, Nat'l Taxi Workers Alliance (June 17, 2015), http://static1.squarespace.com/static/551c0fb1e4b04e2cba203b00/t/5581cfa2e4b03cc04d6801ad/1434570658578/NTWA+and+SFTWA+Respond+to+CA+Labor+Commission+Ruling+on+Uber+Driver+Employee+Status.pdf.

[39] *See* Blum, *supra* note 28, at 413.

[40] *See id.* at 448.

name; and (5) whether the consultation was gratuitous or for a fee. Importantly, only a few of these elements must be met to establish a relationship.[41]

Each of these areas require action on the part of the physician. Physician consent is a necessary and fundamental component of the physician-patient relationship.[42] The Federation of State Medical Boards recommends in its telemedicine policies that "the relationship is clearly established when the physician agrees to undertake the diagnosis and treatment of the patient, and the patient agrees to be treated, whether or not there has been an encounter in person between the physician . . . and [the] patient."[43]

Childs v. Weis, through a disturbing set of facts due to the element of racism, demonstrates the contractual nature of the relationship.[44] In *Childs*, a pregnant African American woman traveling through rural Texas presented herself to the Greenville Hospital emergency room.[45] The nurse examined her, then called the doctor and informed him there was "a negro girl in the emergency room" having pregnancy-related issues.[46] The nurse advised the woman to drive back to her own doctor in Dallas. While driving back to her hospital, the woman gave birth, but the child ultimately died within twelve hours.[47] The court held that there was no physician-patient relationship, as the relationship "in its inception is basically contractual and wholly voluntary, created by agreement express or implied, and which by its terms may be general or limited."[48] Since the doctor never agreed to treat the patient and sent the patient away, no duty existed.

Concerns regarding the physician-patient relationship are especially relevant because establishing the existence of such a relationship is necessary in a medical malpractice case. In the standard framework for a common law tort of duty-breach-causing-injury, the physician-patient relationship is required to establish the duty.[49] In the early days of telemedicine, there was a swath of scholarship addressing the coming crisis for practitioners in terms of medical malpractice risk, but these concerns were overblown given that telemedicine has remained mostly limited to areas of medicine with limited numbers of claims (e.g., primary care). In fact, there have been a bafflingly low number of claims. Teladoc announced in 2016 that it had zero malpractice claims in its first one

---

[41] *See* Granade, *supra* note 28, at 69 (1997) (citations omitted).

[42] Valarie Blake, *When Is a Patient-Physician Relationship Established?*, 14 AM. MED. ASS'N J. ETHICS 403, 404 ("As a general rule, physicians are under no obligation to treat a patient unless they choose to.").

[43] MODEL POLICY FOR THE APPROPRIATE USE OF TELEMEDICINE TECHNOLOGIES IN THE PRACTICE OF MEDICINE, FEDERATION OF STATE MEDICAL BOARDS (2014), http://www.fsmb.org/siteassets/advocacy/policies/fsmb_telemedicine_policy.pdf.

[44] *See* Childs v. Weis, 440 S.W.2d 104, 106 (Tex. App. 1969). This case occurred before the passing of the Emergency Medical Treatment and Labor Act (EMTALA), which requires treatment of anyone presenting to an emergency department.

[45] *Id.* at 105.

[46] *Id.* at 106.

[47] *Id.* at 105.

[48] *Id.* at 107 (quoting *Agnew v. Parks*, 343 P.2d 118, 123 (1959)).

[49] *See* Miller v. Schaefer, 559 A.2d 813, 819 (Md. App. 1989) ("Before a physician may be found liable for an act of medical malpractice, it is essential that a patient-physician relationship be in existence at the time the alleged act occurred.").

million visits.[50] The Medical Director of American Well, another very large provider of telemedicine services, stated in 2014 that "[not] only have we not had any malpractice claims, we've not had any physicians brought before medical boards."[51] As telemedicine technology improves and allows for more complex medical encounters without in-person meetings this may change, but as of now the telemedicine malpractice crisis has been utterly absent.

B. Current Laws Already Allow Physician-Patient Relationships Without Physical Interaction

Telemedicine does not present the first occasion on which doctors have practiced medicine on individual patients without being physically present. In an extreme example, a lower court in New York considered whether a patient simply telephoning to schedule an appointment created a physician-patient relationship.[52] The court denied a motion for summary judgment by the defendant, concluding that whether there was a physician-patient relationship based upon the scheduled appointment was a question of fact for the jury.[53] In another case, Dr. Rodriguez, a general practitioner with staff privileges at a hospital who was on call approved the transfer of an eight-month pregnant patient to another hospital based only on a recitation of the circumstances on the phone with two nurses.[54] The patient died during the trip, and the court found that "in evaluating the status of Mrs. Wheeler's labor and giving his approval, [Dr. Rodriguez] established a doctor-patient relationship with Mrs. Wheeler and accepted the duties which flow from such a relationship."[55] Before the advent of telemedicine, physicality was not a necessary component of the physician-patient relationship.

This has been particularly true in the area of physician-to-physician consultations. Courts have been consistently willing to find a physician-patient relationship to exist (given certain factual circumstances) in the context of such consultations, even though the doctor never actually speaks with the patient. In *Cogswell v. Chapman*, an infant arrived at the emergency room with an eye injury from a fishing accident.[56] The defendant, William Eichner, was a "courtesy/consulting physician at the hospital" and only provided a recommended treatment via a phone call to the emergency room physician.[57] The court acknowledged that "exposure to liability of a consulting physician is limited," but nevertheless affirmed that an issue of fact existed regarding Eichner's potential physician-patient relationship.[58] In general, as Phyllis Forrester Granade has

---

[50] Alan Roga & Henry DePhillips, *Telehealth: 1 Million E-Visits And 10 Lessons Learned*, Teladoc (Feb. 24, 2016), http://communications.teladoc.com/resources/Teladoc1millione-visits10lessonslearned.pdf.

[51] Neil Chesanow, *Do Virtual Patients Increase Your Risk of Being Sued?*, Medscape (Oct. 22, 2014), http://www.medscape.com/viewarticle/833254.

[52] Bienz v. Cent. Suffolk Hosp., 557 N.Y.S.2d 139, 139 (N.Y. App. Div. 1990).

[53] *Id.* at 140.

[54] Wheeler v. Yettie Kersting Mem'l Hosp., 866 S.W.2d 32, 35 (Tex. App. 1993).

[55] *Id.* at 40.

[56] Cogswell v. Chapman, 672 N.Y.S.2d 460, 461 (N.Y. App. Div. 1998).

[57] *Id.* at 460.

[58] *Id.* at 462.

acknowledged, "[N]o physician-patient relationship develops between the patient and the consultant if the consultant informally offers his or her opinion to another physician regarding an anonymous patient's care."[59] If the consultation occurs in a more formal, scheduled setting, however, a relationship will likely be established.

When a physician is an employee of the same hospital and consistently serves as a consulting physician, especially in a specialist role, courts are more likely to find a physician-patient relationship.[60] Courts are also likely to establish such a relationship if the physician recommends a specific course of medical treatment, reviews the patient's chart, and performs similar actions that constitute the practice of medicine.[61] Physicians who serve as a hospital resource for certain types of patients are presumed to have accepted a duty towards the patients on the other end of their medical opinion without having met them.[62] Alternatively, an occasional willingness to provide a doctor with advice appears far from consent to a relationship. In the context of consultations, actually seeing the patient is a presumably sufficient but not necessary component of establishing a physician-patient relationship.

The ability to hold managed care organizations accountable for medical malpractice further demonstrates that physicality is not an absolute requirement of the physician-patient relationship. To be clear, this does not refer to cases in which doctors, ostensibly working as independent contractors, are found to actually act as employees or apparent agents of the managed care organization.[63] This is unlike a claim of corporate negligence under the doctrine relied upon *Thompson v. Nason Hospital*.[64] Rather, courts have demonstrated a willingness to find managed care organizations liable for effectively practicing medicine not in accordance with the standard of care. In *Shannon v. McNulty*, the plaintiff suffered from labor complications and spoke with registered nurses via an on-call number that HealthAmerica, the plaintiff's Health Maintenance Organization (HMO), provided for emergency purposes.[65] The underlying rationale of the decision is that the HMO "was under a duty to oversee that the dispensing of advice by those nurses would be performed in a medically reasonable manner."[66] The HMO had entered into a physician-patient-like relationship by providing the emergency nurse service and

---

[59] *See* Granade, *supra* note 28, at 69.

[60] *But see, e.g.*, Gilbert v. Miodovnik, 990 A.2d 983 (D.C. Ct. App. 2010) (holding that obstetrician did not have physician-patient relationship and therefore no obligation to intervene in plans developed by nurse-midwives).

[61] *See id.* at 1004-11 (J. Ruiz, dissenting).

[62] *See, e.g.*, Corbet v. McKinney, 980 S.W.2d 166, 169 (Mo. Ct. App. 1996) ("Where the consultant physician does not physically examine or bill the patient, a physician-patient relationship can still arise where the physician is contractually obligated to provide assistance in the patient's diagnosis or treatment and does so.").

[63] For an example of a managed care organization being held liable in such a case, see Petrovich v. Share Health Plan of Illinois, Inc., 719 N.E.2d 756 (Ill. 1999).

[64] 591 A.2d 703 (Pa. 1991) (finding four potential duties of hospitals under which corporate negligence claims could succeed).

[65] 718 A.2d 828 (Pa. Super. Ct. 1998)

[66] *Id.* at 836.

was accordingly liable.[67] Evidently, physicality is better understood as a strong signal of consent rather than itself being the basis for a physician-patient relationship.

C. After Formation, Legislation Can Restrict The Extent Of The Physician-Patient Relationship

Telemedicine does not necessarily challenge the core legal underpinning of the physician-patient relationship. Physicians and their patients can certainly consent via the internet; individuals and organizations consent to all forms of agreements online. This is not to say, however, that telemedicine presents no threats to the role of consent in the physician-patient relationship. Indeed, telemedicine companies have apparently gone out of their way to attempt to claim that its doctors were *not* entering into physician-patient relationships.[68] Much of the legislation responding to telemedicine in the context of the physician-patient relationship focuses on ensuring that telemedicine is not treated as an exception to the standard doctrine.

Many states have passed laws, through their Medical Boards or otherwise, confirming that a physician-patient relationship may exist through telemedicine.[69] Arkansas, for example, recently passed an amendment to its Medical Practice Act specifically including the following as a potential method of establishing a physician-patient relationship: "The physician performs a face-to-face examination using real time audio and visual telemedicine technology that provides information at least equal to such information as would have been obtained by an in-person examination."[70] Arkansas repealed the law this year under the Telemedicine-Arkansas Internet Prescription Consumer Protection Act and now requires an in-person relationship before telemedicine can be utilized.[71] The Tennessee Board of Medical Examiners adopted a policy similar to the original Arkansas policy, stating that "[a] physician-patient relationship exists when a physician serves a patient's medical needs whether or not there has been an encounter in person between the physician and patient."[72] States are clarifying through legislation what likely would have been presumed by courts anyway: physician-patient relationships are established through telemedicine just like through in-person interactions via consent.

Simply acknowledging that telemedicine establishes a physician-patient relationship fails to address the real challenge of what exactly doctors can do via telemedicine. States are more aggressively reining in the extent to which virtual interactions may lead to serious medical decision-making. This issue is particularly pronounced in the prescribing of dangerous narcotics. One recent study focusing on Sinusitis and Urinary

---

[67] *Id.*

[68] Colette DeJong et al., *Websites That Offer Care Over the Internet: Is There an Access Quality Tradeoff?*, 311 J. Am. Med. Ass'n 1287, 1288 (Apr. 2, 2014) ("[A]nd one [website] asserts that its service 'does not constitute a physician-patient relationship.'").

[69] *See* Advocacy Resource Center, *50-State Survey: Establishment of a Patient-Physician Relationship Via Telemedicine*, Am. Med. Ass'n (2018) [hereinafter, *AMA 50-State Survey*], http://www.ama-assn.org/system/files/2018-10/ama-chart-telemedicine-patient-physician-relationship.pdf

[70] Ark. Code Ann. § 17-80-118.

[71] 2017 Ark. Acts 203.

[72] Tenn. Code Ann. § 0880-02-16 (West 2017).

Tract Infections found that "physicians were more likely to prescribe an antibiotic at an e-visit for either condition," describing this as a "conservative approach" when physicians cannot see the patient in person.[73] The rise of on-demand prescriptions is a serious concern for telemedicine. One website, Ezdoctorsrx.com, at least for some time guaranteed a prescription or your money back.[74] In the early days of telemedicine, there were many companies that appeared to serve as easy methods of obtaining prescriptions. The Federation of State Medical Boards issued guidelines recommending that issuing prescriptions based solely on an online questionnaire is not appropriate.[75] Now, states are enacting regulation to resist the easy transmission of prescriptions via telemedicine.

Many states have passed blanket bans on the prescription of dangerous drugs via telemedicine. In 2015, Connecticut passed An Act Concerning the Facilitation of Telehealth, which included the provision that "no telehealth provider shall prescribe Schedule I, II, or III controlled substances through the use of telehealth."[76] Delaware takes a different approach, prohibiting pharmacists from dispensing prescription drugs if he or she knows that the prescription stemmed only from a telemedicine consultation.[77] There is undeniably a relationship in that legislators want to limit the prescription of drugs because telemedicine, in its current technological state, may not be an appropriate avenue for *this type* of physician-patient relationship. The contractual core of the physician-patient relationship remains, but these laws limit what care may be provided under the contract.

Limitations on the extent of the physician-patient relationship is not unique to telemedicine. Established health law doctrine recognizes the need to limit the actions of licensed physicians. The contractual requirement of informed consent demands, for example, that "a physician is under a legal duty to disclose to the patient all material information."[78] Therefore, doctors cannot perform procedures or recommend courses of action without making the patient aware of the relevant risks.[79] If a physician practices outside their area of expertise they are much more likely to be held liable for violating the standard of care and face sanctions from the state medical board.[80] The fact that there must be new rules regarding what types of interactions can legally occur via telemedicine is not a disruption of the underlying law. Simply because a new technology complicates a doctrine or demands assessment of new questions does not create legal disruption. Therefore, physician-patient relationship established through

---

[73] Ateey Mehrotra et al., *A Comparison of Care at E-Visits and Physician Office Visits for Sinusitis and Urinary Tract Infection*, 173 J. Am. Med Assn'n.: Internal Med. 72, 73 (2013).

[74] DeJong et al., *supra* note 68, at 1287.

[75] *See* Regina A. Bailey, *The Legal, Financial, and Ethical Implications of Online Medical Consultations*, 16 J. Tech. L. & Pol'y 53, 63 (2011).

[76] An Act Concerning the Facilitation of Telehealth, 2015 Conn. Acts No. 15-88(11)(c) (effective Oct. 1, 2015).

[77] Safe Internet Pharmacy Act, Del. Code Ann. tit. 16 § 4744 (2017).

[78] Arato v. Avedon, 858 P.2d 598, 607 (Cal. 1993).

[79] *Id.* at 599.

[80] *See* Johnson by Adler v. Kokemoor, 545 N.W.2d 495 (Wis. 1996) (holding that evidence regarding surgeon's lack of expertise with particular procedure was admissible).

telemedicine should be regulated in accordance with the constraints applied to all physician-patient relationships.

Another meaningful complication to the physician-patient relationship in telemedicine comes at the point of termination: how, precisely, does a doctor terminate a virtual physician-patient relationship? *Ricks v. Budge* provides a quintessential description of the obligations of doctors when it comes to termination.[81] A doctor treated a patient's hand injury and told him to come back if the injury got worse. When the patient returned, the doctor refused treatment because the patient had yet to pay his bills.[82] The patient walked in the rain to another hospital and ultimately had to have his finger amputated. The court described the obligation of a physician in an ongoing relationship as follows: "The obligation of continuing attention can be terminated only by the cessation of the necessity which gave rise to the relationship, or by the discharge of the physician by the patient, or by the withdrawal from the case by the physician after giving the patient reasonable notice."[83] This continues to reflect the state of the law and the contractual nature of the physician-patient relationship.

Telemedicine complicates the matter. Many telemedicine companies will match patients with any qualified doctor, lacking the priority of maintaining long-term physician-patient relationships. This is not inherent to telemedicine by any means, but it is apparent in many companies' business models.[84] Telemedicine highlights the expected tradeoff between instant access and the guarantee of meeting with your personal physician.[85] If a patient presents via telemedicine with a chronic illness, such as diabetes, however, a more difficult set of questions arises.[86] American Well, one of the largest telemedicine companies, explicitly tells its doctor that it "operates as an urgent care model."[87] But what if a patient presents with a potential respiratory infection but then is diagnosed with a chronic illness—does the physician have an obligation to treat the chronic condition?

Consent again becomes relevant in the context of termination. As Granade explains regarding these "abandonment" claims in the case of telemedicine, there must be "unilateral severance of the physician-patient relationship by the doctor" in order to

---

[81] Ricks v. Budge, 64 P.2d 208, 212 (Utah 1937).

[82] *Id.* at 210.

[83] *Id.* at 211.

[84] *See, e.g.*, DeJong et al., *supra* note 68, at 1288 ("Most websites do not allow patients to request repeat visits with a particular physician.").

[85] In fact, telemedicine arguably has the most promise in the area of chronic disease management where patients may be less mobile and require a large quantity of physician interactions. For a meta-assessment of telemedicine's use in chronic diseases, see Richard Wootton, *Twenty Years of Telemedicine in Chronic Disease Management An Evidence Synthesis*, 18 J. TELEMEDICINE & TELECARE 211, 211 (2012).

[86] This actually happening, as of now, is very unlikely. For one, most telemedicine companies have disclaimers explicitly limiting what type of illnesses patients may be treated for on the website. *But see* Jonah Comstock, *Teladoc Plans Chronic Condition-Focused Program by Year's End*, MOBIHEALTH NEWS (May 18, 2016), http://www.mobihealthnews.com/content/teladoc-plans-chronic-condition-focused-programs-years-end.

[87] *See* Telemedicine Physicians, *Frequently Asked Questions*, American Well, http://providers.americanwell.com/telemedicine-faqs.

have a claim.[88] This is a reasonable standard, as patients should always have the ability to opt out of the relationship but cannot continue to hold the physician liable. Telemedicine can permissibly limit the extent of the physician-patient relationship to the relevant encounter as a result. The law can also recognize that consumers are typically aware of the fact that they are only receiving episodic treatment through telemedicine.

This is precisely what Ohio law does by finding that explicit notice of termination is not required when "[t]he physician rendered medical service to the person on an episodic basis . . . and the physician should not reasonably expect that related medical service will be rendered to the patient in the future."[89] In general, it seems that telemedicine companies are relying on their respective business models to channel patients into the appropriate physician-patient relationship.

The formation of the physician-patient relationship can clearly occur via telemedicine.[90] The actual contents of such a relationship and its potential termination pose more difficult challenges, but ones that can still be reconciled through the existing legal framework. This entire argument is naturally contingent upon the presumption that we believe telemedicine is a valuable technology. If evidence mounts that telemedicine interactions are creating significant harm, the technology can be limited through state legislatures and medical boards. Medicine is heavily regulated and there is considerable risk (i.e., loss of license and prison) for practicing illegally.[91] Alternatively, in the area of international law, a ban may or may not be effective depending on a variety of factors.[92] The fact that regulation can limit telemedicine with such certainty means legal disruption will be a consequence of policy judgments and not the inevitable consequence of the technology's existence.

IV. TELEMEDICINE AND PHYISICIAN LICENSURE

A. State Power to Protect Its Citizens is the Basis For Our Licensure System

The ability of the state to regulate itself under the police power is a core component of the U.S. Constitution's federalist structure. The Supreme Court affirmed this principle in *Dent v. West Virginia*, unanimously upholding a state statute restricting the right to practice medicine.[93] The Court gave significant deference to the right of the states despite a then-recognized countervailing individual right to pursue a profession of one's choosing.

> The power of the State to provide for the general welfare of its people authorizes it to prescribe all such regulations as in its judgment will secure or tends to secure them against the consequences of ignorance and incapacity, as well as deception and fraud. As one means to this end, it has been the

---

[88] *See* Granade, *supra* note 28, at 83.

[89] Ohio Rev. Code. Ann. § 4731.27.02(B)(1).

[90] *See AMA 50-State Survey*, *supra* note 69.

[91] Tex. Occ. Code § 165.153.

[92] *See* Rebecaa Crootof, *The Killer Robots Are Here: Legal and Policy Implications*, 36 Cardozo L. Rev. 1837, 1884-90 (2015) (providing eight factors relevant to the effectiveness of a weapons ban).

[93] 129 U.S. 114 (1889).

> practice of different States, from time immemorial, to exact in many pursuits a certain degree of skill and learning upon which the community may confidently rely. The nature and extent of the qualifications required must depend primarily upon the judgment of the State as to their necessity.[94]

The right of a state to control medical licensing, therefore, remains strongly supported by existing precedent.[95] Like other forms of occupational licensing, the right to control the quality of medical services is a core function of state government.

The policy logic of state-based licensing of medicine, however, has received significant pushback as telemedicine becomes more attractive. As physicians become capable of treating patients throughout the country via virtual visits, the requirements of state-based licensing limit physicians to treating patients only in those states in which they are licensed. One scholar identified the tension between the parochial state-based licensing system and technological advances in medicine.[96] Some have argued that the location of the physician, not the patient, should define the relevant licensing, but this view has been consistently rejected in court.[97] Teladoc, one of the earliest and largest telemedicine companies, successfully obtained a preliminary injunction against a Texas Medical Board regulation effectively preventing the practice of telemedicine on anti-trust grounds.[98] Challenges to the state-based regulation of telemedicine are evidently coming from all angles.[99]

To be clear, this Article does not contend that the state-based licensing system is necessarily optimal. Rather, it recognizes that the right of a state to control occupational licensing is the legal underpinning of the current licensure system, as confirmed in *Dent*.[100] The key question, then, is whether the state-based licensing system can and should withstand the development of telemedicine. Put another way, does the removal of physicality (i.e., the patient being in the room with the doctor) fundamentally alter the underlying logic of the regulatory scheme for licensing? While telemedicine certainly demands new policies, it should not disrupt our recognition of states' occupational licensing rights in our federalist system for two reasons: first, this issue has already been presented and adequately address in other forms; second, there are innovative means of reconciling telemedicine with the existing licensing system, most notably through interstate licensure compacts.[101] Telemedicine would be disruptive of current licensure

---

[94] *Id.* at 122.

[95] *But see* Bill Marino et al., *A Case for Federal Regulation of Telemedicine in the Wake of the Affordable Care Act*, 16 COLUM. SCI. & TECH. L. REV. 274 (arguing that recent Supreme Court decisions have increased the authority of Congress to regulate health, and therefore a federal licensure scheme would likely be constitutional).

[96] Sulentic, *supra* note 2, at 4.

[97] *See* Ameringer, *supra* note 31, at 58 (describing the "general consensus" among state boards that patient location is dispositive for jurisdictional purposes).

[98] Teladoc, Inc. v. Tex. Med. Bd., No. 1-15-CV-343 RP, 2015 WL 8773509 (W.D. Tex. Dec. 15, 2015).

[99] *See id.*

[100] Dent v. West Virginia, 129 U.S. 114, 128 (1889).

[101] *See infra* Section IV.C.

laws if it became optimal to grant licensing control to another body (e.g., the federal government) in order to accommodate the benefits of telemedicine.

B. States Already Allow the Interstate Practice Of Medicine In Various Forms

Before considering how states and institutions respond to a new technology, the existing scheme may instruct how to address similar challenges. This section describes where the state-based licensing system has given way to allow effective health care operations, namely consultations by out-of-state physicians and treatment by physicians when a patient is traveling out of state. In each area, state-based licensing tends to bend but not break.

When it comes to consultations from out-of-state doctors, there is a clear willingness to bypass the state-based licensing requirement. The logic behind such policies is that doctors should be able to consult with specialists and other doctors that may not be licensed in the state where the patient is located. California has an explicit consultation exception, though the out-of-state physician may not have "ultimate authority over the care or primary diagnosis of a patient who is located within [California]."[102] Ohio offers a similar exception as long as the physician does not provide regular or frequent consultation, provides the consultation without compensation, or the consultation is provided as part of a medical school curriculum.[103] It would be difficult to classify such consultations as anything but the practice of medicine, even if the out-of-state physician never actually speaks with the patient. The physicians are clearly advising on a specific course of treatment based upon their knowledge as a physician. Yet state law recognizes the desirability of such consultations, and therefore allows an exception to its licensure laws.

Another notable exception is one that most health care consumers likely take for granted: the ability to receive treatment from an at-home physician while traveling out of state.[104] A patient on vacation in California gets a virus and calls her primary physician in New York, who prescribes some sort of medication to a local pharmacy. Ohio allows a physician from another state to provide "follow-up services in person or through the use of any communication" for one year after the last date that services were provided.[105] State control still governs these physician-patient interactions, but exceptions are allowed in the interest of the health and safety.

There are a variety of other exceptions to physician licensure laws that I have not assessed in full detail here, such as emergency situations,[106] military exemptions,[107]

---

[102] CAL. BUS. & PROF. CODE § 2060 (West 2017).

[103] OHIO REV. CODE. ANN. § 4731.36(A)(3) (West 2017).

[104] This service is being offered by innovative companies like One Medical. *See* Susan Owen, *4 Ways To Use Virtual Care at One Medical* (Jan. 9, 2018), http://www.onemedical.com/blog/get-well/virtual-care-faq.

[105] OHIO REV. CODE. ANN. § 4731.36(A)(4) (West 2017).

[106] *Id.*

[107] All 50 states allow for a military exception. A physician with one state license commissioned in the military may legally practice in all 50 states. *See* CENTER FOR TELEHEALTH AND E-HEALTH LAW,

border state exceptions,[108] and even exceptions for visiting sports team trainers.[109] The takeaway from this section is that while state control is the core legal backbone of existing licensure law, various exceptions to this requirement are already recognized. Any argument that telemedicine requires a fundamental shift in our licensing system ought to acknowledge that our deference to state control does not necessarily result in an extremely rigid system.

C. States Can Achieve The Benefits Of Telemedicine Through Interstate Licensure And Other Legislative Initiatives

States currently have the right to establish requirements for the practice of medicine in their state. A state also has the right, therefore, to offer a significantly expedited licensing process for individuals that have already been vetted by some other credible institution (e.g., another state's licensing board). Such processes are particularly attractive for areas in which a state has a shortage of licensed doctors. This is the basic theory behind interstate licensure compacts, in which participating states create fast-track license application processes for those with licenses in other states that are members of the compact.[110] Note, critically, that this does not necessarily create a new national licensing standard. Individual doctors must still obtain licenses in all states in which they practice, but the process is meaningfully easier.[111] Such compacts have been used effectively in the area of nursing for nearly two decades. In 1998, the National Council of State Boards of Nursing (NCSBN) promulgated the Nurse Licensure Compact.[112] Since that time, twenty-five state legislatures have passed statutes recognizing the compact.[113] Similar efforts have been made for EMS personnel.[114]

The attempt to create an interstate compact for doctors' licenses has been an even more controversial affair, though a recent agreement is cause for optimism on the issue. The Federation of State Medical Boards created and endorsed the Interstate Medical Licensure Compact (IMLC) in 2014.[115] Twenty-eight states participate in the IMLC, and supportive legislation has been introduced in six additional states.[116] Responses to the compact have been mixed. One author suggests that the compact will "undermin[e] state sovereignty, as well as increas[e] the power of a private bureaucratic organization to

---

Executive Summary: New Jersey Physician Licensure Statute, 3, http://ctel.org/annotated_states/New_Jersey_Annotated__%20(2579609_1).pdf.

[108] N.Y. Educ. Law § 6526.2 (McKinney 2017).

[109] Ky. Rev. Stat. Ann. § 311.560(2)(d) (West 2017).

[110] Interstate Medical Licensure Compact, http://imlcc.org/.

[111] *Id.*

[112] American Nurses Ass'n, *Interstate Nurse Licensure Compact* (2016), http://www.nursingworld.org/practice-policy/advocacy/state/interstate-nurse-compact2.

[113] Nat'l Council of State Boards of Nursing, Nurse Licensure Compact (NLC) (2019), http://nurse.org/articles/enhanced-compact-multi-state-license-eNLC/.

[114] Nat'l Registry of Emergency Medical Technicians, *Recognition of EMS Personnel Licensure Interstate CompAct*, http://www.nremt.org/rwd/public/document/replica.

[115] *See* Interstate Medical Licensure Compact, *supra* note 112.

[116] *Id.* (noting that the Interstate Medical Licensure Compact is "an agreement between 28 states and 1 territory").

intervene in, define, and control the practice of medicine."[117] In many state legislatures, representatives advocating for the enactment argued that the bill would help address persistent doctor shortages, especially in rural areas.[118] While there are some legitimate complaints about the IMLC, a close reading indicates various ways in which it preserves the rights of states to control licensing. As Robert Pear acknowledged writing about the compact for the *New York Times*, "[I]t would preserve the authority of each state to regulate the practice of medicine within its borders."[119]

Simply because we can accommodate telemedicine through state-based licensing does not mean we should. Indeed, there is no denying that a national licensure scheme would more easily facilitate the use of telemedicine.[120] A technology is not legally disruptive, however, simply because existing doctrine cannot perfectly accommodate it. The IMLC can be viewed as a compromise position that maintains state control over licensing while recognizing the need for telemedicine to have a role in our health care system. Even imagining legal disruption as a spectrum where telemedicine is somewhat disruptive of the existing licensing scheme, the doctrine does not break.

States still retain significant control over licensing under the IMLC. First, and most transparently, the IMLC is entirely contingent upon the consent of the state legislatures.[121] As the model act makes clear, the IMLC simply "creates another pathway for licensure and does not otherwise change a state's existing Medical Practice Act."[122] The IMLC did not become binding on the original signatories, moreover, until at least seven states signed on.[123] Member states have considerable latitude to still deny an applicant for failing to meet any of the nine required criteria for physicians.[124] These criteria disqualify, for example, any physician whose license has received essentially any form of discipline from a licensing agency.[125] If a state has particularized continuing education requirements, the IMLC makes clear that participating physicians must comply.[126]

---

[117] Jeremy Snavely, Commentary, *The Interstate Medical Licensure Compact: Claims vs. Reality*, 20 J. Am. Physicians & Surgeons 20, 22 (2015).

[118] *See* Mike Richards, *Inviting Skilled Medical Practitioners to Washington*, Lens (Mar. 10, 2017), http://thelens.news/2017/03/10/allowing-expedited-interstate-licensing-for-medical-practitioners (quoting State Rep. Marcus Riccelli: "I know we're all passionate about our underserved and rural areas getting the access they need. [W]e know the technological advances made in telemedicine are a greater way to bring more doctors online faster.").

[119] Robert Pear, *Medical Boards Draft Plan To Ease Path to Out-of-State and Online Treatment*, N.Y. Times (June 30, 2014), http://www.nytimes.com/2014/06/30/us/medical-boards-draft-plan-to-ease-path-to-out-of-state-and-online-treatment.html.

[120] *See id.*

[121] Interstate Medical Licensure Compact § 20(d).

[122] *Id.* at § 1.

[123] *Id.* at § 20(b).

[124] *Id.* at § 2(k).

[125] *Id.* at § 2(k)(7).

[126] *Id.* at § 7(b).

Finally, and critically if one has a more jaded view of the licensure system, states may still charge licensing fees.[127]

The IMLC is the broadest method of reconciling the growth and desirability of telemedicine with the right of states to control medical licensing. At both the federal and state level, however, there have been other attempts at creating narrow carve-outs to the state-based licensing system. In 2011, Representative Glenn Thompson introduced the Servicemembers' Telemedicine and E-Health Portability Act of 2011.[128] This bill would have authorized the Secretary of Defense to allow licensed health care professional to provide care to members of the Armed Forces at any location and regardless of where the professional or patient are located.[129] In 2009, New Mexico passed a statute (since repealed) stating that the medical board of the state shall issue a specific telemedicine license to any applicant with an unrestricted license to practice medicine in another state.[130] Tennessee similarly offered a telemedicine license until October 2016, but applied a stricter standard of care to telemedicine.[131] Various laws with similar implications are currently being considered across the country.[132] Finally, and more narrowly, some states have reciprocity agreements only with bordering states.[133]

There is a fundamental tension between the extent to which such interstate compacts and other licensing accommodations can allow for telemedicine while respecting states' rights. A national licensing scheme, naturally, would be the most effective way to promote telemedicine, but would obviate the states' role in licensing. On the other end of the spectrum, a completely patchwork system of state schemes with unique licensing criteria would make interstate practice of telemedicine exceedingly difficult. The IMLC and other legislation fails to appreciate the immense logistical challenges of operating multiple state licenses. In one survey of practitioners who held multiple state licenses, those who encountered difficulty primarily identified "[d]o not respond to calls or e-mails" and "[d]o not provide updates as to what is missing" as the main issues.[134]

---

[127] *See id.* at § 6(a); *see also Universal Medical Licensing? Won't Happen*, PHYSICIAN'S WEEKLY (Sept. 8, 2014), http://www.physiciansweekly.com/universal-medical-licensing-doctors (arguing that protection of licensure fees constitutes the main reason for the maintenance of state-based licensure).

[128] Servicemembers' Telemedicine and E-Health Portability Act of 2011, H.R. 1832, 112th Cong. (2011).

[129] *See id.*

[130] N.M. STAT. ANN. § 61-6-11.1 (West 2017) (repealed 2016).

[131] *See generally* TENN. CODE. ANN. § 63-1-155; *see also* Tennessee Dep't of Health, *Telemedicine Rules Assigned Effective Date of October 31, 2016*, BOARD OF EXAMINERS ANNUAL NEWSLETTER 1 (Fall 2016) ("As of the rule's effective date [of October 31, 2016], the Board will no longer issue telemedicine licenses."), http://www.tn.gov/content/dam/tn/health/documents/Fall_2016_Newsletter.pdf.

[132] *See On Telehealth License Portability, Each State Follows its Own Path*, MHEALTH INTELLIGENCE (Jan. 28, 2016), http://mhealthintelligence.com/news/on-telehealth-license-portability-each-state-follows-its-own-path.

[133] *See* N.Y. YORK EDUC. LAW § 6526 (West 2017) (providing an example of the restrictions that often come with such reciprocity agreements).

[134] Herbert Rogove et al., *A Survey and Review of Telemedicine License Portability*, 21 TELEMEDICINE & E-HEALTH 374, 378 (2015).

As the researchers noted, respondents who identified unreasonable state boards gave reasons that "dealt primarily with communication issues."[135] By requiring doctors to obtain licenses in all states of practice, rather than an automatic reciprocity agreement, perhaps we are closer to the patchwork end of the spectrum than it would seem.

Other authors have more completely sketched out the models for responding to the licensure issues created by telemedicine.[136] This Article does not seek to provide a comprehensive analysis of the potential licensure systems. Rather, the objective is only to provide some emblematic examples and illustrate how these efforts attempt to maintain state control as the core structure of the licensing system.[137] The IMLC is precisely one way of answering this question while still respecting state control over licensing. In that regard, telemedicine's serious potential value to health care is accommodated under the existing legal regime.

V. TELEMEDICINE AND INFORMATION PRIVACY

A. Current Health Information Privacy Law Strikes A Difficult Balance Between Utility And Security

Samuel Warren and Justice Louis Brandeis warned as early as 1890 that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[138] The concern stemmed from the newly available technology of instantaneous photographs, a quite minor privacy threat relative to that posed by the potential release of Protected Health Information (PHI).[139] In the piece, Warren and Brandeis argue that the common law guarantees the right of each person to decide "to what extent his thoughts, sentiments, and emotions shall be communicated to others."[140] This argument is accepted in the courts, at least to an extent, but it only addresses the question of how to punish or compensate for invasions of privacy.[141] Alternatively, the challenge of privacy in medicine is how to regulate personal information that by necessity must be seen by at least some beyond the individual themselves.

---

[135] *Id.*

[136] *See* Heather A. Daley, *Telemedicine: The Invisible Barriers to the Health Care of the Future*, 9 ANNALS HEALTH L. 73, 89 (2000).

[137] *See* Sulentic, *supra* note 2, at 29 (identifying how the telemedicine licensing issue "merely restates a problem which predates the Constitution itself: how are the legislatures and the courts to deal with industrial or commercial problems that simply will not confine themselves to the boundaries of the state?").

[138] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[139] Under HIPAA, PHI includes all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media. PHI includes any information relating to past, present or future physical or mental health condition. 45 C.F.R. § 160.03.

[140] Warren & Brandeis, *supra* note 138, at 198.

[141] *See* Doe v. Medlantic Health Care Group, Inc., 814 A.2d 939 (D.C. Ct. App. 2003) (upholding claim of invasion of privacy where plaintiff's HIV infection became publicly known).

Privacy presents a distinct set of issues from those raised by licensing and the physician-patient relationship for three reasons.[142] First, regulation of privacy occurs through federal statute as opposed to state law (licensing) or a combination of state law and judicial doctrine (physician-patient relationship).[143] The key pieces of legislation are the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[144] and the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[145] Second, these regulations frequently attempt to hold possessors of private information liable for the criminal activities of other actors (e.g., hackers). Third, health care policy-makers mostly agree that the digitization of medicine, especially when it comes to Electronic Health Records (EHR), is a positive development. Since May 2011, more than $35 billion dollars in incentives have been awarded through the Medicare and Medicaid EHR Incentive Program.[146] The HITECH Act "allocates approximately $44,000 for each practicing clinician and between $2 million and $10 million for each hospital that qualifies as a 'meaningful' user of EHRs."[147] In early 2009, then President-Elect Obama announced the goal of computerizing all medical records within five years.[148]

There is a fundamental tradeoff between the digitization of medical records and protection of patient privacy. As Lawrence O. Gastin noted before HIPAA passed, some scholarship wrongfully "assumes that a significant level of privacy can coexist with the development of a modern health information infrastructure."[149] In fact, security

---

[142] This Part discusses the privacy component of PHI and does not focus on the data access component of health information. Many states have statutes guaranteeing patients access to their own health information. *See* Joy L. Pritts, *Altered States: State Health Privacy laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y, L., & ETHICS 327, 329 (2002); *see also* Hugo Campos, *The Heart of the Matter: I Can't Access the Data Generated by My Implanted Defibrillator: That's Absurd*, SLATE (Mar. 24, 2015) (arguing for stronger rights to the data created by various medical technologies), http://www.slate.com/articles/technology/future_tense/2015/03/patients_should_be_allowed_to_access_data_generated_by_implanted_devices.html.

[143] Privacy is hardly an exclusive concern of the federal government, and states are generally not preempted from creating additional privacy protections to supplement the federal laws. *See, e.g.*, Yath v. Fairview Clinics, N.P., 767 N.W.2d 34 (Minn. Ct. App. 2009) (holding that Minnesota's law providing private right of action for HIPAA violations was not preempted).

[144] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[145] The HITECH Act was enacted as an amendment under the investment recovery act following the late 2000s financial crisis. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 Div. A tit. XIII, 111th Cong. (2009).

[146] *See Payment Data: State Breakdown of Payments to Medicare and Medicaid Providers Through February 28, 2017*, CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS), http://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/dataandreports.html.

[147] Ashish K. Jha, *Meaningful Use of Electronic Health Records: The Road Ahead*, Commentary, 304 J. AM. MED. ASS'N 1709, 1709 (2010).

[148] Dan Childs et al., *President-Elect Urges Electronic Medical Records in 5 Years*, ABC NEWS (Jan. 9, 2009), http://abcnews.go.com/Health/President44/story?id=6606536.

[149] Lawrence O. Gastin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 454-55 (1995) (footnote omitted).

has proven difficult in practice.[150] In 2015 alone, over 113 million health care related records were stolen; health care suffered more data breaches than any other industry, including government and retail.[151] Yet the push for health care digitization continues, albeit with attempts along the way to protect PHI.[152]

The Supreme Court has recognized that the potential for a privacy violation does not constitute a violation of privacy alone.[153] In *Whalen v. Roe*, the Court considered the constitutionality of the New York State Controlled Substances Act of 1972.[154] The Act required the creation of a centralized computer file that tracked the name and addresses of all individuals who had been prescribed certain dangerous drugs. The Court acknowledged the "threat to privacy implicit in the accumulation of vast amounts of personal information."[155] Nevertheless, the Court held that New York's statute "evidence[d] a proper concern with, and protection of, the individual's interest in privacy."[156] Therefore, while some courts recognize a constitutional right to the privacy of health information, the mere existence of potential privacy invasions does not raise constitutional concerns.

The basic legal and policy underpinning of data privacy in health care is a balance between utility and security. HIPAA, for the most part, requires providers to act according to standards instead of follow rules. As Peter A. Winn has argued when describing the lack of privacy in a hospital setting, "[h]ospital stays are notoriously non-private affairs."[157] The drastic increase in digitization, however, has certainly made the issue more prominent and potentially dangerous. Telemedicine fundamentally disturbs this equilibrium by pushing another meaningful component of health care—the consultation itself—online. This shift creates new demands on providers to ensure adequate privacy protections of audio and video communications. The basic legal doctrine, however, remains the same: providers must protect patient data to the best extent possible and patients must be wary of the risk of breaches.

---

[150] *Id.* at 493.

[151] Mayra Rosario Fuentes, Forward-Looking Threat Research Team, *Cybercrime and Other Threats Faced by the Healthcare Industry*, TrendMicro (2017), http://www.trendmicro.com/content/dam/trendmicro/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf (noting that in 2015, 113.2 million healthcare-related records were stolen).

[152] There are efforts to utilize machine learning, artificial intelligence, and other advanced technologies to improve image recognition in radiology. For a discussion of privacy concerns amidst this initiative, see Filippo Pesapane et al., *Artificial Intelliegence as a Medical Device in Radiology: Ethical and Regulatory Issues in Europe and the United States*, 9 Insights into Imaging 745 (2018).

[153] Whalen v. Roe, 429 U.S. 589 (1977).

[154] *Id.* at 600.

[155] *Id.* at 605.

[156] *Id.*

[157] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 Rutgers L. J. 617, 623 (2002).

B. Existing Regulation Of E-Mail And Data Breaches Promote Digitization

Online medical consultations do not constitute the first electronic communication of sensitive health information between physicians and their patients. The regulation surrounding the use of e-mail and text messaging provides a useful point of initial comparison. Doctors may legally use non-encrypted e-mail services (e.g., Gmail) to communicate with their patients, but there are significant limitations on this use.[158] For example, doctors must take certain precautions when sending the e-mail (*e.g.*, double-check the recipient) and, more importantly, should "limit the type of information disclosed" through the messages.[159] In order to be HIPAA compliant in e-mail use, a provider still must meet the security requirements outlined by HIPAA, such as access, control, and integrity.[160] While HIPAA requires certain security measures (*e.g.*, unique user identification),[161] encryption is considered "addressable" and only required whenever deemed appropriate.[162] As one advisory organization put it, "Essentially, you can send [electronic protected health information] via email, but you have to do it securely, on HHS terms."[163]

The patient plays a meaningful role on this issue and may consent to the use of an unencrypted communication as long as the provider has advised the patient of the risk.[164] The theme of consent emerges again, this time with the patient able to accept data privacy risks in exchange for the value of seamlessly communicating with their provider.[165] The regulation of e-mail demonstrates that the general requirement for cybersecurity is not a demand for absolute security at all costs but rather a desire for balancing utility and security.[166]

---

[158] Office for Civil Rights, *Does the HIPAA Privacy Rule Permit Health Care Providers To Use E-mail To Discuss Health Issues and Treatment with Their Patients*?, U.S. DEP'T OF HEALTH AND HUMAN SERVICES (Dec. 15, 2008) [hereinafter *Privacy Rule & E-mail*] , http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients.

[159] *Id.*

[160] *See* 45 C.F.R. § 164.312; *see also Privacy Rule & E-mail*, *supra* note 158.

[161] 45 C.F.R. § 164.312(a)(2)(i) (2013).

[162] 45 C.F.R. § 164.312(e)(2)(ii) (2013). "Addressable" means that encryption is not fully mandatory and need only be implemented after a determination by the entity that it is a "reasonable and appropriate safeguard." *See* U.S. Dep't of Health and Human Services: Health Information Privacy, *Is the Use of Encryption Mandatory in the Security Rule?*, http://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html.

[163] *Sending HIPAA Compliant Emails 101: The Safest Ways to Send PHI*, SECURITYMETRICS, at 101-1, http://www.securitymetrics.com/static/resources/orange/HIPAA_Compliant_Emails_White_Paper.pdf.

[164] *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act, 78 Fed. Reg. 5,566, 5,634 (Jan. 25, 2013) (to be codified at 45 C.F.R. §§ 160, 164) ("We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.").

[165] *Id.*

[166] *See id.*

New entities must consider such tradeoffs. Beyond the challenges created for providers, HIPAA also requires that "Business Associates" of covered entities comply with HIPAA.[167] As HHS explains, "The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity."[168] The business associate must consent to compliance through a Business Associate Agreement (BAA) with the covered entity.[169] The digitization of health information has greatly expanded the number and types of organizations that must sign BAAs. Early examples of BAAs from HHS include third party administrators and independent medical transcriptionists.[170] Now, however, Google will sign a BAA (but only with its paying customers).[171] Verizon has begun offering HIPAA-compliant Virtual Contact Centers so that its clients can communicate PHI over Verizon networks.[172] An entire marketplace has opened up for such HIPAA-compliant communication platforms.[173] The health care industry, due to its size and breadth and now its digitization, touches a more diverse array of companies.

A final question to consider is who should ultimately be responsible when a security breach occurs. Enforcement of penalties for security breaches thus far demonstrate that we are far from a system of strict liability.[174] Under the HITECH Act, covered entities must notify HHS and affected individuals of a breach affecting more than 500 people.[175] Yet a ProPublica analysis found that, through 2014, the HHS Office for Civil Rights fined only twenty-two organizations despite over 1,140 large breaches, a

---

[167] *See* Office for Civil Rights, *Business Associates*, U.S. Dep't of Health & Human Services 1 (Apr. 3, 2003) [hereinafter *Business Associates*], http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html. Per HHS, a Business Associate is "a person or entity that performs certain functions or activities that involve the use of disclosure of protected health information on behalf of, or provides services to, a covered entity." *Id.*

[168] *Id.*

[169] 45 C.F.R. § 164.502(e)(2) ("The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate.").

[170] *Business Associates*, *supra* note 167, at 2.

[171] *HIPAA Compliance & Data Protection with Google Apps: Google Apps for Work HIPPA Implementation Guide*, Google for Work (Feb. 2015), http://static.googleusercontent.com/media/gsuite.google.com/en//files/hipaa-implementation-guide.pdf.

[172] *Verizon Unveils New HIPAA-Ready Solutions*, Verizon (Oct. 23, 2014), http://www.verizon.com/about/news/hipaa-healthcare-contact-center-solutions.

[173] *See* eVisit, http://evisit.com/resources/telemedicine-platform/ (last visited Mar. 15, 2019); *see also* Hale, http://www.hale.co/ (last visited Mar. 15, 2019).

[174] *See* Charles Ornstein, *Fines Remain Rare Even as Health Data Breaches Multiply*, NPR: Shots (Feb. 27, 2015), http://www.npr.org/sections/health-shots/2015/02/27/389328345/fines-remain-rare-even-as-health-data-breaches-multiply.

[175] *See* Breach Notification for Unsecured Protected Health Information: Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009) (to be codified at 45 C.F.R. §§ 160, 164). Before this federal legislation, roughly thirty-three states had their own legislation requiring some sort of disclosure in case of a breach. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 915 (2007).

rate of less than 2%.[176] Admittedly, there are other means of enforcing punishments for data breaches, such as class actions.[177] Paul Schwartz and Edward Janger discuss the "reputational sanction" involved with breach disclosure requirements.[178] Still, two reasonable inferences can be made from the overall low level of enforcement.[179] First, a data breach itself does not guarantee that the breached company violated HIPAA or any other law. Second, a company may follow all of the relevant HHS guidelines and still be vulnerable to an attack from a sophisticated breach. From the perspective of legislators and policy-makers, a reasonable number of breaches may be an acceptable consequence of health care digitization.

C. Some New Privacy Rules May Be Required For Telemedicine

The fundamental change created by telemedicine is that the physician-patient consultation moves online. All other elements, such as prescriptions and sharing of PHI through medical charts or other means, already exist electronically.[180] Moving the consultation from the private confines of an office to the web does have unique and serious consequences.[181] One overarching result is that the change places another weight on the scales of utility in its tension with security.[182] As such risky functionality becomes more accessible and enticing, consumers are going to expect security in their interactions.

One scholar has expressed a hope that telemedicine patients are not having appointments over public Wi-Fi.[183] While perhaps an exaggeration, this is the type of easy access that telemedicine seems to promise. While coffee shop Wi-Fi is not ideal, it seems doubtful that any consumer would worry that their home Wi-Fi network is insufficiently protected for a telemedicine appointment. Mobile health applications suffer from this risk too, and the Food and Drug Administration has acknowledged that device security is "a shared responsibility between stakeholders, including . . . patients, providers, and

---

[176] *See* Ornstein, *supra* note 174.

[177] After the Anthem Life Insurance Company data breach of over eighty million people in 2015, over one hundred class actions were filed that were litigated until 2018. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2018 WL 3960068 (N.D. Cal. Aug. 17, 2018); *see also* Anne Bucher, *Anthem Must Face Data Breach Class Action Lawsuit, Judge Rules*, Top Class Actions (Feb. 19, 2016), http://topclassactions.com/lawsuit-settlements/lawsuit-news/328548-anthem-must-face-data-breach-class-action-lawsuit-judge-rules/.

[178] *See* Schwartz & Janger, *supra* note 175, at 917.

[179] The ProPublica report focuses more critically on the lack of sufficient funding for the Office for Civil Rights at HHS (fewer than 200 employees and a budget under $39 million as of the reporting). *See* Ornstein, *supra* note 174.

[180] Brian Eastwood, *10 Ways Telemedicine Is Changing Healthcare IT*, CIO (Nov. 7, 2012), http://www.cio.com/article/2390576/10-ways-telemedicine-is-changing-healthcare-it.html.

[181] *Id.*

[182] *Id.*

[183] *Healthy Privacy and Security Practices for Telemedicine*, ID Experts: Blog (Mar. 23, 2016), http://www2.idexpertscorp.com/blog/single/healthy-privacy-and-security-practices-for-telemedicine.

manufacturers of medical devices."[184] Patients bear some of the responsibility for device security, evidently, whether they know it or not.[185]

The first and clearest challenge posed by telemedicine is the potential hacking of the cameras themselves. A quick glance around a classroom of laptops usually reveals many people with tape covering their built-in cameras, and with good reason.[186] Video teleconferencing, as HIPAA describes it, however, is not covered under the "Security" portion of the HIPAA rule.[187] HHS guidance has provided that video teleconferencing is not considered electronic media under HIPAA.[188] The logic behind this exception is that HIPAA defines electronic media as requiring storage of data or transmission of information already stored as data.[189] If a telemedicine application records and stores the consultation, then it will be covered under the Security rule.[190]

The lack of coverage for video teleconferencing under the Security rule is at first surprising, but there are still various strong restrictions that demand concern for security. For one, states like California have passed their own legislation expanding the category of covered entities.[191] Second, there are market incentives for providers to guarantee to their customers (i.e., patients) that their telehealth consultations are secure.[192] Third, many applications offer functionality involving storage of ePHI that is covered under

---

[184] Ctr. for Biologics Evaluation and Res., U.S. Dep't of Health & Hum. Servs., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, Food & Drug Admin. 3 (Oct. 2, 2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

[185] *Id.*

[186] *See* Danny Yadron, *Why Is Everyone Covering up Their Laptop Cameras?*, Guardian (June 6, 2016), http://www.theguardian.com/world/2016/jun/06/surveillance-camera-laptop-smartphone-cover-tape.

[187] HIPAA is generally understood to be broken into two categories: Privacy Rule and Security Rule. The Privacy rule covers an individual's control over their own PHI. The Security rule covers technical and physical information safeguards (and most of what this Part has thus far discussed). For a summary of the distinction, see *HIPAA Privacy & HIPAA Security*, W.V. State Privacy Off., http://privacy.wv.gov/tips/Pages/HIPAAPrivacyHIPAASecurity.aspx (last visited Mar. 17, 2019).

[188] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,334, 8,342 (Feb. 20, 2003) (to be codified at 45 C.F.R. §§ 160, 162, 164).

[189] 45 C.F.R. § 160.103.

[190] *See* Adrien Vinches, *HIPAA Considerations When Adding Video Calling To a Health App*, SightCall (Nov. 13, 2014), http://www.sightcall.com/hipaa-considerations-adding-telehealth-video-calling-health-app ("In other words, as long as your app does not record the consultation between the doctor and its patients, the video chat capability does not add additional requirements to meet in regards to the Security Rule.").

[191] *See* Cal. Civ. Code § 56.06(b) (West 2019) ("Any business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . . shall be deemed to be a provider of health care subject to the requirements of this part.").

[192] *See* Judy Robinson, *Why You Must Consider Cyber-Security for Telehealth*, Clinician Today (Jan. 22, 2019), http://cliniciantoday.com/why-you-must-consider-cyber-security-for-telehealth.

the Security Rule.[193] The fact that the live transmission of PHI (e.g., my doctor and I discuss a private health matter during a telemedicine consultation) is not covered should not be viewed as an embrace of utility over security.[194] If telemedicine takes off as many analysts predict, HIPAA may be expanded to cover live videoconferencing.

Regardless of these other protections, audio-visual transmission of PHI, via a consultation or otherwise, should be covered by HIPAA even if the data is not stored.[195] Perhaps those crafting the updated HIPAA rules did not anticipate such a large volume of health care interactions would occur online, and felt this was an unnecessary burden. For example, the standard phone call between a doctor and patient is not covered under HIPAA.[196] It would create undesirable transaction costs if it were, and telemedicine may seem like a close analogy to the phone call. As telemedicine becomes an explicit point of treatment, however, this logic should change. This is not a legal disruption. This change would indicate a shift toward greater recognition of the need for security in non-stored information.[197] Patients could still potentially consent to non-secure communication forms and there are already HIPAA compliant platforms for telemedicine that would meet the providers' demand.

Another security challenge that telemedicine creates is authentication. When a doctor enters into a virtual office and begins speaking with a new patient via videoconference, how can that doctor confirm the patient's identity?[198] Much of the literature in this space recommends the use of two-factor authentication systems, but there is a concern for maintaining the quick and easy access seemingly promised by telemedicine.[199] The American Telemedicine Association explicitly states in its guidance documents that "[i] f multi-factor authentication is available, it should be used."[200] HIPAA requires that covered entities "[i]mplement procedures to verify that a person or entity seeking access to [ePHI] is the one claimed."[201] These requirements reflect the overall sentiment of

---

[193] Office for Civil Rights, *Answered Questions, Health App Developers: Questions About HIPAA?*, U.S. Dep't of Health & Hum. Servs., http://hipaaqsportal.hhs.gov/a/pages/answered-questions (last visited Mar. 14, 2019).

[194] U.S. Dep't of Health & Hum. Servs., *Summary of the HIPAA Security Rule*, U.S. Dep't of Health & Hum. Servs., http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Mar. 14, 2019).

[195] Office for Civil Rights, U.S. Dep't of Health & Hum. Servs., *Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Hum. Servs. 3, http://www.hhs.gov/sites/default/files/privacysummary.pdf (last updated May 2003).

[196] *Id.*

[197] Sharyl J. Nass et al., *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, Inst. Med. 94, 97 (2009).

[198] This is extremely important not only due to PHI but also because it can affect licensing. If the patient is in fact speaking from another state while traveling, the doctor may technically be practicing medicine outside the scope of his or her license.

[199] *See, e.g.*, Dayana P. B. Spagnuelo et al., *Multi-Factor Authentication in Telemedicine Systems*, The Fifth Int'l Conf. on eHealth, Telemedicine, & Soc. Med. 114 (2013).

[200] American Telemedicine Association Standards and Guidelines Committee, *Core Operational Guidelines for Telehealth Services Involving Provider-Patient Relations*, Am. Telemedicine Ass'n 10 (2014).

[201] 45 C.F.R. § 164.312(d).

HIPAA and PHI regulation: manage your risk and take reasonable precautions, but otherwise utilize the technology.

The alternative to such a system would be to impose strict liability for any breach of patient privacy, regardless of the level of care that went into protecting the PHI. Breach notification requirements are arguably a type of *strict reputational liability*.[202] In 2015, the Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held a hearing on data security concurrently with the breach of eighty million individual records at Anthem Life Insurance Co.[203] During the hearing, various industry representatives attempted to make one thing clear to the Senators: breaches are very unfortunate events, but "no system—even the most protected one money can buy—is ever 100 percent secure."[204] The overall tone of each industry representative (and most Senators) was that this is an expected price to pay for technological innovation, and we must require breach notification and that companies be diligent in their protection of data.[205] The responses thus far to security concerns over telemedicine appear to reflect this same balancing effort.

VI. CONCLUSION

Telemedicine is not legally disruptive. Yet simply saying that telemedicine is not legally disruptive fails to capture the true and significant effects of telemedicine on existing health law. First, a technology is not legally disruptive in a broad sense but only in particular areas of application.[206] In some cases, a technology may create drastic change that is completely disruptive of the entire legal regime, but this will be rare.[207] A technology may also create such minimal change as to certainly not be legally disruptive at all (e.g., the electronic car window). Generally, technologies will more frequently disrupt at one level down (and further).

Second, some changes are still clearly needed in order to effectively incorporate telemedicine into the health care system. The risk of over-prescribing of dangerous substances via telemedicine is clearly a challenge that will require additional regulation and consideration by the medical community.[208] The IMLC has only been adopted in twenty-eight states. If that number does not increase, many states will be effectively shut out from the benefits of telemedicine.[209] HIPAA will have to be updated to cover

---

[202] *See Getting It Right on Data Security and Breach Notification Legislation: Hearing Before the S. Subcomm. on Consumer Prot., Prod. Safety, Ins., and Data Sec.*, 114th Cong. 9 (2015) (statement of Cheri F. McGuire, Vice President of Global Government Affairs and Cybersecurity Policy, Symantec Corp.).

[203] *See id.* at 57 (statement of Sen. Amy Klobuchar, Member, S. Comm. on Commerce, Sci., & Transp.).

[204] *See id.* at 6 (statement of Cheri F. McGuire, Vice President of Global Government Affairs and Cybersecurity Policy, Symantec Corp.).

[205] *See id.*

[206] *See supra* note Part II.

[207] *See supra* note Section II.C.

[208] *See id.*

[209] Telemedicine can still occur intrastate in those states that have not adopted the IMLC or created a special telemedicine license.

non-stored information in order to minimize telemedicine security risks. The takeaway from this Article is absolutely not that existing law is completely sufficient and telemedicine creates no legal challenge. Rather, the argument is that most of the benefits of telemedicine can be obtained while maintaining the underlying doctrines.

Changes to the underlying law will affect other elements of health care. Creation of new technology-specific rules or clarification of uncertainty does nothing to the underlying doctrine or other types of technologies or activities it regulates. When the justification for a law has been disrupted, however, the entire legal framework must be revisited, including how the laws apply to activities that previously operated under settled doctrines. Disciplinary systems, specialist boards, and various other roles currently played by state medical boards would all require updating if telemedicine truly disrupted state-based licensing.

Finally, we can only assess the legal disruptiveness of a technology at a given point in time. Technology could evolve such that it would be ludicrous to maintain underlying legal doctrines as applied to telemedicine. If enough of medicine moved to the virtual world, this may or may not disrupt the legal role of the hospital in areas like corporate negligence.[210] Attempting to predict the future use of telemedicine and its legal implications would be a fool's errand. Instead, scholars and policy-makers should remain aware of the state of the technology, acknowledge the underpinnings of existing doctrine, and only disrupt as necessary.

[210] For one assessment of what a hospital of the future may look like, see *How Hospitals Could Be Rebuilt, Better Than Before*, Economist (Apr. 8, 2017), http://www.economist.com/news/international/21720278-technology-could-revolutionise-way-they-work-how-hospitals-could-be-rebuilt-better.