"DO NO HARM": A COMPARATIVE ANALYSIS OF LEGAL BARRIERS TO CORPORATE CLINICAL TELERMEDICINE PROVIDERS IN THE UNITED STATES, AUSTRALIA, AND CANADA

Ian R. Landgreen*

I swear by Apollo the physician and Aesculapius, and Health, and All-heal, and all the gods and goddesses, that, according to my ability and judgment, I will keep this Oath and this stipulation... I will follow that system of regimen which, according to my ability and judgment, I consider for the benefit of my patients, and abstain from whatever is deleterious and mischievous.

Hippocrates

I. INTRODUCTION: VIRTUAL CLINICS

Imagine the following scenario: "The doctor will see you now," is emitted from a computer's speakers as a patient clicks on the virtual clinic icon on her desktop computer while she is on her coffee break at work. During this fifteen minute break, the patient consults her doctor who makes a diagnosis and prescribes treatment, all over a digital connection.

Virtual medical clinics are fast becoming a virtual reality. Using teleconferencing technologies, telemedicine providers connect patients and doctors in a digital environment. Thus, a patient can seek medical advice and treatment via personal computer. Commercial adaptation of this new mode of medical treatment requires a new legal framework for analysis.

This Note comparatively analyzes current legal models in the United States, Canada, and Australia and advocates the development of a legal system tailored to modern and future telemedicine practices. Such a system will create an environment of certainty, which in turn will contribute to capital investment in beneficial technological and organizational models. Specifi-

* J.D. 2002, University of Georgia.

1 See Hippocrates, Hippocratic Oath. Contrary to popular conception, the phrase, "First, do no harm," is not now, nor has it ever been, a part of the Hippocratic Oath to which doctors pledge. See generally "First, Do No Harm" Is Not in the Hippocratic Oath, at http://www.geocities.com/everwild/noharm.html (last visited Sept. 4, 2001); see also Dennis Gersten, M.D., AMA Hippocratic Oath, at http://www.imagerynet.com/hippo.ama.html (last visited Sept. 4, 2001).
ically, this Note reviews the legal barriers to a corporate provider of telemedicine in the three above-mentioned nations.

II. ANALYTICAL BACKGROUND

A. Health Care Innovation Markets

Technological innovations, both mechanical and organizational, have affected all aspects of our lives. With the advent of newer and quicker methods of communication, we are able to communicate across borders and vast expanses at the speed of light. Larger and more specialized organizations capture and distribute economies of scale that were once considered impossible. The practice of medicine is not immune to such changes. Telecommunications systems can transmit and receive information from distant medical experts and databases, increasing overall access to valuable health information. Health care organizations consisting of doctors, administrators, nurses, and citizens have the potential to increase the overall health and wealth of organization members. Indeed, the Internet is a vast source of health-related information and services.²

Health innovations also present disadvantages. An increase in the availability of health information necessarily leads to the distribution of suspect and unreliable information to a large number of people. Likewise, health care organizations are often derided for being bureaucratic and inflexible. Thus, innovations may lead to a short-term decrease in output quality.

Often, the mechanical technology of a potential innovation exists long before the organizational technology can respond with a complementary approach necessary to eliminate economic, legal, and social barriers to the successful introduction of the technology. Conversely, society is often organized and waiting for mechanical technology, but such mechanical breakthrough lags behind our organizational readiness. The impetus for innovation may be private industry’s quest for profit or governmental intervention to improve social welfare. Industry and government may walk

² An estimated sixty million adults used the Web to find health related information in 1998. See Marlene M. Maheu, Delivering Behavioral Telehealth via the Internet: eHealth, at http://telehealth.net/articles/deliver.html (last visited Sept. 4, 2001); see also Service-Growth Consultants, Canada Healthkeepers to the World: Canadian Opportunities in Global Telehealth Markets, Study prepared for Industry Canada, Health Industries Branch, March 1998 (noting that the demand for online health information, estimated at over $800 billion in 2000, has led to estimates that at least ten percent of the total World Wide Web content is related to health care).
hand-in-hand, take parallel paths to the same endpoint, or travel in opposite directions. This dynamic between industry's response to market forces and government's normative approach to social engineering is what shapes the processes and uses of technology.

According to neoclassical economic theory, a perfectly competitive market needs little governmental intervention because market forces will determine the social utility of a product or service. However, innovation markets are rarely perfectly competitive because barriers to entry (economic and legal) inhibit the entrance of technological breakthroughs. A small businessman wishing to introduce a socially useful innovation may lack access to capital markets or may be discouraged by anti-competitive practices of marketers of current (and inferior) technologies. Likewise, because consumers and producers do not possess perfect information, market availability may not reflect consumer preference.

Government intervenes legislatively through the passage of laws that seek to correct market imperfections, administratively through the application of laws, and judicially as the arbiter of the laws as applied to unique and often unanticipated factual circumstances. The goal of governmental regulation of innovation markets is the improvement of aggregate social welfare and individual utility maximization.

Such regulation may take the form of a carrot-like incentive. For example, the government may provide tax breaks for those who devote capital to the research and design of new products or award a patent to the first innovator of a unique product to provide an incentive to devote capital to innovation. These types of regulations function to internalize positive externalities by rewarding the creators of potential long-term public gains with short-term private gains or by eliminating free-rider competitors who seek to capitalize on another's investment in innovation. Regulation of innovation markets may also take the form of stick-like disincentives. For example, a patent infringer may be punished or new inventions may be required to be compatible with current technologies. These negative regulations seek to achieve a smooth transition to new technological innovations by creating market certainty and setting standards of compatibility.

B. Context of Analysis: Corporate Telemedicine

This Note is a comparative analysis of the United States, Australia, and Canada with respect to the legal barriers to the following situation: (1)
practice of clinical telemedicine; (2) by a corporation; (3) that provides a
digital medium; (4) for the exchange of information; (5) between a patient; and
(6) a doctor with whom the patient has a prior relationship.3

Doctor Goodwell, Inc. provides an interesting context for analysis.4 The
Microsoft Corporation is currently partnered with Doctor Goodwell in the
development of a prototype and pilot implementation of an Internet/Intranet-
based solution for the delivery of healthcare information and services to
employees of client corporations.5 Doctor Goodwell will contract with these
employers to provide the technology, training, medical provider networks and
long-term support needed to manage better their healthcare costs, and will
work to enhance the health, well-being, and productivity of the corporate
clients’ workforce.6 From the corporate workplace, employees will access the
system by dialing into the “virtual medical clinic” from a central and
ostensibly secure site reserved for Doctor Goodwell applications, which
include the delivery of targeted medical knowledge, e-mail consultations and
a video-based “virtual office visit” to connect employees and their doctors.7
Doctor Goodwell acknowledges that it cannot replace all in-office doctor
visits, but predicts it can effectively move approximately twenty percent or
more of these visits to videoconferencing or e-mails.8 Such a service would
secure convenient provision of healthcare to employees and at the same time
increase their productivity on behalf of the corporate client/employer.9
Employers will become Doctor Goodwell clients, and the corporation will pay
for the visits as part of an employee benefits program.10 Doctor Goodwell
would open the system to any physicians interested in participating, and the
company hopes that employees would be able to integrate and retain their pre-
existing relationship with their personal physicians.11

Naturally, employees will only be able to consult remotely with those
physicians who choose to participate in Doctor Goodwell’s healthcare system.

3 See Robert Milstein, An International, Comparative Analysis of Policy, Regulatory and
excesum.htm (visited Sept. 4, 2001) (noting that telemedicine is not “[a] single technology or
a discrete set of related technologies; it is, rather, a large and very heterogeneous collection of
clinical practices, technologies, and organizational arrangements”).
5 See id.
6 See id.
7 See id.
8 See id.
10 See id.
11 See id.
A physician's choice to participate depends on a number of factors including the remuneration scale, the physician's degree of autonomy, the utility and efficacy of the system, and other market factors such as patient demand. Likewise, the presence of significant network externalities creates a positive feedback process in which the value of the system increases with the number of users. A successful network would tend to have more users, which in turn would create incentives for internal or external network plug-ins. Thus, the scalability of system applications would have great influence on the growth of a digitally-based healthcare system. Likewise, the degree of government regulation and cooperation will significantly impact the availability of digital health networks.

C. The Commonality of the United States, Australia, and Canada

Although the United States, Australia, and Canada have different social policies and practices regarding the relationships between industry and government, a comparative analysis of the countries' telemedicine policies and regulatory environments is quite revealing, especially considering that Australia in particular models much of its telemedicine legal policy after that of the United States, which provides a forum for experimentation. All three nations face similar situations: a legal system evolved from the British common-law system, a relatively well-connected population, geographically diffuse populations, distribution of health resources that does not match population needs, a rapidly aging population, and a dramatic rise in the cost of healthcare, all of which lead to uneven access to healthcare and an increase

12 See D.G. Breaden & E. Smith, A Report on the First International Conference on Medical Licensure Registration and Discipline, v. 81 no. 4 FEDERATION BULLETIN 243, 247 (1994) (arguing that the "close of the millennium has brought an era in which no nation can ignore the lessons to be learned through sharing of experience, information, research and insights with others around the world"); see also Medical Practitioners Board of Victoria (MPBV) Annual Report for 1997, 4 (1997) (recognizing the "benefit of being aware of new and effective approaches to the regulations of the medical profession developed in other jurisdictions").

13 See Milstein, supra note 3.

14 The United States and Canada are currently experiencing the transition to broadband. See Report on Telemedicine, 4.3.7., at http://biomant.die.unina.it/teleplans_doc/WP4_index.htm (last visited Sept. 4, 2001). Along with eight Asian countries, Australia is linked to a 12,000 kilometer submarine fiber optic cable known as the Asia Pacific Cable Network (APCN). See Life Sciences Branch—Health Industries Canadian International Business Strategy (CIBS) (1999-2000), at http://strategis.ic.gc.ca/SSG/ht0195e.html (last visited Sept. 4, 2001).

15 While Canadian expenditures in the health services sector rose forty-one percent from $56.7 billion in 1997 to $80.0 billion in 1999, the U.S. health care industry is worth over $1 trillion. See CIBS, supra note 14.
in the rate of chronic as opposed to acute health problems. In each country, a profit-oriented business model is replacing the traditional health-oriented model. Thus, an increased emphasis is placed upon efficiency in the delivery of health services.

While similarities abound, and the U.S. system exerts "a powerful influence on Australia" and Canada, there are, however, important regional differences in the practice of medicine. The health systems in Australia and Canada have traditionally been steeped in socialism, while the U.S. system has long been market-driven. This difference has had a number of implications including varying levels of government participation in the development of telemedicine, a greater market for research and development of new medical technologies in the United States, and distinct treatment recommendations.

III. HISTORICAL BACKGROUND

A. History of Telemedicine

Doctors have long taken advantage of communications technology. For instance, the medical profession began using the telephone as a consultation

---

16 See Milstein, supra note 3.
17 See id.
18 See id. (noting that each country is trying to "do more with less").
20 See Report on Telemedicine, supra note 14. In Australia particularly, a large majority of telemedicine projects are sponsored by governmental entities, both national and regional. Id. at 5.1.3.1.1.
21 See CANADIAN SOCIETY OF TELEHEALTH, CANADIAN STRENGTHS AND INTERNATIONAL OPPORTUNITIES IN TELEHEALTH: OBSERVATIONS FROM THE G7-G8 SP4 FORUM: MEDICAL/LEGAL ASPECTS OF NATIONAL AND INTERNATIONAL TELEHEALTH APPLICATIONS, (Jan. 2, 2000), available at http://strategis.ic.gc.ca/SSG/it05376e.html (last visited Sept. 4, 2001) (noting that "Canada's single-payer health care system puts a damper on the development of the entrepreneurial side of telehealth... Particular telemedicine applications may be cost effective, but it will take some time to determine which applications are cost effective. Governments will not be willing to provide telemedicine services that are not cost effective, and because of the single-payer system Canadians may not pay privately for insured services provided by telemedicine"
22 See E. Haavi Morreim, Playing Doctor: Corporate Medical Practice and Medical Malpractice, 32 U. MICH. J.L. REF. 939, 992 (1999) (discussing the reasons that U.S. physicians recommend coronary angiography and revascularization (cardiac bypass surgery) more often than Canadian physicians. Some of the proffered explanations include more widespread availability of facilities and trained personnel in the United States.).
tool shortly after the device’s inception. In Canada in 1956, Dr. Feindel, a Saskatoon neurosurgeon used a closed circuit television system to transmit live electrocorticography tracings. However, most sophisticated telemedicine projects were initially undertaken by governmental organizations. For instance, the National Aeronautics and Space Administration (NASA) developed a system for the remote monitoring of U.S. astronauts in the 1970s. More recently, telemedicine has been used as a teaching tool to provide distance learning, as a conduit of medical services to rural populations, for consultations with distant experts, in the context of home health care, as an automated psychologist, and for the provision of health care to prison populations.

B. Current State of Telemedicine

With the advent of the Internet, the potentials of telemedicine have increased exponentially. As teleconferencing technologies have become more sophisticated and less expensive, new and improved telemedicine applications have become technologically and economically feasible. For instance, it is now possible and affordable to install teleconferencing technologies on an

24 See Report on Telemedicine, supra note 14, at 5.2.2.
25 See id.
26 See Charles R. Doarn et al., Applications of Telemedicine in the United States Space Program, 4 TELEMEDICINE J. 19, 19-20 (1998); see also Patricia C. Kuszler, Telemedicine and Integrated Health Care Delivery: Compounding Malpractice Liability, 25 AM. J.L. & MED. 297, 300-01, 1999 (discussing how NASA’s program was modified by its collaboration with the Indian Health Service and the Papago Indian Tribe to connect underserved rural populations to distant health services, and how later, NASA participation in an international telemedicine project, created a “spacebridge” between the United States and Russia).
27 See Robert Friedman, M.D., Totally Automated Telehealth Systems to Deliver Health Behavior Change Interventions, available at http://telehealth.net/articles/automated.html (last visited Sept. 4, 2001) (describing an automated telephone-linked-computer (TLC) that interacts with callers to assist with behavioral changes such as the cessation of smoking or diet maintenance through behavioral reinforcement comprised of assessment of behavior, behavior intervention, and behavior goal setting).
28 The term “telemedicine” is a sub-species of the term “eHealth,” which refers to all forms of electronic healthcare delivered over the Internet, ranging from informational, educational and commercial “products” to direct services offered by professionals, non-professionals, businesses or consumers themselves. eHealth includes a wide variety of the clinical activities that have traditionally characterized telehealth, but delivered through the Internet. See Maheu, supra note 2.
individual basis rather than limiting access to large and well-funded entities. This progress has the potential to individualize health care by affording more choice and flexibility to patients. However, efforts to marry medicine and information technology have encountered some resistance.

C. Barriers to the Availability of Digital Health Systems

A prospective provider of a digital health system faces a number of potential barriers. First, if the digital system fails, the provider may face damages based on a products liability claim. Second, defects in organization could result in liability similar to recent attempts to hold health maintenance organizations (HMOs) and managed care organizations (MCOs) liable for harm to system members. Third, licensure at the state level could prevent the transfer of digital health care across state lines. Fourth, reimbursement issues, intertwined with anti-kickback statutes, put restrictions on the payment of funds to induce referrals under government healthcare programs. Fifth, similar to anti-kickback provisions, self-referral prohibitions at both the federal and state levels present potential barriers to the provision of clinical telemedicine. Sixth, regulatory agencies could restrict the marketing and distribution of digitally-based healthcare systems. Seventh, privacy and confidentiality concerns regarding the storage and dissemination of patient records is gaining increasing attention by lawmakers and has spawned an entire industry devoted to digital rights management. Other issues beyond the scope of this Note include equal access concerns that may require some regulation to ensure that

---


31 A survey of 257 family practitioners, general practitioners and internists revealed that while 41% were very interested in using the Internet to practice medicine remotely, such as through an audiovisual link, physician interest in telemedicine in the immediate future is limited. (Only 33% of the physicians expressed significant interest in using the Internet for communicating with patients, consulting with colleagues, participating in clinical trials or filing patient insurance claims. Only 27% believe the Internet will save the health system money in the next five years; less than 50% feel it will improve physician-patient communication. And, while many companies are currently developing technology platforms for writing prescriptions online, the survey revealed that few physicians (19%) are actually very interested in using this application in the future) See Web Survey MD: Update on Physicians and the Internet, at http://websurveymd.mt01.com/UpdatePhysiciansInternet.shtml (last visited Sept. 4, 2001).
patients on the wrong side of the "digital divide" have access to digital health systems and the distribution of prescriptions over the Internet, an increasingly hot topic.

Each of the barriers to telemedicine in the United States is further complicated by the fact that telemedicine has been the focus of increased, noncomprehensive, and nonuniform federal legislative activity during the 105th and 106th Congresses. Further illustrating the legislative patchwork regulation of telemedicine in the United States is the fact that during 1999 Arizona, Arkansas, Colorado, Florida, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Oklahoma, Oregon, Tennessee, Texas, Utah, and Virginia, among other states, considered telemedicine legislation.

IV. LEGAL ANALYSIS

A. Liability as Analogous to Medical Device Failures

The danger with introducing new technology is twofold: (1) in the event of a technology failure, the provider may be liable for any harm resulting therefrom; and (2) the availability of technology can increase user expectations, thereby raising the level of the minimum standard of care courts will require. Thus, a provider of telemedicine will want to characterize its service

33 See Julie A. Braun et al., Recent Developments in Medicine and Law, 35 TORT & INS. L.J. 487, 543 (2000) (noting activity in the 105th Congress, including more than twenty proposals or acts).
35 See id. at 543-45 (noting extensive legislative activity at the state level).
36 See Kuszler, supra note 26, at 316-17 (describing such a phenomenon as a "double-edged sword" because it could result in "liability for failing to install a technology that is now 'standard' and liability for any malfunction or misuse of the technology that results in harm to the patient").; see also Monua Janah, Health Care by Cisco, INFO. WK., Feb. 23, 1998, at 116, available at 1998 WL 2358723 (voicing concern that the risk of telemedicine is compounded by a shortage of network professionals and unreliability of the network.); see also Jay H. Sanders & Rashid L. Bashshur, Challenges to the Implementation of Telemedicine, 1
as the provision of a space to be used by a doctor and a patient, similar to a real estate lessor who provides the physical space for a doctor’s clinic.

However, a virtual clinic, as defined in this Note, goes beyond merely providing a space; it involves interactive applications that may be subject to technical errors that could result in faulty transmissions. If an error results in patient harm, the provider may be liable, as a real estate lessor would be if failure to maintain the physical property results in patient harm when a ceiling collapses. Just as formal characterization of the service does not relieve the telemedicine provider of liability, the transfer of title of the equipment from the provider to the physician will not immunize the provider, especially if in charge of maintenance and operation of the information system. Thus, liability for telemedicine failure is not unlike liability for the failure of other medical devices.

The United States, being more litigious than Canada and Australia, is much more likely to host lawsuits regarding telemedicine. Nonetheless, commentators in Canada have urged policy makers to address issues regarding product standards, which are especially important because many telemedicine technologies were originally designed for other uses such as videoconferencing. In Australia, it is argued that a telemedicine provider’s failure to warn of the material risks of a telemedical consultation would be analogous to a doctor’s failure to warn a patient about the risks of a traditional medical treatment.

---

Milstein, supra note 3.

See id. (suggesting that Australian policy makers might adopt a wait-and-see attitude to model its treatment of telemedicine on policies adopted in U.S. courts, the “litigation capital of the world”); see also Industry Canada—Information & Communications Technologies, The Telehealth Industry in Canada: Canadian Capacity to Respond to Traditional Telehealth Markets, (visited Sept. 4, 2001) http://strategis.ic.gc.ca/SSG/it05495e.html (stating that “the authors know of no incident, which has been brought to court in Canada, which might hinder the deployment or development of telehealth”).

See Domenic A. Crolla, Health Care Without Walls: Responding to Telehealth’s Emerging Legal Issues, 19 HEALTH L. IN CAN. 1, 1-32 (Aug. 1998) (urging the Canadian government to classify telehealth instruments as medical devices, which would create an environment of certainty due to the establishment of clear standards for use).

See Rogers v. Whitaker (1992) 175 C.L.R. 479, 490 (“[A] risk is material if, in the circumstances of the particular case, a reasonable person in the patient’s position, if warned of the risk, would be likely to attach significance to it or if the medical practitioner [or the telemedicine provider?] is or should reasonably be aware that the particular patient, if warned of the risk, would be likely to attach significance to it”).
In the United States, liability may take the form of simple negligence or negligence based on *res ipsa loquitur.* Under both types of liability, all involved parties may share liability. Likewise, a patient may even try suing an Internet service provider (ISP) on which the telemedicine provider relies. An ISP, however, would probably escape liability on public policy grounds because to hold it liable for intermittent failures of information transmission could result in such extraordinarily high levels of liability that no one would provide Internet services at a reasonable cost. A telemedicine provider could argue that this same rationale justifies its immunity from liability for network errors. A court would probably (and should) take this into account when judging the reasonableness of the provider's actions. Thus, the duty of care may reflect the value, uniqueness, and availability of the service provided. This reasoning is also applicable if the provider is sued under a theory of institutional liability, as discussed below.

**B. Institutional Liability**

Telemedicine is unique among medical devices because it requires a common network shared by multiple users. The network infrastructure cannot possibly be supplied by individual physicians or their patients because it relies

---


42 *See* Anderson v. Somberg, 386 A.2d 413 (N.J. Super. Ct. App. Div. 1978) (holding that at least one party must be liable among the physician, hospital, manufacturer, and distributor when a metal instrument broke off in the patient. The physician and hospital were sued under negligence theories, while the instrument's distributor and manufacturer were sued on the basis of warranty and strict liability theories respectively.); *see also* Airco, Inc. v. Simmons First Nat'l Bank, 638 S.W.2d 660 (Ark. 1982) (finding liability for the manufacturer of a malfunctioning artificial breathing machine); *see also* Kennedy v. McKesson Co., 448 N.E.2d 1332 (N.Y. 1983) (allowing dentist to recover for claim against manufacturer of anesthetic equipment whose malfunction resulted in death of dentist’s patient).

43 Internet-based communications are so unreliable that there has been consideration of cell-based technologies, which are considered more reliable. *See Janah, supra* note 36.

in large part on the economies of scale that go hand-in-hand with a network that services a large population of users. It is inevitable that telemedicine systems will be part of larger systems, probably part of an integrated delivery system (IDS).\textsuperscript{45} An IDS is similar to a MCO or a HMO in that all three types of entities deliver health care services by affiliating multiple providers and users in a large corporate structure.\textsuperscript{46} The advantages of these corporate structures include the realization of efficiencies, increase of market share, and containment of costs.\textsuperscript{47} These advantages, however, are coupled with a disadvantage: the more control that a corporation has over provision of health care services, the more likely it is to share malpractice liability.\textsuperscript{48} Especially in the United States, the threat of malpractice suits can be a great inhibitor to the provision of telemedicine.\textsuperscript{49}

In the United States, corporate liability first began with hospitals,\textsuperscript{50} and has

\textsuperscript{45} See Kuszler, supra note 26, at 326 n.222 (discussing Rhonda L. Rundle, Tenet and MedPartners Agree to Form Health Network in Southern California, WALL ST. J., Apr. 10, 1997, at B4 (describing the formation of a health care network including thirty-three hospitals and more than 4000 physicians, an arrangement that is "one of the most visible examples so far of how major health-care players are attempting to create big integrated networks that take advantage of economies of scale to gain market share"); see also CIBS, supra note 14 (noting that in the United States seventeen percent of the population is enrolled in managed care plans); but see Report on Telemedicine, supra note 14, at 4.3.8 (noting that “most HMOs are adopting a ‘wait-and-see’ policy, insisting upon proven clinical efficiency and cost-effectiveness before integrating telemedicine as part of their routine health care delivery”).

\textsuperscript{46} See PAUL STARR, THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE 440-49 (1982) (discussing the not-so-recent corporatization of U.S. health care); see also Bashshur, supra note 36, at 7 (noting that “only when viewed as a complete and integrated network will telemedicine’s unique distributive capabilities and integrative functions be maximized”).

\textsuperscript{47} See Kuszler, supra note 26, at 319; see also Morreim, supra note 22.

\textsuperscript{48} In Australia, individual employees may face liability separate from and in addition to the institution. See Milstein, supra note 3 (arguing that “... ‘in-house’ technical personnel, such as health information managers, clinical data specialists, document managers and data security officers, have an increased responsibility and correspondingly an increased ‘exposure’ in a telemedical context”).

\textsuperscript{49} Unlike the many telemedicine barriers in the United States, most industrialized countries are not hindered by excessive threats of malpractice actions. See generally A.C. Dumay, Medicine in Virtual Environments, 3 TECH. & HEALTH CARE 75, 75-89 (Oct. 1995).

\textsuperscript{50} Until the mid-1900s, it was common for hospitals to be given charitable immunity for malpractice that occurred on their property. See Pierce v. Yakima Valley Mem'l Hosp., 260 P.2d 765, 773 (Wash. 1953). This immunity was a vestige of the fact that most hospitals had been founded and maintained on a charitable basis. See id. at 769. With the transition to not-so-charitable corporate entities, this immunity eroded. See id. at 770. Thereafter, hospitals often escaped liability by arguing not that they deserved charitable immunity, but by characterizing their physicians as independent contractors who merely occupied the physical premises of the hospital as a "workshop" and simply "borrowed" the hospital employees such as nurses. See
been recently expanded to include other IDSs. In Australia, duty of care with respect to an individual healthcare practitioner or a corporate healthcare institution is determined, as a matter of law, by applying the concepts of "foreseeability" and "proximity."

An organization may face two theories of liability: vicarious liability and direct liability. Vicarious liability involves a principal-agent relationship wherein the principal is held legally responsible for negligent acts committed by the agent while acting for the principal. The principal’s liability is based on its position as supervisor/employer of its subsidiary agent, not on the formal status as employee. Likewise, the importance of characterizing the physician as an employee of the health organization is less of a critical factor because doctors have increasingly entered into employment contracts with the organization. Nonetheless, in order to avoid liability based on ostensible
agency, a provider of telemedicine should make every effort to inform patients that the physicians are not employees of the organization. However, a duty of care can exist even in the absence of a contract between the provider and the patient.

Ideally, the organization should merely act as an informational conduit between the patient and the patient’s personal physician. That way, the patient’s pre-established relationship with the physician minimizes the risk that the patient can be said to have reasonably believed that the physician was employed by the organization. This will avoid application of the ostensible agency doctrine, but the provider may nonetheless be found liable on the basis of direct liability.

Direct liability can result when a health organization violates a duty owed directly to a patient. Duties may arise under the theories of non-delegable duty, corporate negligence, and defectively designed health care programs. A non-delegable duty includes the provision of services that only the hospital is able to provide. Corporate negligence is intertwined with non-delegable duty and was first applied to hospitals in the classic case Darling v. Charleston Community Memorial Hospital. Since Darling, the doctrine has gained increasing acceptance. Recently the corporate negligence theory has also


58 See Medical Practitioners, in 27-2 [THE LAW OF AUSTRALIA], 13 (LBC Information Services, 1998).

59 See Kuszler, supra note 26, at 320-23 (describing liability for defectively designed health care programs as “arguably” viable).

60 See Jackson v. Power, 743 P.2d 1376 (Alaska 1987) (involving hospital’s delegation of the duty to provide emergency care by an independent contractor physician).

61 Darling v. Charleston Cmty. Mem'l Hosp., 211 N.E.2d 253 (Ill. 1965) (holding hospital could be negligent for failing to ensure that its independent physicians provided competent care on the premises); see also Thompson v. Nason Hosp., 591 A.2d 703, 707 (Pa. 1991) (describing the relationship between corporate negligence and nondelegable duty and noting that the former theory may give rise to the latter. The court divided a hospital’s duties into four categories: (1) duty of reasonable care to maintain safe and adequate facilities and equipment; (2) duty to select competent physicians; (3) duty to supervise the practice of medicine on the premises; and (4) duty to administer institutional safeguards to ensure quality of care.).

been used in suits against HMOs. The doctrine has even been applied in a context reminiscent of telemedicine: an HMO practicing demand management through the use of a physician giving patients advice over the telephone.

In Shannon v. McNulty, a Pennsylvania court held that an HMO could be held liable for the death of a baby born prematurely when, over a period of days and multiple remote consultations, an obstetrician employed by the HMO advised a pregnant plan member via telephone that she was not experiencing pre-term labor. In dicta, Wickline v. State of California implied that the corporate negligence doctrine could be expanded to include liability for the faulty design of a managed care system, and while the expansion has not been universally accepted, it could be particularly relevant in the telemedicine context in which a negligently designed system could have a greater impact on quality of care.

Thus, to provide an environment conducive to certainty, stability and quality care for patients, the scope of corporate liability for acts of doctors using the corporation’s telemedicine infrastructure must be explicitly addressed by statute to determine the proper division of labor between the physicians and the corporation. Traditional statutory delineations of the duty doctrine to allow direct recovery against a hospital for acts committed by independent physicians and surgeons).

See e.g., Shannon v. McNulty, 718 A.2d 828 (Pa. Super. Ct. 1998) (finding “no reason why the duties applicable to hospitals should not be equally applied to an HMO when that HMO is performing the same or similar functions as a hospital. When a benefits provider, be it an insurer or a managed care organization, interjects itself into the rendering of medical decisions affecting a subscriber’s care it must do so in a medically reasonable manner.”); McClellan v. Health Maint. Org. of Pa., 604 A.2d 1053, 1059 (Pa. Super. Ct. 1992) (recognizing that an HMO could face liability for negligent selection of its contracting physicians and holding that an IPA-model HMO may have the duty of certifying its physicians’ credentials); Dunn v. Praiss, 656 A.2d 413 (N.J. 1995); Petrovich v. Share Health Plan of Ill., Inc., 696 N.E.2d 356 (Ill. App. Ct. 1998).


Wickline v. State, 239 Cal. Rptr. 810 (Ct. App. 1986); see also Kuszler supra note 26, at 322 (noting that while Wickline “has not resulted in a significant line of cases . . . in the context of telemedicine ‘defects in design’ could take on a new meaning and be more fruitful in terms of producing case law”).

See Morris v. D.C. Bd. of Med., 701 A.2d 364, 367 (D.C. 1997) (holding that a definition of “treatment” that included any conduct that merely “[a]ffects,” “influences,” or “substantially impacts” on the course of care by others was “so open-ended that it cannot reasonably be squared with the statutory term,” because equating “treatment” with any conduct that “practically [a]ffects” it in ways potentially involving no exercise of medical judgment, is contrary to sensible statutory interpretations); see also Morreim, supra note 22, at 1036-39 (arguing that the proper scope of medical malpractice and other tort liability for MCOs can only be discerned after it is determined what duty of care MCOs owe their subscribers. This question,
of care owed by the physician and the ISD were not drafted to encompass modern and future telemedicine practice methodologies. Malpractice statutes require legislative reexamination to reflect the reality of telemedicine. This will create certainty as to the proper role of communication infrastructure providers, which in turn will further encourage the creation of facilities that are capable of fairly distributing quality care at an affordable price. If malpractice standards are not statutorily adopted, providers may be either over-deterred or under-deterred, depending upon the approach taken by local courts. Courts should not be making public policy decisions regarding telemedicine because the legislature is the more appropriate forum for evaluating and weighing the various and complex advantages and disadvantages of remote medical communications systems.

Reform proposals often focus on whether the healthcare system interferes with the autonomy of the physician in recommending a course of medical treatment. Critics argue that corporations should be allowed to practice medicine as long as control over medical decisions is retained by licensed doctors. Indeed, a number of states have taken this tack. However, the degree of permissible interference with a doctor's judgment is unclear, particularly in the context of a telemedicine system, where the system is a self-
described diagnostic tool designed to externally augment a physician’s internal skills. On one hand, the system may provide for early detection of medical conditions, thereby positively contributing to the practice of preventive medicine. However, the system may also inhibit a physician’s diagnostic capabilities because a thorough physical examination cannot be conducted using current remote technologies. A system administrator would argue that a doctor should know the limits of remote diagnoses and that when a telemedicine consultation proves to be inconclusive, the doctor should recommend an in-person follow-up. Thus, a pure telemedicine system, operating without technological error and without further organizational restrictions that inhere in IDSs, should not significantly interfere with a physician’s independent judgment.

Whether a digital health provider faces vicarious or direct liability, it may nonetheless escape liability because some courts have held that if the health care is provided as part of a self-funded employee benefits program, then liability is federally preempted by the Employee Retirement Income Security Act of 1974 (ERISA). However, ERISA preemption may not immunize the provider from liability if the actions of the health plan were what precipitated the negligent medical care. Thus, if telemedicine is provided negligently to an employee, the underlying claim probably would not be preempted by ERISA because a medical decision would be centrally involved. But, if telemedicine facilities are denied altogether, ERISA probably would preempt the claim because the substantive issue involves a benefits decision. However, denial of benefits cannot be wholly isolated from the practical impact on the patients’ decisions to seek further treatment. Some authorities nonetheless

69 See Ricci v. Gooberman, 840 F. Supp. 316, 317-18 (D.N.J. 1993) (finding ERISA preemption of a vicarious liability claim made by an employee against her HMO’s physician); see also Kuhl v. Lincoln Nat’l Health Plan, 999 F.2d 298, 303 (8th Cir. 1993) (preempting a direct liability claim); see also Corcoran v. United Healthcare, 965 F.2d 1321, 1331 (5th Cir.), cert. denied, 506 U.S. 1033 (1992) (finding ERISA preemption because the MCO made a benefits decision that was merely an interpretation of the insurance contract, rather than a medical decision as to the necessity of the particular procedure involved. The court noted, however, that a claim might not be preempted if the MCO goes beyond administrative claims-handling by denying coverage such that the logic of a benefits determination is inapplicable. While the exact bounds of such a situation are not clear, the court noted that prospective utilization review decisions have a powerful influence on patient treatment decisions because the patient often chooses to forego medical care for which he or she bears the cost.).


71 See Long v. Great West Life & Annuity Ins. Co., 957 P.2d 823, 827 (Wyo. 1998), where the Wyoming Supreme Court noted that in the case of an MCO (and not in the context of telemedicine) “[a]lthough the attending physician is the ultimate decisionmaker regarding a patient’s treatment, it is, as commentators note, naive to assume that a provider’s determination
explicitly hold that doctors performing utilization reviews\(^{72}\) are not practicing medicine and, thus, are not subject to "the regulatory, investigatory, or enforcement authority of the State Medical Board."\(^{73}\) If utilization review decisions are not the practice of medicine on the state level, they should fall under ERISA protection to provide some measure of recovery to the plan member for denial of treatment/benefits.

In *Rudolph v. Pennsylvania Blue Shield*,\(^{74}\) the Pennsylvania Supreme Court allowed a physician to legally challenge the validity of a utilization review that found a lack of medical necessity and thus refused reimbursement.\(^{75}\) The critical question, then, is whether or not a patient, who is denied a telemedicine consultation or a referral to another physician based on a telemedicine consultation, can hold the provider liable for the patient's inability, be it financial or physical, to seek a source of treatment external to the telemedicine program. If the telemedicine system is linked with an HMO-type program, the provider could theoretically be liable for harm to a patient when the provider knows the telemedicine system is used as a putative filter to decide whether a patient should be reimbursed for prospective in-person health care. Although the digital provider would not itself be making any medical decisions, physicians working within the confines of a system are limited to the inherent diagnostic capabilities of that system. If the digital provider is aware of, or should be aware of, certain diagnostic loopholes that are likely to evade physician detection, it is quite possible that a corporate provider could be held liable when the system has the practical financial impact of denying healthcare coverage.

---

that recommended care is not medically necessary, and therefore not covered by insurance or the health plan, will not affect the treatment ultimately received by the patient"; *see also* Cypress Fairbanks Med. Ctr. Inc. v. Pan American Life Ins. Co., 110 F.3d 280, 283 (5th Cir. 1997) (citing Memorial Hosp. Sys. v. Northbrook Life Ins. Co., 904 F.2d 236, 246 (5th Cir. 1990) ("recogniz[ing] the 'commercial realities' facing third-party providers of health care services ... one of the first steps in accepting a patient for treatment is to determine a financial source for the cost of care to be provided")).


\(^{74}\) *See* Rudolph v. Pennsylvania Blue Shield, 717 A.2d 508 (Pa. 1998).

\(^{75}\) *See* id.
C. Licensure

Another barrier to providers of clinical telemedicine occurs when a doctor provides services across state and national boundaries. Although the practice of medicine does not vary significantly from state to state, in both the United States and Canada, each country's states (or provinces) require doctors practicing within its borders to be licensed within the state. In the United States, such power to regulate local activities is granted to the states by the Tenth Amendment, and in Canada the practice of medicine is likewise regulated on the provincial level. In Australia, on the other hand, doctors must register to "protect the public by establishing and enforcing standards of practice." But, Australia is "arguably better positioned" than either the United States or Canada to deal with licensure issues because Australia operates under a mutual recognition scheme embodied by the Mutual Recognition Act of 1992 on the Commonwealth level and its mirror legislation in the States and Territories, wherein each state reciprocally recognizes medical licenses (or "registrations") issued by other states. Nonetheless, even with Australia's reciprocal licensing, issues still arise regarding jurisdictional choice of law questions.

Thus, in all three countries, the federated treatment of licensure issues inhibits telemedicine because each state defines the "practice of medicine" differently: in terms of whether or not medicine is being practiced and, if so, where the practice is taking place, and thereby subject to regulation. Lately,
however, U.S. states have begun to recognize their mutual interest in allowing some form of licensure reciprocity wherein a doctor licensed in one state is allowed, with some limitations, to practice medicine in another state. Indeed, state licensure of medicine is much less logical than state licensure of the practice of law because the practice of medicine does not vary significantly from one modern state to another. Even if a state-to-state system of reciprocity is established, questions will still remain as to where the doctor is held accountable. Failure to address these questions could inhibit the development of a telemedical system because a doctor may be unwilling to subject himself to suit in a distant and unfamiliar forum. The World Health Organization has proposed making a doctor accountable in his home jurisdiction but has yet to formulate a definitive policy.

D. Reimbursement

In the United States, a corporate provider of clinical telemedicine services may likewise be restricted by statutory anti-kickback provisions on both the

---

81 See Laura Keidan Martin, Not So Fast, It's Regulated Some Warnings for the E-health Biz, BUSINESS LAW TODAY, Sept./Oct. 2000, at 10-12 (discussing the Federation of State Medical Boards' (FSMB) 1996 endorsement of model legislation (the 'Model Act') that would create a "special-purpose license" to practice medicine across state lines for a doctor holding a full and unrestricted license to practice medicine in any state. Under the Model Act, "[t]his special-purpose license would not be required of doctors who engage in the practice of medicine across state lines less than 'regularly or frequently,' meaning less than once a month, less than ten patients per year or less than one percent of the doctor's practice. Nor would a license be required for medical services rendered in emergency situations or for doctor-to-doctor consultations across state lines, unless such consultations took place according to a formal, contractual agreement. The FSMB specifically declined to endorse a model that would have created a single, nationwide license to practice. Several states have adopted legislation based on the Model Act, including Alabama, California, Montana, Oregon, Tennessee and Texas. Others considered but rejected legislation based on the Model Act, including Maryland, North Dakota and Wisconsin.).

84 The Department of Defense (DOD) and the Veterans Administration (VA) are among the most active proponents of telemedicine, ostensibly because their physicians are free to work across state boundaries. See Report on Telemedicine, supra note 14, at 4.3.4.1.

85 See RAYMOND W. PONG ET AL., TELEHEALTH AND PRACTITIONER LICENSURE ISSUES, DISCUSSION PAPER FOR THE ADVISORY COUNCIL ON HEALTH INFO-STRUCTURE 4 (Jan. 1999) (referring to accountability as the "jurisdiction that has the ultimate authority to investigate and discipline telehealth practitioners when things go wrong or when patients lodge complaints").

86 See Sleightholm, supra note 77 (stating "though it is tentatively proposed that practitioners of telehealth would be governed by the rules and regulations which apply to them in their own jurisdictions, there has been no official stance on this question . . . Interprovincial and international telepractice almost certainly will require legislative change.").
federal and state levels. These provisions put restrictions on the payment of funds to induce referrals. Federal anti-kickback provisions apply only to payment under government health care payment programs such as Medicare and Medicaid. While providers need not pay much attention to federal anti-kickback provisions, because Medicare and Medicaid typically do not cover services or devices making use of Web-based technology, many states have adopted analogous prohibitions that apply regardless of the payor.

Canada, with a largely socialized medicine system, has yet to adopt a comprehensive telemedicine reimbursement policy, but some provinces allow reimbursement. Canada's failure to reimburse across the board for telemedical services acts as an inhibitor to the technology because doctors are reluctant to offer a service unless they can be assured that the market will bear the cost. However, governmental reimbursement depends upon doctors proving the efficacy of telemedicine. Thus, telemedicine in Canada faces a “Catch-22” because its usefulness cannot be measured until it is implemented on a large scale and this requires governmental reimbursement, which awaits definitive proof of telemedicine's impact.

---

87 See 42 U.S.C. § 1320a-7(b); see also Office of Inspector General (OIG) Advisory Opinion 99-14 (Jan. 6, 2000) (holding that the use of federal grant funds and the continued operation of a telemedicine network could, according to the circumstances, constitute grounds for the imposition of sanctions for violations of the Anti-Kickback Law, pursuant to § 1128(b)(7) and § 1128A(a)(7) of the Act).


89 See Martin, supra note 83 (discussing various state approaches).

90 See Pong, supra note 85, at 12 (stating that “[b]ecause of uncertainties and concerns about the impact of telehealth, many third-party payers, including provincial/territorial Ministries of Health, are reluctant to change reimbursement policies to fund telehealth”).

91 Four Canadian provinces—Nova Scotia, Manitoba, Saskatchewan and Alberta—have adopted reimbursement policies for their practitioners. See Industry Canada, supra note 38.

92 See Pong, supra note 85, at 3 (stating that “unless the reimbursement issue is appropriately addressed, it is unlikely that telehealth will be implemented on a broad scale. Physicians are unlikely to provide extensive telehealth services if they are not compensated, in one way or another, for their time and effort.”).

93 See id. at 12 (noting that “unless telehealth is practiced in real-life settings and on a much broader scale, we will not be able to assess its impact and implications”).
E. Anti-Self-Referral

Similar to anti-kickback provisions, self-referral prohibitions on both the federal and state levels in the United States provide potential barriers to the provision of clinical telemedicine. These provisions regulate the referral of a patient to another provider who has a financial relationship with the entity or doctor making the referral. As with kickback prohibitions, federal restrictions are not a major concern because they only apply when the payor is a federal health care program and Medicare and Medicaid typically do not cover telemedicine services. However, because many state regulations apply regardless of the payor, a provider of telemedicine will need to structure its business model accordingly and may have to refrain from offering participating doctors equity interests or other financial incentives that induce referrals.

F. Regulatory Agencies

In the United States, the regulatory environment for telemedicine is crowded. The Federal Trade Commission (FTC) and the Food and Drug Administration (FDA) regulate telemedicine providers. Marketing and advertising are subject to FTC regulation, while the FDA is charged with regulating medical devices and pharmaceuticals. The 1996 Telecommunications Act mandates that the Federal Communications Commission (FCC) and the states take measures to increase advanced telecommunications services such as the requirement that the FCC assure that health care providers serving rural areas have access to telecommunications services "necessary for the delivery of health care" at rates that are comparable to those for similar services in urban areas. Additionally, states may enact statutes that regulate advertising of health services. In Australia, despite a distinct absence of a national regulatory policy regarding telemedicine, the national government is working to ensure rural access to telemedical services.

94 See The Stark Act (42 U.S.C. §1395nn); see also Martin, supra note 83, at 12-14.
95 See Martin, supra note 83, at 12-14 (discussing the range of state regulations: from prohibitions that only bar referrals to entities in which a doctor has an investment interest, to prohibitions that bar referrals to any entity with which a doctor has any compensation relationship to prohibitions that provide for exceptions as long as the doctor's financial interest is disclosed to the patient or as long as the physician refers within his or her group practice).
97 Report on Telemedicine, supra note 14, at 4.3.4.3.
98 See Martin, supra note 83, at 12-13.
99 Accordingly, the Commonwealth Government intends to include a requirement for the
G. Confidentiality

Telemedicine providers should be aware of privacy and confidentiality concerns regarding the storage and dissemination of patient records. Treatment of telemedicine privacy issues should not substantially differ from treatment of "traditional" storage of electronic health records. Although many industry participants argue that government regulation is a superfluous addition to self-regulation through internal organizational policy, the Law Council of Australia (LCA) noted that "[a] set of national principles, which are not legislatively based, are [sic] relatively meaningless from a legal perspective."

While regulations exist at both the state and federal levels in the United States, the broad requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must be examined with scrutiny because unauthorized disclosures can result in substantial civil and criminal penalties. HIPAA directly regulates the security and privacy of electronic health-care information maintained or transmitted by health-care providers, health plans and health-care clearinghouses. The statute also indirectly regulates patient information of other entities by requiring covered entities to maintain contractual "chain of trust agreements" with all business partners to

---

100 See J.P. Fanning, Confidentiality of Individually-Identifiable Health Information: Recommendation for a Federal Law, A PAPER DELIVERED TO THE JOINT WORKING GROUP ON TELEMEDICINE, May 21, 1998 at 14 (arguing that "many issues . . . can be dealt with by thoughtful application of principles and practices we already know"); but see National Technical Information Service, U.S. DEP'T OF COMMERCE TELEMEDICINE REPORT TO CONGRESS (1997) (arguing that "telemedicine technology brings with it concerns about privacy, security and confidentiality that go beyond those associated with protecting medical records . . . [and that] because of the unique combination of patient data, video imaging, and electronic clinical information that is generated between two distant sites during a telemedicine encounter, privacy concerns that normally pertain to patient medical records may be magnified within the telemedicine arena or may be different in character altogether").

101 See National Research Council, Computer Science and Telecommunication Board, For the Record: Protecting Electronic Held Information (1997) at 166 (arguing that "[o]rganizational policies and practices are at least as important an element of security [as is legislative intervention]").


ensure that those partners institute appropriate procedures to ensure confidentiality.

HIPAA regulations impose a wide array of security requirements such as certification requirements, data back-up plans, personnel security, regular virus checks, access-control features, security incident procedures, authentication requirements, and prior authorization by patient before individually identifiable health-care information may be used or disclosed for a variety of purposes. Two requirements that have particular relevance to telemedicine are the requirements that all health information be kept in electronic form and that each individual be given a unique health identifier. Acting in combination, the provisions create a series of nationwide and potentially interconnected databases of individually-identifiable medical records.

In Australia, there is more concern with linking multiple databases and including individual identifiers. The Australian government's proposal for an Australia Card, which was to be a unique identifier for every Australian, was met with intense debate between 1985 and 1987 and the proposal was permanently tabled due to privacy concerns. Although such a database would have enabled many demographic studies and allowed better enforcement of laws, the Australian public thought the benefits were outweighed by the potential invasion of their privacy. Although Australia has no legislation which protects privacy across all jurisdictions, it has developed an Australian standard: "Personal privacy protection in health care information

---

104 See Martin, supra note 83, at 13-14.
105 42 U.S.C.A. §§ 1320d-2, 1320d-4 (West Supp. 1998) (requiring health plans to conduct electronic transactions when requested, either directly or through a clearinghouse, which implicitly requires the information to be available in electronic form).
109 See id. (noting that there is only a Commonwealth Privacy Act 1988, which does not apply outside Commonwealth organizations or to any private sector organization. The Australian states do not have any privacy legislation, though New South Wales is working on a bill); see also Milstein, supra note 3 (illustrating the Australian privacy "patchwork quilt" by noting the existence of "the Federal Privacy Act, the Victorian Health Services Act 1988 (particularly section 141); the National Principles for the Fair Handling of Personal Information published by the Federal Privacy Commissioner, a series of standards promulgated by Standards Australia (for example, the Standard Personal Privacy in Health Care Information Systems AS4400-1995); and the Victorian Data Protection Framework bill.")
The standard is a statement of general principles and procedures and is not currently a prescriptive technical document, though technical issues will be addressed. The standard anticipates situations involving cross-border information transmission and thus reflects international data management standards. In addition to legislative standards, Australia has appointed a Privacy Commissioner to oversee national privacy policy.

As with Australia, Canada has enacted standards reflecting international privacy standards. Canada’s privacy policy has been described as a “patchwork” because jurisdiction is shared by both the national and provincial governments. The Canadian Standards Association (CSA) Model Code for the Protection of Personal Information is a voluntary code intended to harmonize Canadian standards with the same OECD code on transborder personal data flow with which the Australian standard complies. On the federal level, the protection of personal information only applies to information that is in the public sector. While such information is also regulated according to provincial and territorial laws, regulations, and guidelines, with the exception of Quebec, no state has a comprehensive policy that covers data in both the public and private sectors. In October 1998, however, the federal government introduced legislation that would cover private sector data for a limited time period. Similarly, the Canadian Institute for Health Information (CIHI) recommended that the CSA’s Model Code for the


111 See Cheong, supra note 108.


113 See Kevin O’Connor, Confidentiality, privacy and security concerns in the modern healthcare environment, v. 26 no. 3 AUSTRALIAN COMPUTER J. 70-77 (1994) (noting the Commissioner’s broad approach to privacy concerns stems from a belief that privacy is considerably more encompassing than either “security” or “confidentiality”).

114 See Report on Telemedicine, supra note 14, at 5.2.3.1.11.


116 See Report on Telemedicine, supra note 14, at 5.2.3.1.11.

117 See Bennett, supra note 115.

118 Bill C-54, the Personal Information and Electronic Documents Act.
Protection of Personal Information be adopted. 119 This patchwork of regulation has inhibited the development of telemedicine systems in Canada because the variety of standards have interfered with creation of requisite economies of scale that allow the operation of a healthy business model. Likewise, as in any industry, uncertainty interferes with capital formation.

V. CONCLUSION

Telemedicine applications have the potential to drastically alter the delivery of medicine. However, the scattered legal treatment of telemedicine lacks logical coherence. As a result, the introduction of new digital technologies are inhibited in the United States, Canada, and Australia. Thus, the national legislature in each nation needs to address telemedicine needs in each country to answer timely and important questions. Without a definitive statutory response, the capital markets are forced to conjecture as to whether or not traditional legal principles apply to the regulation of telemedicine.

119 See Industry Canada, supra note 38.