

## TELEMEDICINE AND THE LAW

LTC Lanie Olmsted<sup>1</sup>

Background: Telemedicine<sup>2</sup> is not medicine of the future; but rather a growing trend of the here and now. Almost three quarters of the healthcare executives responding to a 1995 national survey on trends in healthcare reported that their organizations were involved in telemedicine projects or that they are a priority for the future. The Federal government has been funding telemedicine graphics totaling more than \$100 million through a variety of agencies. The technology is moving with alacrity to satisfy the demand for telecommunications and video to connect geographically separated health care organizations.

As is often the case, the legal and regulatory environment has not kept pace with the technology. The extent to which the YOYO (you're on your own) principle has been applied to the information superhighway makes hard and fast policies difficult to articulate; accordingly, this article will attempt to point out the potholes to dodge along the way with preventative recommendations albeit that may, in the future, prove futile.

Telemedicine's legal issues fall into three categories: (1) the traditional medico-legal issues not unique to the medium; (2) conflicts in state law, which telemedicine amplifies because it connects geographically separate facilities; and (3) issues unique to telemedicine. Given the general familiarity with the issues in the first category, I will emphasize the second and third categories.

Assumptions: For the purposes of legal analysis, assume the following telemedicine scenario. A medical center of excellence, typically an urban, tertiary-care academic-based or large medical center (the "host") is linked to smaller, often rural, general community hospitals and health centers. The purpose of telemedicine in this environment is for remote clinical diagnosis and treatment, remote continuing medical education, and access to central data repositories for electronic patient records, test results, and care outcomes. Each system user has varied access to information and other users. The system also identifies and evaluates clinical pathways and is used to develop clinical guidelines. It is these guidelines that the network would

---

<sup>1</sup>Center Judge Advocate, Madigan Army Medical Center, Tacoma, WA

<sup>2</sup>Literally, "telemedicine" is medicine at a distance ("tele" is a Greek-based prefix meaning distant or at a distance).

apply to credential its clinical staff, govern the distribution of hardware, software, and access.

Licensure:

One issue that comes to mind, given the assumptions above, is whether the network itself needs to be licensed. One goal of a licensure requirement is ensuring that facilities meet minimum quality standards. Historically, hospitals have received licensure for their facilities with the State of operation. Would a health care system, then be required to possess a license from the State in which it has a "virtual" facility? It is likely that states may require some form of licensure or other assurances of minimum technological standards (such as the minimum resolution of network-transmitted images).

The question of licensure also becomes an issue to the individual telemedicine practitioner. Is it necessary to obtain a license in another state where telemedicine consultations are performed?

A survey of State laws reveals the panoply of approaches.<sup>3</sup> Some, like California, have opened their borders to telemedicine, both by defining telemedicine narrowly to exclude telephone conversations and E-mail communications between health care practitioners and patients, and by relying on the requirement that the patient give advance informed consent to receipt of health care via telemedicine.<sup>4</sup> In contrast, Georgia, which has developed an elaborate intrastate telemedicine network, has enacted a tough new licensing law which appears designed to protect the Georgia medical establishment from out-of-state telemedicine practitioners. Only if an out-of-state physician renders the telemedicine services without compensation, on an emergency or occasional basis, or to a Georgia medical school, will that physician not be deemed to be practicing medicine without a license in Georgia.<sup>5</sup>

Continuing a survey of states<sup>6</sup> that have addressed the interstate practice of telemedicine reveals that the answer to the individual licensure requirement for physicians question varies from state to state. The regulatory efforts

---

<sup>3</sup> See "An Overview of State Laws and Approaches to Minimize Licensure Barriers," Linda Gobis, Telemedicine Today Magazine, Vol. 5, #6 and Vol. 6, #1.

<sup>4</sup> Cal. Bus & Prof. Code §2290.5(a).

<sup>5</sup> Ga. Code Ann. §43-34-31.1 (1997).

<sup>6</sup> Since 1994, twenty state have passed laws which specifically address telemedicine licensure.

have often created rather than eliminated barriers.<sup>7</sup> In an effort to establish uniformity there is a proposed model statute.<sup>8</sup> No state has adopted the model statute to date.

Until resolved by a national standard, physicians and their legal advisors should research the laws in the states where they intend to practice telemedicine to determine the following:

- In how many states will the telemedicine consultations be performed? If the answer is only one or two, it may be easiest to simply obtain licensure in those states. In the instance of physicians employed in the Federal sector it is not as difficult an issue.
- Do the states where telemedicine practice is planned have a physician consultation exception? What are the limitations of this exception?
- What types of healthcare providers will be involved in the consultation? The licensure requirements may differ if a non-physician is involved.
- If the law is unclear or appears to be unfavorable, is it possible to obtain advance approval or an opinion from the state medical board?

The consulting physician is not the only one at risk. A licensed physician who aids a non-licensed physician in practicing medicine may also face civil fines, suspensions or revocation of his or her medical license.

Accreditation:

Federal regulations, state law, and private accrediting standards (such as JCAHO standards) require hospitals to adequately credential providers and to ensure that medical staff members are competent in their practice areas. Individual institutions may also have divergent credentialing standards. Recently, the JCAHO has promulgated guidelines to accredit healthcare networks, but

---

<sup>7</sup>Kansas state law requires physicians who treat, practice or diagnose individuals residing in Kansas to obtain a medical license in that state. K.A.R. 100-26-1 (1995). See also, Center for Telemedicine Law--Newsletter (June 1997), for a comprehensive discussion of state law licensure and practice of medicine issues.

<sup>8</sup>In April, 1996, the Federation of State Medical Boards developed a Model Act to regulate the practice of medicine across state lines to respond to telemedicine issues. The Act would require physicians practicing medicine across state lines to obtain a special license issued by a state medical board. This "special purpose" license would be limited to practicing across state lines if a physician regularly or frequently engages in telemedicine.

questions still remain. Must hospital-based telemedicine networks focus attention on, and draft medical staff bylaw changes to reflect telemedicine proficiency? Must there be separate standards at all for "virtual" practice? Must remote physicians be admitted to the host's medical staff? If so, does this then impose upon the host a duty to continuously monitor remote physicians' competence and skill to the same degree as it does with other staff members? No clear answers emerge.

Further, practitioners who use the new technologies must upgrade their skills appropriately. Failure to correctly calibrate an instrument can increase the likelihood of inaccurate diagnosis. Deficiencies or failures in equipment used to transmit an image, video clip or patient record may increase liability. In addition, the potential to recover large awards from telecommunications companies and manufacturers may create incentives to bring suit against all of those involved in a telemedicine consultation.

#### The Electronic Medical Record: Privacy

Telemedicine does not change the duty of confidentiality and the fundamental privacy issues involved, but it does raise the concern that patients may be unaware of the extent to which their medical information may be disclosed to others. Virtually any telemedicine consultation involves electronic transfer of patient medical records and information. Patient privacy must be a major consideration in the development of information systems. However, like the blind man and the elephant, the consideration of privacy may depend heavily on who is examining the system. To the patient, it means that no one has unnecessary access to his data. To the hospital administrator, it is an impediment to his access to data needed for management. To physicians, it can represent a time-consuming limitation on medical practice. To information system developers, it is expensive, inelegant, and time consuming. Given that the patient is only one of these participants, it is not surprising that there is a tendency to compromise patient privacy in any system development.

At the current time, medical privacy regulations normally do not contain specific technical requirements. Some states like California, attempt to deal with the privacy issue by requiring patients to give informed consent to health care delivery via telemedicine (See fn. 4). Will consenting patients fully appreciate the consequences of having their examinations electronically communicated to numbers of

people they cannot see, including technical support people as well as health care professionals?

Congress is required, by the Health Insurance Portability and Accountability Act of 1996, to enact national legislation protecting health information by August 1999.<sup>9</sup> The Executive Branch has proposed privacy rules as part of the Patient's Bill of Rights initiative. To date, these efforts appear mired in election related political debate and have not progressed through Congress.

The Federal Privacy Act is the major legal protection of individual privacy for the data contained in systems of records maintained by the federal government. It is the model upon which state systems are developed but it contains few specific measures which must be taken to protect privacy. In a similar way, hospitals cannot automatically assume that compliance with existing clinical system norms or privacy accorded to paper records in hospitals sets the level of privacy required in the electronic medium. The novel methods of using data inherent in a computerized information system also allow novel methods of invading privacy.

Access to networked systems increases both the number of users and the number of patient records. Arguably then, the risk of invasion of privacy increases exponentially with the increasing number of participants. Many users rely on a kind of paper privacy, such as requiring all employees to sign documents that they will not reveal medical data. Unfortunately, such methods have met with limited acceptance by the courts. In a case involving the inadequacy of the hospital protection of a patient's chart containing a diagnosis of AIDS, the court stated:

While there is some dispute as to the propriety of charting an acceptable medical practice, the Medical Center felt there were safeguards in the general confidentiality guidelines set forth in its by-laws and employee manuals. According to stated policy, charts were limited to those persons having patient care responsibility, but in practical terms, the charts were available to any doctor, nurse or other hospital personnel. Despite the CDC's recommendation that access to HIV results be limited, the Medical Center had no policy physically restricting access to the HIV test results or the charts containing the results to those involved with the particular patient's care.

---

<sup>9</sup>Pub.L.No. 104-91, August 21, 1996.

It is not the charting per se that generates the issue; it is the easy accessibility to the charts and the lack of any meaningful Medical Center policy or procedure to limit access that causes the breach to occur. Where the impact of such accessibility is so clearly foreseeable, it is incumbent on the Medical Center, as the custodian of the charts, to take such reasonable measures as are necessary to insure that confidentiality. Failure to take such steps is negligence . . . .

Insuring confidentiality even by Medical Center employees required more, in the present case, than simply instructing employees that medical records are confidential. The charts are kept under the control of the Medical Center with full knowledge of the accessibility of such charts to virtually all Medical Center personnel whether authorized or not. Little, if any, action was taken to establish any policy or procedure for dealing with a chart such as plaintiff's.<sup>10</sup>

The language above should bring shudders to the average hospital administrator or legal advisor. Since virtually any telemedicine consultation involves electronic transfer of patient medical records and information, it is imperative that systems be constrained by some sort of guidelines. Unfortunately, since the flow of health care data across state borders, often with conflicting regulations, can result in confusion for providers and patients alike, it is imperative that telemedicine providers reexamine their traditional record keeping protocols.

Consider the following in devising appropriate protocols:

Who is responsible for retaining records of the consultation? Are all staff involved in the consultation trained to ensure that electronic patients records are properly created, updated and archived?

Is access to sensitive information restricted?

In what format should information from the consultation be stored?

Some of the pitfalls surrounding electronic patient records can be avoided by establishing and enforcing strict protocols that are clearly understood by staff. These guidelines are not, in and of themselves, enough protection.

---

<sup>10</sup>Beringer v. The Medical Center at Princeton, 249 N.J. Super. 597; 592 A.2d 1251; April 25, 1991.

Even though no security system for information will be completely immune from discontented insiders or determined hackers, health information managers should implement a system which ensures high levels of clinical access and utility while maintaining secure and confidential patient information. Technical safeguards, as well as administrative and procedural methodologies, should be established.

An example of a technical safeguard useful for telemedicine is cryptography. Cryptography can be used to encode data either before transmission or while stored in a computer (encryption), and can provide an electronic signature and/or verify that a message has not been tampered with (message authentication). Encryption scrambles a message so that its meaning is not easily read. Only authorized individuals have the decrypting key. Message authentication is also possible. Encryption algorithms can be used to authenticate messages. Besides cryptography, there are a variety of methods which can be utilized depending on the health information system. Personal identification and user verification also act to ensure that those accessing a network are authorized to do so. Although authentication that relies solely on passwords can fail to provide adequate protection for computer systems, they add a degree of protection that will have to suffice until the industry develops a readily available and inexpensive alternative.<sup>11</sup>

#### Malpractice Liability:

Health care systems owe a duty to patients in their facilities to prevent harm negligently caused by them, their employees, and agents. The law has developed to where health care systems must adequately supervise and credential their staff and independent physicians providing services under their auspices. Courts have not been faced, however, with the situation where a telemedicine host has no other affiliation with remote physicians and hospitals than their involvement in the network. One can conceive a court placing upon a network a duty to adequately supervise the usage of the telemedicine system by all network partners, especially as the host exercises increasingly greater control over network activities.

---

<sup>11</sup>See "TechTalk: Security of Internet-based Telemedicine Systems," Telemedicine Magazine (Jan 98), for a comprehensive discussion of information security issues regarding the challenge facing health care information systems managers.

Some believe that use of these technologies will lower liability since telemedicine consults involve two practitioners working together resulting in more comprehensive care leading to better patient outcomes. Alternatively, as technology increase in sophistication, so do patient expectations.

Historically, physicians were held to the standard of care practiced by the average member of the medical profession practicing in the same medical specialty and same geographic location as the defendant physician. This "locality rule" has been significantly eroded in the last 20 years by the nationalization of medical education, residency training and continuing medical education requirements. Now telemedicine is likely to eliminate the locality rule entirely.

Legal parameters for medical malpractice are the same whether the claim relates to telemedicine or other technologies. First, it must be determined that a physician-patient relationship existed. If so, the issue of whether the physician breached his or her duty of care must be addressed. A physician-patient relationship may arise out of an expressed or an implied agreement. Generally, the courts have found that provision of medical care creates that relationship, even in the absence of reimbursement. Most telemedical consultations would likely be viewed as establishing the requisite physician-patient relationship. Accordingly, practitioners wishing to limit involvement in a case should define the limits of their participation to the patient up front. Such a consent should be in writing and retained by the consulting physician.

At first glance, the duty of care owed to a patient is not extraordinary. As noted above, providers must exercise the same degree of skill ordinarily exercised by other members of their profession. It is important to consider that the particular circumstances under which a physician practices are not irrelevant. Whether a diagnosis made via telemedicine will be held to the same standards of care as one made in person will depend on available alternatives, sophistication of the technology, and patient expectations.

Unlike other medical technologies, many of the tools involved in telemedicine consultations or decision support systems were developed for non-medical purposes. Even telemedicine experts disagree about optimum technical specifications for compression, resolution and matrix size. Finally, because even state-of-the-art technology quickly becomes outdated, it is unclear what obligations practitioners have to upgrade their systems.

Technical issues do not present only legal considerations. The appropriateness of using telemedicine in a particular setting might also be argued. Allowing non-physicians to participate in a telemedical consult, or to use a medical database to engage in electronic patient triage, present other potentially contentious issues in the areas of informed consent and choice of laws.

The issues become murkier as telemedicine matures. For example, if remote robotic surgery is done through an interstate network or if telemedicine networks make physicians available to patients in the absence of physicians at the patient's location, it seems clear that the physician who remotely diagnoses and treats patients interstate would be required to secure a patient's informed consent to render care. The standards for when consent is "informed" vary by state. To the extent that the standards conflict, which state's standards apply? One glaring example of conflict is illustrative. In some states, the information necessary for a patient to give an informed consent is that which the reasonable patient would consider important. In others, the standard is what the prudent, reasonable provider would consider necessary. The answers to these questions often determine the outcome of medical malpractice litigation. Cases involving "tele-consultation" across state lines will raise classic choice of laws issues. Should the court apply the law of the state in which the patient lay on the examining table, or the state where the "tele-expert" viewed the patient?

As telemedicine and healthcare information systems become widely adopted, providers face a catch-22. They may be just as liable for not using technology as they are for applying technology inappropriately. It is imperative for providers to stay apprised of developments and make informed decisions about how those developments should be deployed.

#### Conclusion:

Advances in integrated health information systems create opportunities to streamline and improve delivery of quality health care. Computerized health care delivery, and telemedicine applications in particular must address informational privacy issues. National legislation is certainly necessary to clarify the vagueness stemming from inadequate federal and state laws. However, until such legislation is passed, those involved in the delivery of health care must take what steps they can to ensure that personal records remain confidential and secure. Internal

and external reviews of one's existing and/or proposed recordkeeping methodologies, from both a legal and a technical perspective, are advisable. By showing that privacy controls and safeguards are being researched and implemented, one may lessen the opportunity for allegations of negligence or reckless disregard for privacy concerns.

HELPFUL WEB SITES:

1. Center for Telemedicine Law: [www.ctl.org/](http://www.ctl.org/)
2. ArentFox Telemedicine Home Page:  
[www.arentfox.com/telemedicine.html](http://www.arentfox.com/telemedicine.html)
3. Telemedicine Today Magazine: [www.telemedtoday.com/](http://www.telemedtoday.com/)

