Does Products Liability Litigation Threaten Picture Archiving and Communication Systems and/or Telemedicine?

Joseph P. McMenamin

Numerous writers have commented on barriers to the growth and progress of telemedicine. Among these barriers are reimbursement concerns, professional liability exposure, licensing restrictions, hospital credentialing questions, and other problems. A legal threat not generally described in the literature to date is the possibility that products liability claims could be brought against manufacturers and distributors of hardware, software, and peripherals used in providing telemedicine services. Several of these concerns extend to picture archiving and communication systems (PACS), including, of course, teleradiology. This article considers that possibility in the context of several potential plaintiffs' theories, discusses currently applicable law, and proposes approaches to diminishing the magnitude and severity of this potential threat. Copyright © 1997 by Defense Research Institute Inc.

KEY WORDS: Radiology, PACS, legal aspects, products liability, confidentiality, encryption, data compression, artificial intelligence, telemedicine

TELEMEDICINE can be defined in various ways, but a serviceable definition in common use is "medical practice across distances via telecommunications and interactive video technology."¹ High speed computers and broad bandwidth communications links permit a physician in one location to examine and treat a patient in another city, state, or country, or at sea or in space, through rapid, two-way transport of voice, video, and data. Telemedicine tends to encourage the creation and maintenance of electronic medical records, which may improve collection and preservation of health data, permit automated pharmaceutical requests, and facilitate comparison of current diagnostic images with old studies. Telemedicine may also expand educational opportunities for health care providers, increase local medical self-reliance, and diminish the sense of professional isolation that can sometimes afflict practitioners in rural areas. Another attractive feature of telemedicine is its potential to enhance understanding of the epidemiological profile of a particular community, including, eg, a specific medical center. This could improve antibiotic selection and permit earlier detection of epidemics.² Educational seminars brought to patients by telecommunications could enhance their understanding of their own medical problems, and home health applications may permit cost-effective

monitoring of vital signs and improve patient compliance.

Picture archiving and communication systems (PACS) also handle images and text using computers and high bandwidth communications. Initially focused in single radiology departments, PACS now are found not only throughout hospitals but also in enterprise-wide medical networks spanning a number of hospitals, offices, and municipalities. A growing trend toward filmless radiology places complete reliance on these computer-based systems for the handling, display, and archiving of these medical images. PACS are also used for handling images in dermatology, pathology, cardiology, and other medical specialties, and for medical conferencing and teleconferencing. Teleradiology is often part of a PACS, and some of the better teleradiology systems have been developed as part of a PACS. With their common grounding in technology, PACS and telemedicine give rise to some of the same legal concerns.

Transmission of medical data to locations distant from the patient currently requires use of one of three following main technologies: microwave (line-of-sight only), satellite (costly), and long distance carrier lines (either fiber optics or copper cables). A telemedicine system also requires computer technology, with or without multimedia capability. Just as transmission systems may differ, so too can the other components of a telemedicine system. In a simple system there may be one-way visual capability and phone consultation by fax, with or without one-way audio for use in continuing medical education, for example. In more elaborate systems there may be two-way video and audio capabilities; dermoscopes, otoscopes, ophthalmoscopes, eye-movement monitoring cameras, electronic stethoscopes, endoscopes, microscopes, and other visual

From the Richmond office of McGuire, Woods, Battle & Boothe, L.L.P.

Communications regarding the article should be directed to Dr. Joseph McMenamin, McGuire Woods Battle & Boothe LLP, One James Center, 901 E Cary St, Richmond, VA 23219.

Copyright © 1997 by Defense Research Institute Inc.

Reprinted courtesy of Defense Research Institute Inc., Chicago, IL.

0897-1889/98/1101-0003\$8.00/0

diagnostic tools; and digitized “conventional” radiographs, ultrasound images, pathology images, echocardiograms, computed tomography (CT), magnetic resonance imaging (MRI) scans, and so on. In the future, artificial intelligence (see later section) may guide paramedics or physicians’ assistants in performing techniques solely restricted to physicians today. Exotica such as robotic surgery may move from science fiction to reality, particularly, as in warfare, where doctors are scarce and the need is acute. To a limited extent, in fact, services of this type are being provided today.³

Telemedicine may permit health care services to be offered in ways never previously available—but it also faces thorny legal problems. Many of these have received fairly extensive attention, including reimbursement limitations, licensing problems, hospital credentialing questions, medical malpractice (with its potentially complicated jurisdictional and conflict-of-laws issues), antitrust, and regulatory concerns. Most commentators seem not to have focused extensively on the possibility of products claims, however, perhaps because none has yet been reported. It may be a mistake, however, to dismiss the possibility that manufacturers and distributors of hardware, software, and peripherals may face increased exposure to claims as a result of their activities. In at least one case, a litigant, himself a teleradiologist, alleged that a competitor’s “excessive” use of teleradiology to transmit “non-emergency films” resulted in “poorer film quality and poorer correlation between radiological studies and pathological results. . . .”⁴ Telemedicine advocates might well deny the claim that image degradation is a significant problem in teleradiology, but the fact that such a claim has been made in a medical staff dispute suggests the possibility that it could be raised in other settings. In this article, we consider some technical aspects of telemedicine, and then consider some features of the legal maze that practitioners and those supporting them may be required to navigate as telemedicine services become more widespread.

SOME TECHNICAL ASPECTS OF POTENTIAL LEGAL SIGNIFICANCE FOR PACS AND/OR TELEMEDICINE

Confidentiality

A healthcare provider’s duty to maintain the confidentiality of medical data is at least as old and well-accepted as the Hippocratic Oath: “What I

may see or hear in the course of the treatment or even outside the treatment in regard to the life of men, which on no account must one spread, I will keep to myself.” Security in multiuser and distributed computer systems, however, is difficult to achieve.⁵ Those claiming a right of access to health data have never been more numerous than they are today, for they include providers, insurers, self-insured employers, managed care organizations, public health agencies, researchers, oversight agencies, and managers of pharmaceutical benefits programs. It is not clear whether companies providing telemedical support need meet confidentiality obligations of health care professionals, but plaintiffs might so argue.

Four types of confidentiality problems have been anticipated in telemedical practice.

1. Improper disclosure—such as leaving visible or at least easily retrievable data on a screen.
2. Unauthorized access—the hacker problem.
3. Identifying individual patients by aggregating data. “Computers linked together make it possible with relative ease to aggregate into a mosaic a large amount of individual data stripped of personal identifiers that will identify a particular individual with high confidence.”⁶
4. Data integrity and authenticity. “Preservation of data integrity means preventing improper alteration or deletion of data, while data authenticity requires assurance that information presented as related to a specific patient is not mismatched or forged.”^{6,7}

Risk managers and counsel to entities engaged in telemedical services should anticipate the possibility that claims could arise out of all of these situations.^{8,9}

Current Law on Confidentiality. Existing law offers only limited guidance in structuring telemedicine systems to protect confidentiality, and in some ways may actually aggravate the problem. First, there seems to be no overarching authority to consult.¹⁰ Under the Privacy Act of 1974,¹¹ the provider owns the data in a patient’s chart, but for administrative uses in support of reimbursement, the patient must release them.¹² Information not originating from federal agency records enjoys no protection under this section.¹³ Neither a state university¹⁴ nor a hospital is an agency of the federal government within the meaning of the Act,¹⁵ even if it receives federal research grants.¹⁶

Private not-for-profit corporations engaged in business with the United States government are not agencies of the government within the definition of the Privacy Act even though such businesses receive funding from and to some extent are regulated by the federal government.¹⁷ The Privacy Act, then, would presumably be inapplicable to business corporations.

The Americans with Disabilities Act (ADA)¹⁸ provides that certain types of medical data on employees must be kept confidential, in part to protect covered employees from discrimination. The scope of this protection, however, is not yet clearly defined. ADA restricts employer access to information in preemployment physicals and other sources, but it provides no guidance on whether employers may gain access to information generated in employee health benefit programs.¹⁹ Other legislative initiatives in the last Congress would have offered extensive privacy protection: The Medical Records Confidentiality Act of 1995,²⁰ the Fair Health Information Practices Act,²¹ and the Medical Privacy in the Age of New Technology Act.²²

Under the Uniform Healthcare Information Act,²³ healthcare information and personal data are deemed sensitive if when improperly released they could harm a patient's interests.²⁴ The Act restricts release of information and provides procedures necessary for release, but it has so far been adopted only by Montana and Washington. Medicare permits, and in fact encourages, use of electronic records, but only if providers promote their security by limiting access to those authorized to read them.^{2,25} A second indication of the limited guidance of existing law on telemedicine confidentiality is that the law varies greatly from state to state. In fact, the law of one state may be inconsistent with that of another and with federal law with respect to who is entitled to access to records, and what steps need to be taken to protect privacy.^{2,10} Third, even within a given state, applicable law is often fragmented and can arise from both civil and criminal statutes, from common law, and sometimes from regulations.² Fourth, again merely within a single state, applicable law may vary with the type of provider.² In short, current law on confidentiality is a welter of conflicting, confusing authority, and such inconsistency and complexity may create a trap for the unwary.

The (Kennedy-Kassebaum) Health Insurance

Portability and Accountability Act of 1996²⁶ is mainly concerned, as its popular name suggests, with transferring health insurance coverage when an employee changes jobs. In its Administrative Simplification section (codified at 42 US Code [USC] §§ 1320d- 1320d-8), however, the Act requires development and adoption of standards for the electronic exchange of health information, and directs Congress or the Secretary of Health and Human Services to develop privacy rules to govern such exchanges by February 1998. It also establishes standards for electronic claims processing, referrals, and other financial and administrative functions. The Act provides for the establishment of unique identifiers for providers, patients, employers, and plans, which may facilitate sharing of data and linkage among physicians, programs, plans, and agencies. It preempts state "quill pen" laws and provides for "electronic signatures," which may improve message authentication, streamline information processing, and reduce the need to maintain paper records for legal accreditation or regulatory purposes. Perhaps most important for the future growth of telemedicine are the provisions in Section 192, which directed the Health Care Finance Administration to report to Congress by March 1, 1997 on its study of reimbursement for telemedicine services. The Act's contribution to clarity and efficiency, however, must be considered in light of its creation of potential liability. The easier it is for authorized health professionals to get access to sensitive information, the easier it may be for others, presumably, to do so as well—perhaps as easily as one can gain access to information on the internet.²⁷ The consequences of violations are serious: the Act establishes fines of up to \$250,000 and prison terms of up to 10 years for anyone who breaches the confidentiality of an individual's medical record.²⁶

Universal Identifiers, Authentication, and Audit Logs. Universal identifiers assign a particular code to a particular individual, effectively creating a national identification mechanism. Assigned to a provider, such a number (or alphanumeric code) could help reduce the risk that a patient's data could be sent to the wrong physician. Assigned to a patient, an identifier could reduce the risk that the wrong patient's data are transmitted. To improve the chances of reasonable efficacy, such identifiers should probably be unique to each individual. Proposals to use a patient's Social Security number

for this purpose have been criticized, in part because doing so could give access to so much other data unrelated to health care.²

Other techniques are available to verify the identities of the communicators. Called "authentication techniques," these include the use of passwords, keys, and other automated identifiers.^{2,5} Audit logs can be used to discourage data theft.^{2,5}

Arguably, the confidentiality that can be achieved in electronic medical record-keeping is equal to or better than that obtained in a paper-based system. Given the ability of a determined hacker to probe such sensitive data as the inner workings of the nation's defense system, however, it seems highly unlikely that a foolproof electronic system is possible. A password that can be overheard or easily guessed, for example, may offer little protection. More complex passwords, or those that must be changed periodically, are harder to remember, and so more difficult to use, and so less likely to be widely adopted. More elaborate systems are available, but at present are not generally deemed cost-effective in healthcare.

Cryptography. "Encryption . . . involves running a readable message known as 'plaintext' through a computer program that translates the message according to an equation or algorithm into unreadable 'ciphertext'."²⁸ This process renders data difficult or impossible to read without a codebook or deencryption key.¹⁹ Encoding may be done either before transmission of data or while they are stored in computer memory, and may employ public-keys (available to anyone to encrypt messages), private keys (which decrypt messages), and message authentication codes, digital signatures, authentication and identification schemes, intrusion and virus detection techniques, and firewalls.

Some are calling for obligatory encryption now.¹⁰ Telemedicine, however, envisions practice across not only state lines, but across national boundaries as well, and export of cryptographic techniques (except to Canada) has historically been subject to significant governmental control. New Commerce Department regulations of export of encryption related software, hardware and other technology became effective December 30, 1996. Before then, encryption devices and software were designated as defense articles under Category XIII(b)(1) of the highly regulated U.S. Munitions List.²⁹ There have been some recent liberalizations of existing law on export of cryptographic technology by adoption of

a "key management" approach, under which encryption software of any strength (usually measured by bit size) may be exported without a license so long as a "key" to breaking the code is held by an acceptable recovery agent. Changes to the International Traffic in Arms Regulations (ITAR), which controlled encryption export before December 30, 1996, had already allowed broader export trade in strong cryptography. Implemented by the Office of Defense Trade Controls, ITAR restricted export of dual-use cryptography: that which could serve both military and civilian purposes.

Under the new regulations, three categories of encryption items are exportable under Commerce License Exceptions: 40-bit "mass market" encryption software, subject to a one-time review by the Bureau of Export Administration (BEA); 56-bit key length nonrecovery encryption software (provided the exporter implements a business plan designed to make its encryption products recoverable by the end of 1998, and subject to review every six months); and key recovery encryption software of any length. "Recovery encryption software" means those encryption software products designed with a key that converts the encoded data into plain text. The keys must meet certain technical requirements, and be held by a key recovery agent acceptable to the BEA. This agent, whether internal or external to the customer, would be subject to disclosure, certification and record keeping requirements, and would be required to turn the key over to the authorities upon presentation of a proper court order. If the item to be exported does not fall within one of the three License Exception categories, exporters must apply for export licenses, to be reviewed by Commerce on a case-by-case basis.³⁰ More relaxation is proposed, but restrictions remain, and litigation is pending concerning them.²⁸ Legality aside, there is some doubt that healthcare professionals are willing at present to employ a technology that is intended, after all, to diminish access to information.²

Data Compression

Telemedicine may, and generally will, require management of copious quantities of data. "For example, pulse oximeters report with every heartbeat the concentration of dissolved gases in the blood. Transferring this oxygenation data directly into the record would generate about 1.5 million bytes of information per day per patient—equiva-

lent to about 400 pages of numbers—and the majority of the data would never be accessed again.”² Visual data, whether high resolution still images or motion video, require a much larger spectrum than voice.²

Without data compression, dealing with all this information could overwhelm the capacity of the computers integral to telemedicine.² “Compression of computer files is the action of making the file take up less memory or storage space. There are various techniques for doing this, but essentially they all work by finding and shortening up redundancies in . . . [the] file (such as finding repeated sequences of characters and using a short code for this sequence instead of the full sequence).”³¹ This reduces the overall stream of data transmitted and makes it more manageable. It also saves storage space, transmission time, and cost. Some assert, however, that as compression ratios increase, the risk of image degradation may also increase.²

There are two types of image compression methodologies. Both rely on compression algorithms, some of which are proprietary. The first category is “lossless,” a reversible method that loses none of the image’s original quality (hence its name). Lossless compression of medical images is generally limited to a maximum data compression ratio of about 3 or 4:1. A 3:1 compressed image can be transmitted in one-third the time required to send the same uncompressed image, and will require about one-third the memory to store. It can also be retrieved from memory in less time.³² The other major type of compression is termed “lossy” because some of the image quality is sacrificed to make the electronic format smaller. Lossy compression attempts to identify, and then discards, information not normally visible in the human visual system; it is capable of compression of 20:1 or greater. Some argue that significant compression can be achieved only with lossy algorithms.³³ Original pixel values of a location inside a compressed region, however, cannot be recovered. On the other hand, although an original radiograph and a compressed radiograph are “virtually indistinguishable, . . . subtracting one image from the other (and enhancing the contrast with the result) reveals the information that was lost in the compression.”² Lossy compression algorithms can achieve much higher compression ratios, but some claim that there may be trade-offs in image quality, such as diminished spatial resolution.^{2,4}

The extent to which image quality could deterio-

rate may differ with the type of study involved. Musculoskeletal films seem to be more susceptible to compression than are chest radiographs, for example. Aberle et al argue that accuracy in interpretation of chest films is not harmed by compression.³⁴ Yoshino and colleagues assert that accuracy in reading cervical spine films is poorer when such films are transmitted than when they are read conventionally.³⁵ The subtlety of the pathology may make a difference; in Kondoh’s study, eleven radiologists detected significantly less disease in computed radiography images than in conventional radiographs.³⁶ One could argue on this basis that findings such as subperiosteal bone resorption might be missed because of compression. Moreover, compression may be more difficult in studies with less pixel-to-pixel correlation such as CT and MRI. Rinde and associates suggest broadly that teleradiology may not be able to achieve quite the same level of reliability as in-person viewing of radiographs.³⁷ The radiology community has warned against “significant loss of spatial or contrast resolution from image acquisition through transmission to final image display” where “a teleradiology system is used to produce the official authenticated written interpretation” of a diagnostic imaging study.³⁸ Moreover, not all methods of compression of a given ratio necessarily produce equivalent images; therefore, the use of different methods of compression may create image compatibility problems.³² Research currently under way is intended to identify the image resolution needed for clinical problems.³⁹

Artificial Intelligence

The National Library of Medicine divides telemedicine into three areas: (1) aids to decision-making, (2) remote sensing (transmittal of data and educational materials between sites), and (3) collaborative arrangements for real-time management of patients at a distance.⁴⁰ Among the “aids to decision making” is artificial intelligence (AI). Students of this subject split AI into “two different categories: one attempts to shed light on the nature of human intelligence by simulating it or components of it, with the eventual aim of replicating it (or even surpassing it); the other attempts to build expert systems that exhibit intelligent behavior regardless of their resemblances to human intelligence.”⁴¹

An expert (or “knowledge-based”) system can “ask questions, discard irrelevant information, and

produce both a reasoned conclusion and a credible explanation of how that conclusion was obtained."⁴² Advocates say that an expert system is "able to solve problems in its particular area of expertise at a level of skill approaching that of a human expert."⁴³ At present, however, an expert system generally cannot recognize the fact that a problem it is asked to solve has exceeded its area of expertise.⁴⁴ Critics of expert systems are skeptical about how nimble such systems can be in dealing with the vicissitudes of healthcare.⁴⁵ The Public Health Service's Agency for Health Care Policy & Research (AHCPR), in an interagency agreement with the National Library of Medicine, is funding a study on computerized drug monitoring systems and design and implementation of a drug alert notification subsystem for use in different clinical settings.⁴⁶ At a cost of \$4.55 million, AHCPR is also funding a three-year study of the value of computerized decision-support systems in five projects: post-transplant care, family linkages supporting hyperbilirubin guidelines, depression care, childhood preventive care, and interactive guidelines-based decision support on the world wide web.⁴⁷

There are several artificial intelligence systems already in use in health care today. Mycin, for example, is an expert algorithmic system used to assist in management of infectious disease.⁴¹ Acute Physiology and Chronic Health Evaluation (APACHE) III helps to manage intensive care unit (ICU) patients.⁴¹ Inputting 27 factors per patient per day, the system claims 95% accuracy in predicting chances of death.⁴⁸ Computers and software programs are also used to assist in calculating doses of radiation for patients with prostatic carcinoma,⁴⁹ and to generate warning labels for prescription drugs.⁵⁰ The National Aeronautics and Space Administration (NASA) is seeking to transfer a device called a general image pattern classifier to the private sector for telemedicine applications. Initially designed to permit retrieval of images from large image collections when the images themselves had been but sparsely described, the technology has been used to categorize slides of white blood cells into two distinct groups using the stored judgments of a practicing pathologist.⁵¹

TeleMed, a joint project of the National Jewish Center for Immunology and Respiratory Medicine and Los Alamos National Laboratory, provides, among other things, automated data analysis of radiographic images.

This tool provides the physician with an *agent* who browses radiographic data and calls the physician's attention to suspect areas. One typical agent can analyze CT images from patients with lymphangioleiomyomatosis (LAM) disease . . . A pulmonary CT study reveals a primary signature of the disease, namely the presence of many cysts throughout the lungs. LANL's Computer Research and Applications Group has created algorithms that automatically locate the cysts in the pulmonary CT data and record their size. One can compute a histogram of the cyst sizes, which is called a cystogram. The cystogram provides a meaningful quantitative measure of the progress of a disease.⁵²

Another application is the recognition of cardiac dysrhythmias.

Electrocardiogram monitors, for instance, often average the shape of a patient's ECG trace for about 20 heartbeats to build a profile of a 'normal trace'. Subsequent traces are then compared to the normal trace; if they differ significantly, they are classified as aberrations and an alarm can be passed on to a care giver. Moreover, the aberrant signals can themselves be sorted according to their shapes and a library assembled of arrhythmias specific to the patient. Further traces are then compared to the patient's own customized library of heart problems, and the urgency of an alarm matched to the severity of the abnormality.²

To apply AI in a telemedicine setting, it may be helpful to bear in mind the limitations of the technology. In a study comparing four AI diagnostic systems with each other and with the conclusions of expert physicians, the authors found that the systems provided useful, but potentially misleading, information:

A majority of the diagnoses that the systems listed were correct (or closely related to the correct diagnosis), but the correct diagnosis usually did not appear in the top five diagnoses listed by the systems. Moreover, far less than a majority of the diagnoses they listed were considered relevant. On average, they listed less than half of the diagnoses identified by the expert clinicians, but they listed about two additional irrelevant diagnoses not originally identified by the clinicians.⁵³

Applied to telemedicine, AI could potentially lead to claims of information overload distracting to the clinician, or perhaps be characterized in pleadings as a set of rigid rules trumping physician judgment.² On the other hand, as the technology grows more sophisticated, there is reason to be optimistic that many of these problems can be ameliorated if not solved.

LEGAL IMPLICATIONS

The technical aspects of telemedicine discussed earlier—confidentiality, compression, and artificial

intelligence—are all evolving, as is the technology itself. As they change, and as other features of telemedicine change, the appropriate legal analysis will need to change as well. With technological progress, the ability of telemedicine to withstand attack may improve. At present, however, the risk of exposure to damages claims deserves consideration. Breaches of confidentiality, for example, have the potential to lead to allegations of adverse employment decisions or of damage to interpersonal relations, among other problems. Data compression and artificial intelligence could possibly engender allegations that faulty medical decisions emanated from their use leading to personal injury or death. We turn now to consider the legal framework into which claims might be placed. Many of these are extensions of legal concepts originating in the law of computers, which are cousins, if not sisters, of the devices used in telemedicine.

Contract Claims

Contract claims against software vendors are usually based on the Uniform Commercial Code (UCC).⁵⁴ Plaintiffs suing companies supporting telemedicine could presumably devise theories based on breaches of express warranties, UCC §2-313 (1989), or on breaches of implied warranties of merchantabilities UCC §2-314, perhaps alleging third-party beneficiary status respecting contracts between software companies, for example, and healthcare providers.

Tort

A claim in a telemedicine context could be based on negligence, perhaps in reliance on §552 of the Restatement (Second) of Torts: Information Negligently Supplied for the Guidance of Others:

(1) One who, in the course of his business, profession, or employment . . . supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.

Can a computer manufacturer be held liable based on §552? In defense, it can argue that it sells machines, not information.⁵⁵ A manufacturer of telemedicine devices, such as a digital camera, for example, could offer the same defense, arguing that negligence could not be established by transmis-

sion of inaccurate data where the camera used met industry standards.

One problem with this approach at the moment is that such standards are in many instances just emerging now. One such emerging standard for the transfer of images and other data “between computers and peripheral devices such as printers” is Digital Imaging and Communication in Medicine (DICOM) 3.0, created by the collaborative efforts of the American College of Radiology and the National Electrical Manufacturers Association.⁵⁶ DICOM, which already sets standards for image data files and compression methods in radiology, may be extended to include telepathology.⁵⁷ The American College of Radiology, the “principal organization of radiologists, radiation oncologists, and clinical medical physicists in the United States,” has promulgated standards for teleradiology, which it defines as “the electronic transmission of radiological images from one location to another for the purposes of interpretation and/or consultation.” These standards include provisions for the qualifications of personnel (physician, technologist, physicist), equipment guidelines (specific and general), and provisions for licensing, credentialing, liability, communication, quality control, and quality improvement.³⁸ The American Electroencephalographic Society of Bloomfield, Connecticut has established standards for transmitted electroencephalograms (EEGs).⁵⁸ Other such standards may soon be in place.¹⁹

The closer a manufacturer comes to offering AI, however, the more difficult it may be for the manufacturer to defend itself by arguing that if its product met industry standards it should not be liable. Moreover, the rapidity of evolution of telemedicine technology may present plaintiffs with opportunities to allege that a particular device or system was obsolete at the time of the alleged harm, and that the manufacturer should have updated, or advised purchasers and users to update, its apparatus.

A slightly more sophisticated theory is professional malpractice. Medical malpractice claims could certainly be brought against practitioners using telemedicine systems for adverse outcomes and would presumably proceed along familiar principles. A more novel theory, targeting manufacturers and distributors of the software and possibly the hardware or peripherals, would be “transmission” malpractice, extending the concept of so-called computer malpractice.⁵⁹ Plaintiffs may argue

that, because of the complexity and rapid evolution of the technology, professional judgment, actionable if substandard, is implicated. It may then require no enormous leap to move from computer malpractice to transmission malpractice.

[T]hose responsible for deploying, sustaining and managing information and telecommunications systems and programs face an often confusing array of constantly changing hardware and software options, many of which are not tailored to healthcare users. Assessing the utility of advanced technologies can be difficult particularly given the frequent need to consider options in combination, and not just individually. New systems generally have to be patched together with existing or legacy systems that cannot be immediately replaced.¹⁹

This emphasis on the intricacies of selecting the appropriate technology, and the consequent dependency of the purchaser on the expertise of the vendor, could provide a launching pad for a transmission malpractice claim.

In the confidentiality area, the uncertainty of the law might encourage allegations of malpractice *per se*; that is, malpractice that can be treated as negligence without any proof as to surrounding circumstances, based on claims that the defendant violated an applicable statute or regulation. In the absence of unambiguous law, it may not be difficult to fashion an argument that a breach of confidentiality occurred in violation of such authorities.

Finally, strict liability theories could be asserted, seeking recovery for harm without fault. "Liability" means a condition of being actually or potentially subject to an obligation to perform an act immediately or in the future, such as a duty to pay money or perform some service. Historically, liability in a litigation context arose from a demonstration that the defendant had breached a duty to the plaintiff, and that this breach caused harm to the plaintiff for which the law would require the defendant to pay compensation. In the law of negligence, there could be no recovery no matter what harm had come to the plaintiff, if the defendant had acted reasonably—which in general was ascertained by comparing his conduct with that of others in his field under similar circumstances. Strict liability is a theory originating in the law of products liability; it provides that one who sells a product in defective condition unreasonably dangerous to the consumer is liable for harms caused to that consumer, provided that the defendant is in the business of making or selling such products, and that the product reaches the consumer in a condi-

tion substantially unchanged from that in which it was sold. In strict liability theory, the defendant can be found liable even if his conduct was similar to that of other, reasonably prudent actors within the same field or discipline. One rationale for this approach is that manufacturers and sellers of products are well situated to spread the risks attendant to the use of their products by developing and utilizing a pricing structure that takes such risks into account. A plaintiff seeking to advance a strict liability theory might possibly proceed under §402A of the Restatement (Second) of Torts. This notion may be less farfetched than it seems. First of all, there could be relatively straightforward assertions that in a given case, the image resolution or sound quality, or the speed of the equipment for encoding and delivery, were defective because the machinery used was defective. "Off-the-shelf" software, after all, is often mass-produced. Programs can be owned and ownership can be transferred. In telerradiology, where the best reliability data may exist, improvements in the equipment, especially high-resolution monitors, are said to generate results now comparable to those with conventional image interpretation.⁶⁰ In teledermatology diagnostic inaccuracies could arise if the color of a lesion were inaccurately transmitted.⁶¹ Another example arises in home health, where there have been reports of noise from electrocardiogram (EKG) electrodes, resulting in loss or distortion of monitored EKG signals. This could create false alarms over apparent but imaginary ventricular ectopic beats or asystole.⁶² But claims of defective equipment may not be the only approach.

Providers of services, such as physicians, are generally not subject to strict liability.⁶³ Yet some courts have already imposed strict liability on ideas. One court has held that the publisher of a cookbook failing to state that a given ingredient, raw, was poisonous, can be held strictly liable.⁶⁴ In *Winter v. G.P. Putnam's Sons*,⁶⁵ dicta suggested that software "that fails to yield the result for which it was designed" could be subject to strict liability. A plaintiff might be prepared to argue that cases of this type illustrate that the technology used in support of telemedicine services is a product (or a group of products) and not a service, and so strict liability should apply. Plaintiffs might also attempt to analogize, especially when dealing with AI, from cases holding that for tort liability purposes, navigational charts may be deemed to be products.⁶⁶ Such cases deem aeronautical charts to be analogous to

other navigational devices, such as compasses.⁶⁷ In computer technology, some commentators have already argued for strict liability.⁶⁸ Likewise, some writers have argued for strict liability in the health-care information field.⁶⁹ Manufacturers and providers should gear up for analogous arguments.

DEFENSES

Space does not permit a full exploration of this topic. To each of these attacks, however, there is an answer.

Contract

Healthcare information systems vendors use standardized contracts to “exclude all implied and express warranties in part through the insertion of integration clauses; to disclaim special, indirect, and consequential damages, and to set caps on total liabilities under the contracts.”⁷⁰ Companies providing telemedicine devices and services could and should do the same. They can dispute the applicability of UCC sales provisions on the theory that software is not a “good.”⁷¹ As has long been done in other contexts, they can also negotiate for favorable choice of law provisions.

Tort

Preemption. A “medical device” is “an instrument, apparatus, implement, machine, contrivance . . . or other similar or related article, including any component, part or accessory, which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease. . . .”⁷² As of this writing, the Food and Drug Administration (FDA) has neither approved nor disapproved technology employed in telemedicine practice, but given the breadth of this definition, it is not surprising that the FDA has taken the position that devices or software used in aid of telemedical practice are “devices” within the meaning of the Federal Food, Drug, and Cosmetic Act.²

If the FDA determined that a device used in telemedicine practice is a Class III device,⁷³ and thus a premarket approval (PMA) would be required for it to be marketed, its manufacturer might assert that FDA’s approval of a PMA application insulates the manufacturer from liability.⁷⁴ This is so-called preemption argument. Under *Medtronic, Inc. v. Lohr*,⁷⁵ however, such a defense has become more difficult. *Lohr* interpreted the preemptive effect on Florida state product liability claims

against the manufacturer of a pacemaker and pacemaker leads of the Medical Device Amendments of 1976, 21 USC §§301 *et seq* and, in particular, 21 USC §360k(a). Five Justices joined in a rather fractured opinion that concluded, in part, that design defect claims (sounding in both negligence and strict liability) were not preempted, because the 510(k) procedure under which the device was marketed did not impose any federal “requirement” on the pacemaker that could conflict with common law liability under state law. A 510(k) device, such as the *Lohr* pacemaker, is one judged to be substantially similar to devices already on the market,⁷⁶ not one that had received PMA under 21 USC §§360c(a)(1)(C), 360e. This distinction could permit a company making devices used in telemedicine, if granted PMA, to distinguish *Lohr* and invoke preemption. A similar argument could be made even for a device marketed under 510(k) approval if the device were subjected to investigational device testing, a mechanism that without PMA permits the use of certain investigational products to treat patients with serious disorders for which no satisfactory alternative treatments are currently available so as to permit further assessment of the device’s value.⁷⁷ Given the cost in time and money of obtaining PMA, and the benefits of an available §510(k) route to the market, a PMA may not be a practical option. A more effective argument may be to show that regulations governing the device are sufficiently specific that preemption applies despite *Lohr*.⁷⁸

Strict Liability

Manufacturers should vigorously defend the traditional product/service distinction.⁷⁹ From a policy perspective the nature of computer programming should be recognized as a service: “Software’s complexity makes it virtually impossible to prevent some defects (called ‘bugs’) from showing up in programs, even when the software has been on the market for several years.”⁸⁰ Debugging, in fact, may be the most costly aspect—in both time and dollars—of software development.⁸¹ An argument that may be persuasive here is that telemedicine concerns, like software companies, provide ongoing services, not finished products: “[D]eveloping a computer program is a continuing process, rather than a single act. . . .”⁸² Strict liability is inappropriate for a “product” in continual evolution.⁸³

In their advertising, their contracts, and in court, telemedicine-related companies should stress the

individualistic, customized nature of what they do, and demonstrate that the hardware or the software was made to meet the needs of a particular clinical setting. They should also point out the extent to which the purchaser can and does modify the system further, the comparatively direct and personal relationship they often have with healthcare providers, and the difficulty in their market of spreading risks.

The strongest arguments for denying recovery against manufacturers of products used in telemedicine are probably policy arguments. Telemedicine's potential to expand access to care, and to improve its quality, should be recognized as social benefits of sufficient value to deserve the encouragement of the nation and the protections of its laws. We should not impose liability without fault for the simple reason that telemedicine should be given some reasonable opportunity to prove its worth. Moreover, the ability of many vendors in the field to spread risks is far more limited than that of larger manufacturers, which has traditionally been one of the reasons why strict liability has not been applied to providers of services.⁸⁴

Other Defenses

A reasonable position for a manufacturer to take is that a telemedicine system cannot be subjected to strict liability because it plays a merely consultative role, and does not render final medical judgment.⁸⁵ This is essentially a variant on the learned intermediary principle, under which pharmaceutical houses, for example, may not be liable to a patient for harms caused by their products where the patient was exposed to the product only after a physician (the learned intermediary), educated in the product's benefits, prescribed it for him.⁸⁶

Legislation

Legislation may be needed to provide a legal framework to protect this technology in its infancy from predatory litigation. There is already "significant support" for "some degree of federal action to regularize protections for sensitive medical data . . . although disagreement about the extent of these protections blocked legislation through mid-1996."¹⁹ The preemption issue would appear to be another area where legislative action may be in order to cover areas not addressed in *Lohr*.

CONCLUSION

Telemedicine has the potential to improve the quality of health care around the world, by enormously expanding access. The technology may allow patients with unusual or complex disorders to get the benefit of advice and treatment from the most highly trained specialists at major medical centers far removed from the patient's location. Telemedicine may also afford expanded educational opportunities for medical professionals at all levels. PACS similarly uses technology to handle and deliver medical images and text data more widely and rapidly than heretofore possible. Unfortunately, these technologies face several threats, many of them legal. Among the more obvious are reimbursement and professional liability concerns. Perhaps less obvious, but potentially equally or even more threatening are products liability claims that might be predicated on a variety of theories. The products liability threat may be aggravated by the fact that the current state of the law is unsettled, and variable from one jurisdiction to the next. Another exacerbating factor, as with virtually all other torts, is that under a contingent fee arrangement, plaintiff's counsel are incentivized to invent novel theories of recovery. Although at this writing, to the writer's knowledge, no products claim has been brought in the telemedicine arena, breaches of confidentiality, possible diagnostic errors through data compression, and possible diagnostic or therapeutic errors through the use of artificial intelligence could all potentially give rise to claims. To some extent, suits predicated on these or similar theories can be avoided with careful drafting of contracts and with the continuing progress in the sophistication of the technology. To some extent, defense theories useful in other contexts could be imported into the telemedicine arena to protect against such claims. It is possible, however, that these measures will be insufficient to protect growth and development in the technologies. If so, legislation will be needed to diminish these and other risks so that PACS and telemedicine have the chance to achieve their potential.*

*Note: This paper is condensed from a longer manuscript entitled "Telemedicine: Technology and the Law,"⁸⁷ that is available through the author. The full paper contains detailed citations omitted from this version. These citations permit the interested reader to explore more thoroughly ideas discussed herein and to identify source materials.

ACKNOWLEDGMENTS

The writer wishes to thank Jeffrey P. White, Esquire for providing a critical analysis of early drafts of this paper, his colleagues Clive O'Grady and Cecil Martin for their assistance in preparation

of its "cryptography" section, and his partner Deborah M. Russell, Esquire for her critique of the paper generally and of its preemption section in particular.

REFERENCES

1. Council on Medical Education and the Council on Medical Service of the American Medical Association: Joint Report. Released at the AMA Annual Meeting, Chicago, IL, June 1994
2. Office of Technology Assessment, Congress of the United States: Bringing Healthcare Online: The Role of Information Technologies. OTA-ITC-624, 1995, (GPO Stock No. 052-003-01433-5)
3. Grigsby J, Schlenker R, Kaehny M, et al: Analysis of Expansion of Access to Care Through Use of Telemedicine. Report 4: A Study Summary and Recommendations for Further Research. Denver, CO, Center for Health Policy Research, 1994
4. *Chabra v. Southern Monterey County Memorial Hospital, Inc.*, 1994 (WL 564566)
5. Birz SS, Anderson JS: Is the Computer a Threat to Confidentiality of Psychiatric Records? A Review, Lecture at Proceedings of SCAMC. Presented at Symposium on Computer Applications in Medical Care, November 1-4, 1987. Reprinted in Computer Society of the IEEE Press, 1987.
6. Computer Science and Telecommunications Board: Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. <http://www2.nas.edu/cstbweb/21ba.html> (last updated 11/7/95) at 2, 3
7. Institute of Medicine: The Computer-Based Patient Record: An Essential Technology for Health Care, in Dick R, Steen E (eds): The Computer-Based Patient Record. Washington, DC, National Academy Press, 1991
8. U.S. Congress, Office of Technology Assessment: Protecting Privacy in Computerized Medical Information. 1993
9. Computer Science and Telecommunications Board, National Research Council: For the Record: Protecting Electronic Health Information. Washington, DC, National Academy Press 1997
10. US Government Printing Office: Highway to Health: Transforming U.S. Healthcare in the Information Age. Washington, DC, US Government Printing Office, 1996
11. Public L No. 93-579, 88 Stat. 1986 (codified as amended at 5 USC § 552a)
12. 5 USC § 552a(b)
13. *Winters v. Board of County Commissioners*, 4 F 3d 848 (10th Cir 1993), *cert denied*, 511 US 1031 (1994)
14. *Krebbs v. Rutgers*, 797 F Supp 1246 (D NJ 1992)
15. *Gilbreath v. Guadalupe Hospital Foundation, Inc.*, 5 F3d 785 (5th Cir 1993)
16. *Dennie v. U. of Pittsburgh School of Med.*, 589 F Supp 348 (D VI 1984), *aff'd*, 770 F 2d 1068, *cert denied*, 474 US 849 (1985)
17. *Unt v. Aerospace Corp.*, 765 F 2d 1440 (9th Cir 1985)
18. 42 USC §§ 122101-122213, Pub. L No. 101-336, 104 Stat. 327 (1990)
19. Field MJ (ed), Institute of Medicine: Telemedicine: A Guide to Assessing Telecommunications in Health Care. Washington, DC, National Academy Press, 1996
20. S 1360 104th Cong., 1st Sess. (1995)
21. HR 435 104th Cong., 1st Sess. (1995)
22. HR 3482 104th Cong., 2d Sess. (1996)
23. §§ 1-101 to 9-106, 9 ULA 479-529 (1988)
24. § 1-101, 9 ULA 479
25. Federal Privacy of Medical Information Act, HR 5935, 96th Cong. 1st Sess. (1979) and 2d Sess. (1980)
26. HR (3103) Pub. L No. 104-191, 110 Stat 1936
27. Schwartz J: Health Insurance Reform Bill May Undermine Privacy of Patients' Records. A23: Washington Post (August 4), 1996
28. *Bernstein v. United States Department of State*, 945 F Supp 1279, 1282 (ND Cal 1996)
29. 22 CFR § 121.1, XIII(b)(1)
30. 22 CFR, Subchapter M, §§ 120-130 (1994)
31. Backup Vault Inc: "Backup Vault Glossary." 1996. <http://backupvault.com/bvglos.htm>
32. American College of Radiology, Committee on Research and Technology Assessment of the Physics and Radiation Protection Commission: A Guide to Teleradiology Systems. Richmond, VA, ACR, 1993
33. Cosman, et al: Evaluating Quality of Compressed Medical Images: SNR, Subjective Rating and Diagnostic Accuracy. Proceedings of the IEEE: 919-932, 1994
34. Aberle, et al. The effect of irreversible image compression on diagnostic accuracy of thoracic imaging. *Invest Radiol* 28:398, 1993
35. Yoshino, et al: Diagnostic performance of teleradiology in cervical spine fracture detection. *Invest Radiol* 27:55, 1992
36. Kondoh, et al: A comparison of conventional film screen radiography and hard copy of computed radiography in full and two-thirds sizes in detection of interstitial lung disease. *J Digit Imaging* 7:193, 1994
37. Rinde, et al: Telemedicine in Rural Norway. *World Health Forum*: 14 71-77, 1993
38. American College of Radiology: ACR Standard of Teleradiology, Res. 21-1994. Standards 27, 1995
39. Perednia, et al: Comparison of the clinical informativeness of photographs and digital imaging media with multiple-choice receiver operating characteristic analysis. *Arch Dermatol* 131:292-297, 1995
40. Scannel KM, et al: Telemedicine: Past, Present, Future. Bethesda, MD, National Library of Medicine, 1995
41. Forester T, Morrison P: Computer Ethics: Cautionary tales and ethical dilemmas in computing. (2nd ed). Cambridge MA, MIT Press. 1994 p 164
42. Gill CJ: Medical Expert Systems: Grappling with Issues of Liability. *High Tech Law Journal* 1:483-484, 1986
43. Edmunds, RA: The Prentice Hall Guide to Expert Systems. Englewood Cliffs, NJ, 1988, p 28
44. Waterman, DA: A Guide to Expert Systems. Menlo Park, CA, Addison-Wesley, 1985, pp 12-13
45. Shortliffe, EH: Computer Programs to Support Clinical Decision Making. *JAMA* 258:61, 1987
46. Computerized Studies for Clinical Decisionmaking. *AH-CPR Research Activities* 200:18-19, 1997

47. Projects look at value of decision support software. *Am Med News* 40(2):23, 1997
48. Schwartz EI, Treece JB: Smart Programs Go to Work. *Business Week* (March 2):97-99, 1992
49. *Jones v. Minnesota Mining & Manufacturing Co.*, 669 P 2d 744 (NM App 1983)
50. *Frye v. Medicare Glaser Corp.*, 219 Ill App 3d 931, 579 NE 2d 1255 (1991)
51. BRS Software Products. <http://iridium.nttc.ed...p/GLD5/telemedicine+/2>
52. TeleMed: A Joint Project of National Jewish Center for Immunology & Respiratory Medicine & Los Alamos National Laboratory. <http://www.acl.lanl.gov/sunrise/Medical/telem.html> (last updated 1/25/96)
53. Berner et al: Performance of Four Computer-Based Diagnostic Systems. *New Engl J Med* 330:1792, 1994
54. Horovits BL: Computer Software as a Good Under the U.C.C.: Taking a Byte Out of the Intangibility Myth. *Boston University Law Review* 65:129, 1985 (note)
55. *Black, Jackson and Simmons Ins. Brokerage, Inc. v. IBM*, 109 Ill App3d 132, 440 NE 2d 282 (1982)
56. Swartz D: Introducing DICOM 3.0. A Standard for Medical Imaging. *5 Telemedicine Today* 5:24, 1997
57. Weinberg DS: How is telepathology being used to improve patient care? *Clin Chem* 42:831-835, 1996
58. Pendrak RF, Ericson RP: Telemedicine May Spawn Long Distance Lawsuits. *National Underwriter* (November 4):44-45, 1996
59. Gaziano SG: Computer Malpractice—A New Tort on the Horizon? *Rutgers Computer and Tech Law Journal* 17:177, 1991
60. Gitlin JN: Understanding Teleradiology. Harrisburg, PA, Society for Computer Applications in Radiology, 1994 (intro)
61. Dunn et al: An Evaluation of Four Telemedicine Systems for Primary Care. *Health Care Services Research* 12:19, 1977
62. Zhang Y, et al: First Trial of Home EKG and Blood Pressure Telemonitoring System in Macau. *Telem J* 3:67-72, 1997
63. *Porter v. Rosenberg*, 650 So. 2d 79 (Fla App, 1995)
64. *Cardozo v. True*, 342 So 2d 1053 (Fla App), *cert denied*, 353 So 2d 674 (Fla 1977)
65. 938 F 2d 1033 (9th Cir 1991)
66. *Aetna Casualty & Security Co. v. Jeppesen & Co.*, 642 F 2d 339 (9th Cir 1981).
67. The American Law Institute: Restatement of the Law Third, in Restatement of Law, Torts: Product Liability, Tentative Draft No. 2, Section 4, Product Defectiveness. pp 154-156, 168, 169. (March 13, 1995)
68. Godes JN: Developing a New Set of Liability Rules for a New Generation of Technology: Assessing Liability for Computer-Related Injuries in the Health Care Field. *Computer Law J.* 7:517, 1987
69. Dahm LL: An Innovative Theory of Recovery for Patients Injured Through Use or Misuse of Health Care Information Systems. *J. Marshall J Computer and Info L* 14:73-79, 1995 [citing Restatement (2d) of Torts, Section 402 A (1965)]
70. Schleifer LA: Damage Awards and Computer Systems—Trends. *Emory LJ* 35:255-259, 1986
71. *Triangle Underwriters, Inc. v. Honeywell, Inc.*, 604 F 2d 737 (2d Cir 1979).
72. Federal Food and Cosmetic Act, 21 USC § 321 (h).
73. 21 USC § 360c(a).
74. 21 USC § 360k(a).
75. 116 S Ct 2240, 135 L Ed 20 700 (1996).
76. 21 USC § 360(h) and 21 CFR § 807.81(a).
77. 21 USC § 306j(g); 21 CFR §§ 812 and 813, particularly 812.1(a).
78. *Berish v. Richards Medical Co.*, 937 F Supp 181, 185 (ND NY 1976).
79. *Birmingham v. Fodor's Travel Publications, Inc.*, 833 P 2d 70 (Hawaii 1992).
80. Davis GG: Special Problems Involving Software Warranties and Indemnities for Mass-Distributed Software. Practising Law Institute/Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series 191:597-604, 1984
81. Gemignani MC: Product Liability and Software. *Rutgers Computer and Tech LJ* 8:173, 1981
82. Brannigan VM, Dayhoff RE: Liability for Personal Injuries Caused by Defective Medical Computer Programs. *Am J Law Med* 7:123-126, 1981
83. Freed RN: Products Liability in the Computer Age. *Forum* 12:461, 1977
84. Maule MR: Applying Strict Products Liability to Computer Software. *Tulsa LJ* 27:735-751, 1992 (comment)
85. Cole GS: Tort Liability for Artificial Intelligence and Expert Systems. *Computer LJ* 10:127-162, 1990
86. *Abbot v. American Cyanamid Co.*, 844 F 2d 1108 (4th Cir 1988).
87. McMEnamin, Joseph P., "Telemedicine: Technology and the Law." For the Defense (July), 1997