

TELEHEALTH: RISK MANAGEMENT IN THE RE-TOOLING OF HEALTHCARE

by Marlene M. Maheu, PhD

This article is an attempt to outline a conservative, yet proactive, approach to risk management in healthcare delivery through telehealth. Although many of us do not feel prepared to make decisions regarding risk management without more information, the developers of technology march on – faster than we can adapt. In many cases, we clearly need to move ahead and adopt some technology, despite a limited amount of information regarding the full impact of technological change. This is the dilemma: either we become part of the development of these new systems, tools, protocols and guidelines for their use – or others will do it for us. Meanwhile, our risk only increases because we are on new terrain. As Cepelewicz states when discussing telehealth liability, “it’s only a matter of time before we see a dramatic increase in the number of malpractice cases” (1998, p. 3).

Telehealth practice complicates issues of risk management for several reasons. First, the practitioner–patient relationship with various patient populations in face-to-face consultation is now potentially further complicated by communication technology. Research regarding the ways in which such technology either alters or maintains existing relationship elements is just beginning to emerge in the literature (O’Conaill and Whittaker 1997; Whittaker and O’Conaill 1997). Therefore, by potentially adding emotional as well as physical distance between practitioner and patient, technology not only raises questions due to change of service delivery system, but may actually alter currently unidentified or defined elements of that

essential relationship. Thus, transmitting healthcare through technology increases the risk of lawsuit.

Secondly, since the professional relationship with patients via technology has not been well defined, courts and ethics boards will probably render their determinations when challenged by examining existing case law and ethics codes. They are also likely to use traditional perspectives and consultants to more clearly define whether a professional relationship exists in each of the variety of new circumstances created by technology, e.g., email, chat rooms, and videoconferencing using Internet or ISDN lines. This practice could be problematic owing to the shift in power between practitioners using traditional and technical approaches to service delivery.

Given the unprecedented rate at which technology is being developed and used to deliver healthcare, and the increased readiness with which younger generations are adopting technology, the time-worn mentor–mentee relationship model of training and decision-making in healthcare may pose problems. Senior administrators and clinicians with superior expertise in ethics and practice may lack technical expertise or perspective. Similarly, junior administrators and clinicians with superior expertise in technology may lack a seasoned perspective in working with patients. Attempts at bridging this generation gap could be augmented in both directions when the parties are overly enthusiastic about their respective positions. In the courtroom, similar generational problems may appear, thereby rendering legal and

risk management decisions more difficult to predict.

Third, the respective and joint liability of referring practitioners and consulting practitioners is even more ambiguous. The definition of negligence with respect to either or both types of practitioners is unclear. These roles and definitions are likely to undergo a similar process of examining existing case law and ethics codes in the courts and before ethical boards.

Fourth, jurisdiction as defined by various state laws is unclear, as are the state licensing boards about how new laws ought to be worded. As it stands, telehealth consultants could be subject to the jurisdiction of the state where they reside, every state where they practice and the state where the patient resides. One thing is clear, however: to initiate any malpractice lawsuits, plaintiffs must substantiate that there was a patient–professional relationship, that the consultant somehow breached the applicable standard of care and that this breach caused an injury (Cepelewicz 1998). The respective liabilities of institutions housing such services are also ambiguous.

A careful look at the literature shows a number of substantial documents outlining laws, standards and guidelines, and research comparing essential elements of responsible and reasonable practice. Following is a checklist of risk management practices drawn from many summary articles describing existing programs. Please adapt recommendations to your circumstance, and discuss with ethical, legal and insurance counsel if questions arise.

Recommendations

1. Obtain copies of, read carefully and understand your state laws regarding telehealth liability. Subscribe to publications to keep yourself current on these and other laws passed in your state.
2. Weigh the advantages and disadvantages of becoming licensed and credentialed in all states for which you intend to provide telehealth services.
3. Obtain professional liability insurance coverage for the specific duties you are performing in telehealth; understand the limits of your liability for telehealth practice, and obtain the details of coverage as well as limits of your liability for telehealth practice from your specific carrier. Obtain a written agreement from your carrier regarding its coverage of your specific program and its specific services. Do not settle for written agreements or form letters that don't specify your program and its services.
4. Be aware of the accepted standard of care for telehealth service delivery in your particular field, if one exists. This can differ from community to community as well as from state to state. For example, delivering care to remote areas may incur an obligation to be aware of norms and customs of peoples treated. However, use of the Internet could result in allegations related to a slow rate of transmission or unreliable information. Be informed regarding expectations of populations served, as well as local events, such as floods or other natural disasters, wars and catastrophes. Some of your best sources for such definitions of expectation are your state licensing board, ethics boards of local chapters of your professional organizations, and peers that you may formally consult in your community.
5. Provide patients with written lists of alternatives and behavioural suggestions in the case of equipment failure, accident or catastrophe. Obtain human-subjects committee approval prior to delivering formal experimental services, obtain proper release forms from subjects and provide debriefing for all patients participating in research.
6. When delivering innovative service in an area where validated research has not yet been established, fully inform all clients both verbally and in writing of such practices as being outside the standard, and in any area not yet validated by research. In the consent form, include issues such as advantages and limitations of telehealth service delivery, including inherent deficiencies in the electronic equipment possibly interfering with diagnosis or treatment; issues related to equipment failure; choice of venue waivers to resolve issues of jurisdiction; a brief description of equipment and services to be delivered; and the purpose, benefits, potential risks and other consequences of services delivered. Describe the specific roles of the consultant and local referring practitioner, indicate which one has ultimate authority over the patient's treatment and state that the information will be stored in a computerized database. Be sure to inform patients of practitioner licensure, and provide state licensing board contact information. Collect patient satisfaction measures regularly throughout service delivery. Arrange for proper scanning and sharing of release forms signed by patients so that local practitioners, remote consultants and patients themselves can have copies for their files.
7. Document and record the patient's history, precipitating events to seeking treatment, socio-cultural contexts, previous assessments, diagnosis, treatments, consultations and recommendations. Photos or snippets of videotaped consultations might be collected to supplement the medical record and provide evidence that treatment is consistent with the standard of care. When dealing with children, understand that videotaped and photographic records are more sensitive and can be highly controversial. For these reasons, some organizations choose to keep only minimal electronic video and photographic records for children.
8. Be certain that your staff is following whatever standards of care might exist in telehealth for your program specialty area. Check with your professional associations for their statements regarding telehealth practice, research or education.
9. Attend and document all continuing education classes taken in telehealth, including legal and ethical practice workshops.
10. Document the role of your organization and practitioners in relation to that standard of care for all diagnostics and treatment delivered to patients – i.e., use encryption for email exchanges to protect confidentiality during transmission; learn about other breaches of confidentiality and security; learn about storage and retrieval procedures for audio and video records; understand and adhere to appropriate supervision protocols.
11. Write to your local, state and national professional association ethics and licensing boards to request approval of your program(s). Provide as much detail as possible in your description of recruitment strategies for obtaining referrals; consent forms to be signed by patients and their families; services delivered, including assessment protocols; medical records, including their storage and retrieval procedures; and termination and case disposition protocols. Even if such ethical boards respond by saying they can't render a decision owing to vagueness in your profession's ethics code, you will have documented your attempt to seek the guidance of your peers.
12. Seek consultation from leaders in the telehealth community and document details of such consultation,

including dates, topics discussed, suggestions made and your rationale for decisions regarding whether or not to follow obtained suggestions.

13. Develop transmission verification procedures for both local and remote transmission sites. In medical records transmission, for example, procedures are needed to confirm the receipt of the data, check for errors, and certify that the images are appropriate for diagnosis. Use actual data as a reference for transmitted data, e.g., actual images compared to transmitted images and data.
14. Engage information systems staff to provide information regarding questions related to the technology you are using – i.e., be aware of the degree of distortion in transmitted images, and the chances of security leaks when using your particular type and brand of telehealth technology (email, chat rooms, electronic medical record transmissions, videoconferencing).
15. Train staff regarding the importance of patient confidentiality, equipment failure backup procedures and security threats for medical record keeping. For example, consider using biometric devices to control access to records. These currently include mapping the pattern of blood vessels in the retina, fingerprints and voice recognition. Regulations by the US Food and Drug Administration permit the use of electronic signatures based on biometrics or a combination of identification code and password.
16. Take measures to ensure that your staff is dealing with the person with whom they think they are dealing by using code words and/or passwords to reduce risk of imposters and underage clients. Verify identity of the parent when working with a minor.
17. Develop staff procedures that involve a separation of duties. Assign checks and balances within a system to limit the impact of a single user. Give staff

members the least amount of access to information needed for them to accomplish their duties. For example, use read-only access to data files so that files cannot be manipulated. Have documentation procedures clearly defined, i.e., intake forms, releases, case notes, email exchanges, and selected audio and video footage go into the patient's medical records.

18. Document the equipment being used, its owners and parties responsible for equipment maintenance; the format for transmitting the medical information; what transmissions are to be interpreted by whom; hours of staff availability and procedures for setting appointments; frequency and format of reports; quality assurance mechanisms desired; and important staffing issues.
19. Invest in well-designed systems that offer the greatest security with respect to cost, prevention and deterrence of privacy abuses. Security measures that go beyond needed levels can be unduly expensive, delay information access and make access inconvenient. Computers can be built and programmed from the beginning to offer greater security so that they disclose only necessary information.
20. Fully investigate the vendors from which you purchase hardware and software. Pay particular attention to equipment maintenance and support programs. Seek references before investing in such products and services. Determine whether or not they have product liability insurance to cover suits from disgruntled patients seeking recourse for faulty hardware, software or support services. Seek vendors willing and able to provide
 - support 24/7 to train new staff and patients, as well as avoid errors leading to data destruction;
 - downtime instructions for accessing emergency information during scheduled and unscheduled down times;

- contracts that detail specific protections and maintenance services to be implemented;
- clear documentation for regular maintenance requirements, procedures and logs to record such maintenance;
- backup systems, such as an alternative equipment, power sources and off-line data storage; and
- documentation of disaster recovery protocols.

21. Above all, our professional responsibility towards patients must be tantamount. Furthermore, active involvement of the patient must be at the forefront of our thinking.

References

- Cepelewicz, B.B., L.J. Dunn Jr, D.M. Felch, L.J. Levin, B.C. Nelson, I.S. Rothschild, M.E. Rust and M.J. Zaremski. 1998. "Recent Developments in Medicine and Law." *Tort Insurance Law Journal* 33(2):583–603.
- O'Conaill, B. and S. Whittaker. 1997. "Characterizing, Predicting, and Measuring Video-Mediated Communication: A Conversational Approach." In K.E. Finn, A.J. Sellen and S.B. Wilbur (Eds.), *Video-Mediated Communication* (pp. 107–131). Hillsdale, NJ: Lawrence Erlbaum Associates.
- Whittaker, S. and B. O'Conaill. 1997. "The Role of Vision in Face-to-Face and mediated communication." In K.E. Finn, A.J. Sellen and S.B. Wilbur (Eds.), *Video-Mediated Communication* (pp. 23–49). Hillsdale, NJ: Lawrence Erlbaum Associates.
-
- Dr. Maheu is a licensed psychologist in San Diego. She speaks internationally and is an established author. Her previous books are *E-Health, Telehealth & Telemedicine: A Guide to Startup and Success* and *Infidelity on the Internet*. Her next book, *The Mental Health Professional and the New Technologies: A Handbook for Practice Today*, is to be released by Lawrence Erlbaum Associates, Inc. in May 2004.