## Chapter 14: Electronic Considerations

1) Overview
    a. Electronic communication with clients
    b. New social media
    c. Recording conversations
    d. Recording others/electronic snooping: Concerns re unauthorized access to other's email/computer
2) Statutes
3) Cases
4) Professional ethics

### Overview

Most ethical and legal guidelines were created in a time when face-to-face, mail or a telephone call were the only ways to communicate. Email, video conferencing (e.g., Skype, FaceTime) are newer methods for connecting the professional and individuals. Also, the "new social media", which includes websites or applications, exist to connect members socially. Facebook, Twitter, LinkedIn, Google+, Pinterest, Tumblr, Flickr, and Instagram and are a few of the prominent sites/applications. The statutory law and case law on these electronic avenues of communication between a mental health professional and their client are non-existent or in their infancy of development. While new social media certainly poses an opportunity for inexpensive advertising unheard of for previous generations, the opportunities for danger abound. This chapter addresses email, video conferencing, social media sites and considerations in recording conversations. Chapter highlights:

1) The possibility of unintentionally waiving privilege by the communication of privileged information to third parties.
2) To be privileged, the communication must be expected to be private.
3) Employer email accounts have no expectation of privacy.
4) If client-therapist information is waived in one setting, it will be waived in all.
5) There is no expectation of privacy in posting to social media sites; this is true if either the therapist or client makes the posting.
6) It is illegal to intercept electronic communication (e.g., phone conversations, email) without consent. There are criminal and substantial civil penalties for violating this.
7) It is illegal to video record others where there is an expectation of privacy.
8) It is legal to record your own conversation with anyone personally (not on phone) without their permission. Some states require both parties of a phone conversation to given consent to record. Tennessee requires that one party given consent.
9) A parent can give consent on their minor child's benefit to record conversations between the minor and others.
10) If a client posts a negative review about you online, ignore it. Any attempt to refute, oppose will likely be a breach of confidentiality.
11) Professional rules about tele-counseling are beginning to emerge.

**Electronic Communication with Clients**

Email communication with clients are problematic in that general email is not secure, if the client accesses email through an employer email system, there is no expectation of privacy and the asynchronous aspect of email robs both the client and the therapist of normal visual information that face-to-face communication provides. Despite wiretapping laws, email accounts and communication are subject to hacking by third parties including family members.

Generally communication with clients electronically shares the same characteristics as communication face-to-face. That is, there is an expectation of privacy, a privilege exists and the therapist must protect confidentiality of the communication. This is true if the communication is merely communication versus conducting therapy via electronic means. When initiating non-face-to-face contact with a client, a therapist should familiarize themselves to several published guidelines: 1) APA Ethics Committee 1997 Statement on Services by Telephone, Teleconferencing, and Internet; 2) American Psychological Association "Ethical principles of psychologists and code of conduct", *American Psychologist*, 57(12), 1060-1073; 3) American Counseling Association (1999) ACA Code of Ethics; 4) American Mental Health Counselors Association "Code of Ethics of the American Mental Health Counselors Association, Principle 14, Internet on-Line counseling"; 5) American Telemedicine Association (2009) "Practice Guidelines for Videoconferencing-Based Telemental health"; 6) eRisk Working Group for Healthcare (2002) "Guidelines for Online Communication".

The issues raised include:

Security

1. Clients are informed about technology limitations and impact on confidentiality.
2. Services provided on secure website using encryption technology.
3. Authentication of communications to assure that the therapist is communicating with the client and not someone posing as the client.

Disability

4. Technology is barrier free for clients with disabilities

Informed Consent

5. Information about the risks of electronic communication is given
6. Client notified if they need encryption technology, and if therapist will provide it.
7. Client is informed and consents if communication is stored.
8. Client is informed about the possible misunderstandings when visual cues are absent.
9. Client is informed about possible technological/communication delays.

Other

10. Other methods of contacting client are obtained.
11. Therapist is aware of resources local to client to address emergency situations.
12. Record of electronic communication are made apart of medical records.
13. Client is informed of alternative treatment should electronic not be appropriate.
14. Services are not performed where client resides in a state in which the therapist is not licensed.
15. The appropriateness of this method of treatment fits both client and therapist.

If a client of yours that resides in your state moves to a different state that you are not licensed in, you cannot treat them via electronic means as a way to bypass getting licensed in that state.

It would be permissible to treat someone on vacation that is domiciled in your state. Some therapists offer psycho-educational workshops for the public. That is a legitimate undertaking. A therapist can offer a workshop even to out of state participants, but must be careful to not allow individualized exchange that leaves the normal public question and answer format and transition to a private discourse that is therapeutic in nature.

**New Social Media**

Social media sites offer individuals many ways to communicate socially. Three ethical issues arise; 1) if the client or therapist posts confidential information on a social media website, they are waiving privilege; 2) if a client posts negative information about a therapist on a social media website, how can/should the therapist respond; and 3) if a therapist has a social media page, how should they respond to client contact. To address the first issue we must first discuss privilege. Most of the privilege statutes for therapists as discussed in chapter five are likened to that between an attorney and client. Let's look at that privilege. TCA §23-3-105 states,

> *No attorney, solicitor or counselor shall be permitted, in giving testimony against a client, or person who consulted the attorney, solicitor or counselor professionally, to disclose any communication made to the attorney, solicitor or counselor as such by such person, during the pendency of the suit, before or afterwards, to the person's injury.*

Case law has demonstrated that the privilege is not absolute. *Humphreys, Hutcheson & Moseley v. Donovan*, 568 F. Supp. 161, 175 (MD. Tenn. 1983) in construing the statute ruled that:

(1) the asserted holder of the privilege is or sought to become a client;
(2) the person to whom the communication was made
    (a) is a member of the bar of a court, or his subordinate and
    (b) in connection with this communication is acting as a lawyer,
(3) the communication relates to a fact of which the attorney was informed
    (a) by his client
    (b) without the presence of strangers
    (c) for the purpose of securing primarily either
        (i) an opinion on law or
        (ii) legal services or
        (iii) assistance in some legal proceeding, and not
    (d) for the purpose of committing a crime or tort and
(4) the privilege has been
    (a) claimed and
    (b) ***not waived by the client***.

Waiver of the privilege can be intentional (when a client signs a release of information) or unintentional. Unintentional waiving of a privilege includes communicating the substance of the privileged communication to a person with whom the confidential relationship does not exist. In email this can occur by forwarding the email to someone other than the client. Also, using an employer email system, where there is not an expectation of privacy, waives the privilege. A single waiver of the attorney-client privilege can have dramatic effects that must be considered before deciding whether to voluntarily waive the privilege. Clients should be made aware in the Informed Consent they are provided, that their posting private information about therapy on a public forum can waive privilege on their part.

If a client posts negative information about a therapist on a social media site, how should a therapist respond? Some call this being "Yelped" from the website www.yelp.com where reviews can be posted about a professional. By fighting back, posting a response, the therapist would be acknowledging the therapeutic relationship. Any public response certainly risks breaching our primary responsibility of confidentiality. Just because the client breaches some of the confidential information, the therapist has not been given consent to do the same. Most therapists writing about this scenario suggest doing nothing in response. What a therapist can do is to avail themselves to publish positive online articles to combat any negative perceptions that may occur due to the negative post. Companies like www.reputation.com basically help you post sufficient articles so as to push down the negative information when doing internet searches. What you can't do is log in and make a fake post (deceptive advertising), ask clients to sign a statement agreeing not to post negative reviews (not enforceable), or ask the website to remove the post (won't do without a court order). Another legitimate approach is to contact the client privately and offer to resolve the conflict with them. Suing the client for slander is not only costly but not likely to succeed and more likely to involve breaching confidentiality.

The third issue asks how a therapist should handle having a social media presence. There two possible social media presences; the first is that the therapist has a professional page on social media, for example, a Facebook page for their practice, and second, to have a personal "social" page. For a professional page the site would be public and there would have to be settings so that posts could not be made to the site. Settings on Facebook that make it a professional site include strict filtering of messages to inbox, only friends of friends can send friend requests, No "friending" of any third parties. By having no friends and only allowing friends of friends sending you a friend request, then no client will be able to send you a friend request. Your posts would just be professional posts, psychoeducational in nature. The therapist having a social page is potentially problematic. By allowing a client to see your personal life via Facebook, can be construed as the therapist establishing a dual relationship (therapeutic and social). Certainly friending a client does create a social relationship. By the therapist limiting viewing to only friends, and accepting only friends of friends as "friend requests" you have limited clients from accessing your personal life and perhaps misconstruing this as an invitation for a dual relationship. Here the only problem you will have if a friend seeks out you as a therapist. This situation is not any different than when a non-Facebook friend seeks you out as a therapist. Also you may have at times a client who is a Facebook friend of one of your friends. You would have to decline/ignore their request to friend you via Facebook. I recommend you include in your informed consent the fact that you will not accept any social media requests for communication or friending by clients. This will ease the fact that you later refuse their friend request. Managing the social media site as a therapist with a social presence is very important in avoiding dual relationships.

**Recording Conversations**

It is legal to record [record, intercept??] a conversation between you and another party in a face-to-face conversation without gathering permission of the other party. Therapeutically most ethical guidelines state that the therapist must get the written consent of the client to record sessions (APA Code 4.03 "Before recording the voices or images of individuals to whom they provide services, psychologists obtain permission from all persons or their legal

representatives"). Regarding telephone recording, Tennessee is a one-party consent state; this means that only one party must consent to recording a conversation on the phone. However, the followings states require both parties to consent to recording a conversation: California, Connecticut, Delaware, Florida, Illinois, Massachusetts, Maryland, Michigan, Montana, New Hampshire, Pennsylvania, and Washington. If you are calling someone who is located in one of those states, you must have both parties permission to record. If the party is a client, recording may be legal but would be a violation of the ethical code unless you had written permission.

At times a therapist is aware that their client is involved in recording a spouse. This occurs to attorneys also, especially in the practice of family law. It is wise to familiarize yourself with the law in this area. It is illegal to record third parties (i.e., you are not on the phone) on a phone conversation or to electronically intercept emails between two other parties without their knowledge and consent (Electronic Communications Privacy Act –ECPA; Tennessee Wiretapping and Electronic Surveillance Act, TCA §39-13-601). Criminal and civil penalties can ensue. There is a Tennessee statute (TCA § 39-13-606) that prohibits putting a tracking device on a motor vehicle without the permission of all the owners. Individuals have an expectation of privacy. Installing video surveillance in one's home may or may not be legal, depending upon where it is placed (not in bedroom or bathroom… place where there is an expectation of privacy).

At times during couples treatment, a party will give consent to their spouse or significant other to see all emails, posts, or computer activity. I would suggest such agreements are made in writing so that there is no confusion later should one party blame the other for wiretapping. Also, realize that any consent may be limited in time or scope. Giving one permission to use your computer to access the internet is not giving permission to access email accounts or to install spyware. Consent, once given, can be revoke. It would be a violation of wiretapping laws to continue to access information that was once allowed but subsequently revoked. If a party has granted permission that they later revoke, they need to document the revocation and particularly that the other party was notified of the revocation. Sending certified mail can document the sending and receipt of a revocation of permission.

**Statutes**

**Licensed Professional Counselors-**TCA 63-22-101 to 63-22-207 is the statute that creates the Board of Examiners over the Licensed Professional Counselors. That Board enacted rules and regulations. The rules and regulations enacted by the Board governing LPCs states in 0450-1-.13 "In addition to the other requirements of this rule, all licensees and certificate holders who practice counseling electronically shall comply with the Ethical Standards for Internet Online Counseling adopted by the American Counseling Association, www.counseling.org, except to the extent that they conflict with the laws of the state of Tennessee or the rules of the Board. If the standards for the ethical practice of internet counseling conflict with state law or rules, the state law or rules govern the matter. Violation of the standards for the ethical practice of web counseling or state law or rules may subject a licensee or certificate holder to disciplinary action." Per the documentation on ACA's site, the Ethical Standards for Internet Counseling is no longer in force as section A.12 of the Code of Ethics was updated to address issues previously listed outside of the Code of Ethics. This section addresses informed consent, accessibility, web-presence and providing assistance to those who require it in using technology.

Standard A.12.e., "Laws and Statutes. Counselors ensure that the use of technology does not violate the laws of any local, state, national or international entity and observe all relevant statutes." Technology-assisted counseling, whether conducted by telephone, Internet, e-mail or other application, often results in the crossing of jurisdictional lines. So laws which apply in Texas may not apply in New York. It is incumbent upon a counselor to know and be in compliance with all laws in both their state or jurisdiction and the state or jurisdiction of the client. Thus for LPCs, the Code is incorporated into the Rules and Regulations by reference.

Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C. §§ 2510–2522)

TCA §39-13-601
(a)(1) Except as otherwise specifically provided in §§ 39-13-601 – 39-13-603 . . . a person commits an offense who:
(A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (2) A violation of subdivision (a)(1) shall be punished as provided in § 39-13-602 and shall be subject to suit as provided in § 39-13-603.
(5) *It is lawful* under §§ 39-13-601 – 39-13-603 and title 40, chapter 6, part 3 *for a person* not acting under color of law *to intercept a wire, oral, or electronic communication*, where the person is a party to the communication or *where one of the parties to the communication has given prior consent to the interception*, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the state of Tennessee.

The Tennessee Wiretapping and Electronic Surveillance Act, for example, makes it a Class D felony to intentionally intercept, access or procure another person to intercept or access unauthorized communications. Civil damages include:

> The sum of the actual damages, including any damages to personal or business reputation or relationships, suffered by the individual and any profits made by the violator as a result of the violations; or 2) Statutory damages of one hundred dollars ($100) per day for each day of violation or ten thousand dollars ($10,000), whichever is greater; and 3) Punitive damages; and 4) Reasonable attorney's fees and other litigation costs incurred.

TCA § 39-13-606—Electronic tracking of motor vehicles (as of 2012) reads, as follows:
(a) (1) Except as provided in subsection (b), it is an offense for a person to knowingly install, conceal or otherwise place an electronic tracking device in or on a motor vehicle without the consent of all owners of such vehicle for the purpose of monitoring or following an occupant or occupants of such vehicle. (2) As used in this section, "person" does not include the manufacturer of the motor vehicle.
(b) (1) It shall not be a violation if the installing, concealing or placing of an electronic tracking device in or on a motor vehicle is by, or at the direction of, a law enforcement officer in furtherance of a criminal investigation and is carried out in accordance with applicable state and federal law. (2) If the installing, concealing or placing of an electronic tracking device in or on a motor vehicle is by, or at the direction of, a parent or legal guardian who owns or leases such vehicle, and if such device is used solely for the purpose of monitoring the minor child of such

parent or legal guardian when such child is an occupant of such vehicle, then the installation, concealment or placement of such device in or on such vehicle without the consent of any or all occupants in such vehicle shall not be a violation. 3) It shall also not be a violation of this section if the installing, concealing or placing of an electronic tracking device in or on a motor vehicle is for the purpose of tracking the location of stolen goods being transported in such vehicle or for the purpose of tracking the location of such vehicle if it is stolen.
(c) The provisions of this section shall not apply to a tracking system installed by the manufacturer of a motor vehicle.

**Case Law**

Social media

*McMillen v. Hummingbird Speedway, Inc.*, No. 113-2010, Pa. County Ct. Sept. 9, 2010 "When a user communicates over Facebook or MySpace, he or she understands and tacitly submits to the possibility that a third party recipient . . . will also be receiving his or her messages . . . ." In a case addressing the confidentiality of social media, a Pennsylvania court ordered a personal injury plaintiff to allow opposing counsel access to his password-protected Facebook and MySpace accounts to investigate whether information on those sites contradicted his claims.

Recording

*Lawrence v. Lawrence*, Ct. Appeals November 2010

Leigh Ann Lawrence ("Mother") secretly tape recorded her 2 1/2-year-old daughter's telephone conversation with the child's father, Chris Lawrence ("Father"), during the course of a divorce and custody dispute. After the divorce was concluded, Father filed a complaint against Mother seeking damages for, among other things, wiretapping in violation of Tenn. Code Ann. §39-13-601 (2006). Father filed a motion for partial summary judgment which the trial court denied upon finding that "[n]o set of facts would create liability under §39-13-601 et seq. for [Mother's] interception of [Father's] communication with his daughter." The court then entered partial summary judgment in favor of Mother and certified the judgment as final. Father appeals. "Accordingly, we hold that, as a matter of law, Mother had the right to consent, as that term is used in Tenn. Code Ann. § 39-13-601, vicariously to intercepting, recording and disclosing the child's conversation with Father."

*Robinson v. Fulliton*, Court of Appeals May 2002

This is a wiretapping case. A husband and a wife were experiencing marital difficulties. During that time, the husband tape recorded a telephone conversation between his wife and her brother without the knowledge of either. When the brother found out, he filed a lawsuit against the husband, his brother-in-law, seeking damages under the civil damages provision of the Tennessee wiretapping statutes, Tenn. Code Ann. § 39-13-603. The trial court, sitting without a jury, held that the husband was liable to his brother-in-law, and awarded nominal compensatory damages, litigation expenses, and attorney's fees. The husband and the brother-in-law both appeal that decision, arguing that the damage award was erroneous. We reverse the trial court's award of damages, finding that the statute requires that, when a violation is established, the trial court must award either the actual damages or the statutory minimum penalty of $10,000, whichever is greater.

*Klumb v. Goan*, 2-09-Cv-115 (E.D. Tenn.; July 19, 2012) Federal District Case

Plaintiff Roy Klumb brought this action alleging defendant Crystal Goan, formerly is wife, violated the federal Wiretap Act, 18 U.S.C. 2510 et seq., and the Tennessee Wiretap Act, Tenn. Code Ann. 39-13-601et seq., by installing spyware on his computers without his consent to intercept his incoming email. A bench trial was held and, having heard all the evidence, the Court concludes that defendant Crystal Goan did violate the two wiretap statutes, that the plaintiff is entitled to the statutory damages of $10,000, and that defendant's violation of the wiretap acts was part of a larger scheme to gain advantage of the plaintiff during their divorce thereby warranting punitive damages in the amount of $10,000. The plaintiff is also entitled to reasonable attorney's fees and costs. An appropriate judgment shall be entered.

Waiving privilege
*In re Columbia/HCA Healthcare Corporation Billing Practices Litigation*, 293 F.3d 289 (2002), the District Court of Appeals held that a client cannot selectively waive the privilege. Columbia/HCA voluntarily waived the privilege by providing the Federal government with privileged communications in order to resolve charges of criminal and civil violations brought by the government. The Court held that the waiver of the privilege to the government waived the privilege in all other Columbia/HCA cases for which the same information was sought, e.g. lawsuits by insurance companies seeking reimbursement for improperly billed medical services. "The client cannot be permitted to pick and choose among his opponents, waiving the privilege for some and resurrecting the claim of confidentiality as to others, or to invoke the privilege as to communications whose confidentiality he has already compromised for his own benefit." Permian, 665 F.2d at 1221.

*Rule 502 of the Federal Rules of Evidence* provides that a party's intentional disclosure of a privileged communication or an attorney work product waives the privilege as to all other communications or work product regarding the same subject matter "if they ought in fairness to be considered together." Fed. R. Evid. 502(a). Courts will not allow a client to waive only those communications favorable to its cause. Rather, fairness requires that once a client voluntarily waives the privilege regarding a communication, all other communications relating to it must be disclosed, as well. Determining the scope of a subject matter waiver is a fact intensive inquiry: "There is no bright line test for determining what constitutes the subject matter of a waiver, rather, courts weigh the circumstances of the disclosure, the nature of the legal advice sought and the prejudice to the parties of permitting or prohibiting further disclosures." *Fort James Corp. v. Solo Cup Co.*, 412 F.3d 1340, 1349-50 (Fed. Cir. 2005).

*Lenz v. Universal Music Corp.*, No. 5:07-03783, N.D. Cal. Nov. 17, 2011, a California court found that the plaintiff in a copyright infringement suit had **waived the attorney-client privilege by sending emails to third parties and creating blog posts** regarding conversations with counsel. The infringement dispute arose when plaintiff sued Universal Music Corporation, claiming that Universal knowingly misrepresented that a video plaintiff posted on YouTube infringed Universal's copyright in a song.

**Professional Ethics**
**ACA: see section A.12.a-h**
**AMA Guidelines**
New communication technologies must never replace the crucial interpersonal contacts that are the very basis of the patient-physician relationship. Rather, electronic mail and other forms of

Internet communication should be used to enhance such contacts. Patient-physician electronic mail is defined as computer-based communication between physicians and patients within a professional relationship, in which the physician has taken on an explicit measure of responsibility for the patient's care. These guidelines do not address communication between physicians and consumers in which no ongoing professional relationship exists, as in an online discussion group or a public support forum.
(1) For those physicians who choose to utilize e-mail for selected patient and medical practice communications, the following guidelines be adopted.

**Communication Guidelines**

1. Establish turnaround time for messages. Exercise caution when using e-mail for urgent matters.
2. Inform patient about privacy issues.
3. Patients should know who besides addressee processes messages during addressee's usual business hours and during addressee's vacation or illness.
4. Whenever possible and appropriate, physicians should retain electronic and/or paper copies of e-mails communications with patients.
5. Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) permitted over e-mail.
6. Instruct patients to put the category of transaction in the subject line of the message for filtering: prescription, appointment, medical advice, billing question.
7. Request that patients put their name and patient identification number in the body of the message.
8. Configure automatic reply to acknowledge receipt of messages.
9. Send a new message to inform patient of completion of request.
10. Request that patients use auto reply feature to acknowledge reading clinicians message.
11. Develop archival and retrieval mechanisms.
12. Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use blind copy feature in software.
13. Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages.
14. Append a standard block of text to the end of e-mail messages to patients, which contains the physician's full name, contact information, and reminders about security and the importance of alternative forms of communication for emergencies.
15. Explain to patients that their messages should be concise.
16. When e-mail messages become too lengthy or the correspondence is prolonged, notify patients to come in to discuss or call them.
17. Remind patients when they do not adhere to the guidelines.
18. For patients who repeatedly do not adhere to the guidelines, it is acceptable to terminate the e-mail relationship.

**Medicolegal and Administrative Guidelines**

1. Develop a patient-clinician agreement for the informed consent for the use of e-mail. This should be discussed with and signed by the patient and documented in the medical record. Provide patients with a copy of the agreement. Agreement should contain the following:
2. Terms in communication guidelines (stated above).
3. Provide instructions for when and how to convert to phone calls and office visits.
4. Describe security mechanisms in place.
5. Hold harmless the health care institution for information loss due to technical failures.

6. Waive encryption requirement, if any, at patient's insistence.
7. Describe security mechanisms in place including:
8. Using a password-protected screen saver for all desktop workstations in the office, hospital, and at home.
9. Never forwarding patient-identifiable information to a third party without the patient's express permission.
10. Never using patient's e-mail address in a marketing scheme.
11. Not sharing professional e-mail accounts with family members.
12. Not using unencrypted wireless communications with patient-identifiable information.
13. Double-checking all "To" fields prior to sending messages.
14. Perform at least weekly backups of e-mail onto long-term storage. Define long-term as the term applicable to paper records.
15. Commit policy decisions to writing and electronic form.

(2) The policies and procedures for e-mail be communicated to all patients who desire to communicate electronically.

(3) The policies and procedures for e-mail be applied to facsimile communications, where appropriate. (BOT Rep. 2, A-00; Modified: CMS Rep. 4, A-01 and BOT Rep. 24, A-02)

**AMA Ethics Policy**

The following recommendations of the AMA Council on Ethical and Judicial Affairs were adopted as AMA Ethics Policy at the December 2002 Interim Meeting of the AMA House of Delegates.

Electronic mail (e-mail) can be a useful tool in the practice of medicine and can facilitate communication within a patient-physician relationship. When communicating with patients via e-mail, physicians should take the same precautions used when sending faxes to patients. These precautions are presented in the following considerations:

- E-mail correspondence should not be used to establish a patient-physician relationship. Rather, e-mail should supplement other, more personal, encounters.
- When using e-mail communication, physicians hold the same ethical responsibilities to their patients as they do during other encounters. Whenever communicating medical information, physicians must present the information in a manner that meets professional standards. To this end, specialty societies should provide specific guidance as the appropriateness of offering specialty care or advice through e-mail communication.
- Physicians should engage in e-mail communication with proper notification of e-mail's inherent limitations. Such notice should include information regarding potential breaches of privacy and confidentiality, difficulties in validating the identity of the parties, and delays in responses. Patients should have the opportunity to accept these limitations prior to the communication of privileged information. Disclaimers alone cannot absolve physicians of the ethical responsibility to protect patients' interests.
- Proper notification of e-mail's inherent limitations can be communicated during a prior patient encounter or in the initial e-mail communication with a patient. This is similar to checking with a patient about the privacy or security of a particular fax machine prior to

faxing sensitive medical information. If a patient initiates e-mail communication, the physician's initial response should include information regarding the limitations of e-mail and ask for the patient's consent to continue the e-mail conversation. Medical advice or information specific to the patient's condition should not be transmitted prior to obtaining the patient's authorization.