

The Legal Aspect of Communications

Chapter FastFACTS

- 1. E-mail has increased the incidences of unintended, unauthorized disclosures.**
- 2. Web-based e-mail services like Yahoo may not be safe enough for e-mail communication with patients.**
- 3. Unsecured text messaging is risky because the texts can stay on your phone indefinitely and can be read by anyone.**
- 4. Prevent legal headaches by getting patients' approval in writing before beginning e-mail communication.**
- 5. Other risks include delegating online communication to someone else in your office.**

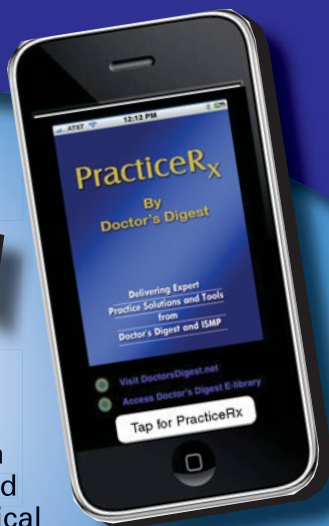
When does your telephone or online communication with patients cross legal boundaries? Although patients increasingly want electronic communication, the rules for what is and isn't allowed aren't always clear; but the consequences can be severe. "The number of complaints involving unauthorized release of patient information has increased substantially since the effective date of HIPAA privacy regulations," Mr. Kern states.

Patients are, with few limitations, entitled to complete information about their medical conditions. When that information is communicated face to face, the risk of unauthorized disclosure of personal health information is easily limited by simply ensuring that no one lacking the patient's authorization is present or

Reach Your National Patient Safety Goals With Our

Free iPhone/iPad App

PracticeRx by Doctor's Digest



Now, instantly and securely report medication safety errors and receive REAL-TIME Instant Medical and Hazard Alerts from ISMP with our FREE iPhone/iPod Touch/iPad App under the Medical Category in the Apple iTunes Store.

- **ISMP Med Safety Alerts:** Urgent audio alerts in Real time!
- **Medication Errors Reporting Program (MERP):** Report errors securely and directly to ISMP.
- **Essential Practice Management Tips from *Doctor's Digest*:** In text, audio and video format.
- **Free e-subscription to *Doctor's Digest-Money Matters*:** Personal financial tips for MDs from the experts.

To register, please go to iTunes App Store and search for PracticeRx.

Don't have an iPhone? Go to www.doctorsdigest.net/ismp to sign up for REAL-TIME Medication/Hazard alerts to be sent directly to your e-mail address.

able to overhear the conversation, Mr. Kern says. “[But] when communicating by telephone or electronically, the risks of unauthorized disclosure increase substantially. Even something as



“Have a written authorization with sufficient information about the third-party, such as address and date of birth, to enable you to [verify the identify of that party].”

Steven Kern, Esq.
Principal

Kern Augustine Conroy & Schoppmann P.C.
Bridgewater, N.J.

innocent as confirming an appointment can be problematic, especially for physicians whose area of practice could suggest the reason for a visit,” he says. Knowing how to disclose information appropriately and what is or isn’t acceptable is key to avoiding legal problems.

Disclosing Information

For now, the HIPAA privacy rule is considered the “least common denominator for privacy regulation,” says the ACP, because it requires forthright patient consent only for use and divulgence of information “beyond the purpose of treatment, payment, or operational activities.” (Go to www.hhs.gov/ocr/hipaa/ for more information.) In other words, personal health information can be disclosed only to someone authorized by the patient to receive that information (or to a parent or guardian, with certain exceptions). When communicating with a patient via telephone, be sure that the person you are communicating with is, in fact, the patient and that the method of communication is secure, Mr. Kern advises. Obtaining the patient’s date of birth, the last four digits of a Social Security number, and a home address, as well as insurance information, can help guard against disclosure to someone falsely claiming to be a patient.

Similarly, if the patient has authorized you to disclose information to a third party by telephone, be sure that you are able to verify the identity of that party. “Have a written authorization

with sufficient information about the third party, such as address and date of birth, to enable you to do so,” Mr. Kern says. (See “What Your Authorization Should Include” for more details.)

Using e-mail has increased the opportunities for unintended, unauthorized disclosures. When communicating via the Internet, not only must you be sure that the person with whom you are communicating is the patient or other authorized person, but you must also be confident that no one without authorization has access to the information being transmitted. Just as with telephone communication, it is essential that the person to whom you are disclosing confidential health information is authorized to receive it. In addition, you must be confident that the information is not accessible to unauthorized personnel, either in your office, or at the recipient’s location. For example, a patient’s e-mail address at her office may be accessible to her employer; and her home e-mail may be used by other family members. Therefore, before using e-mail or other electronic communication, obtain written authorization from the patient and acknowledgement that the address where the electronic communication is being sent is not accessible to any other person.

What Are the Risks?

Are you using Hotmail, Yahoo, MSN, or gmail to send e-mail to your patients? Those Web-based e-mail services may not be secure enough, say legal and privacy experts. First, find out what’s allowed in your state—there may be specific privacy laws related to e-mail communication about medical issues. In addition, some state medical boards restrict the use of virtual office visits. They may, for example, require physicians to see patients in person before writing a prescription for them. In these cases, you may choose to limit virtual office visits to established patients. However, some states are not clear on what’s allowed,

Changes in Tax Deduction for Medical Equipment



Read about how you can take advantage of the new cap on medical equipment deductions for 2010 in the latest issue of *Doctor's Digest-Money Matters* at www.doctorsdigest.net.

according to Dr. Saylak, and thus may follow federal guidelines or statutes.

This patchwork of legal guidelines has come about because most existing state and federal privacy laws didn't anticipate virtual office visits and e-mails, and so are not designed to cover those types of doctor-patient communication—a problem that



“Some cellphone vendors, e-mail service providers, and third-party vendors do provide encryption. The encryption provider lets you know when you have an e-mail so that you can log into it through a protected server to access your e-mails, or even phone calls and voicemails.”

Kevin J. Ryan

Chair, Healthcare Law Group
Much Shelist
Chicago, Ill.

will need to be rectified given that this type of communication will grow “exponentially over the next few years,” Dr. Saylak explains.

Although the legalities of doctor-patient e-mail messaging differ by jurisdiction, sharing general medical knowledge is acceptable, according to Dr. Saylak. The problems begin once the information becomes more specific and detailed, because it's difficult to ensure that the e-mail is going to the person for whom it was intended. This differs from giving advice over the phone for something like a urinary tract infection, which some physicians are comfortable doing because they can verify the phone number and because they recognize the patient's voice. Until secure communication can be ensured, he urges caution. “The individual doctor is going to have to carefully assess the risks of online communication with his patients,” Dr. Saylak says.

Christoph U. Lehmann, MD, FAAP, associate professor at Johns Hopkins University, Baltimore, Md., and director of medical health informatics for AAP, says he's even more concerned about text messaging because messages can stay on your phone forever, enabling anybody to read them. Until security can be

What Your Authorizations Should Include

It is critical to have patients sign an authorization form that states your conditions for e-mail communications. Authorizations for release of information to a third party should be witnessed to confirm the identification of the person authorizing the release, according to Mr. Kern. The authorization should include identifying information about the patient (birthdate, last four digits of Social Security number, insurance policy number, and photo ID) and should specifically state that the patient authorizes the physician to release all information concerning the patient's health history, examination, test results, treatment, and recommendations, to (blank). Such information may be released through the following means:

- ✓ Written documentation addressed to: _____
 - ✓ Telephone communication to the following telephone number:

 - ✓ Message on answering machine or voicemail at the following number:

 - ✓ Electronic communication via e-mail to the following e-mail address:

- Other: _____

If the authorization does not include all information, it should specifically indicate exactly what information may (or may not) be disclosed. The authorization should also be time limited to no more than one year, Mr. Kern adds.

Understanding Which IRA is Best For You

It may be a Roth IRA instead of a traditional IRA now that new health insurance legislation is taking effect. Find out more in the latest issue of *Doctor's Digest-Money Matters* at www.doctorsdigest.net.



guaranteed—HIPAA requires encryption at the 128-bit level—the only roles he sees for unsecured e-mail and texting are for scheduling and confirming appointments.

Kevin J. Ryan, chair of the healthcare law group at Much Shelist, Chicago, says that more and more e-mail software programs and cellphone service providers today are providing secure encryption. If you use either to communicate with patients or other healthcare providers, he recommends searching online for a term like “HIPAA-compliant e-mail” or “HIPAA-encrypted cellphones” in order to verify that your cellphone provider and e-mail are, in fact, secure. The search can also identify providers who offer the necessary encryption for your mobile device. “Some cellphone vendors, e-mail service providers, and third-party vendors do provide encryption. The encryption provider lets you know when you have an e-mail so that you can log into it through a protected server to access your e-mails, or even phone calls and voicemails. You are then required to log in with an ID and password in order to view or hear your message,” Mr. Ryan explains. “This type of security is similar to the security used in remote banking.”

Seattle Children’s Hospital physicians have secure e-mail messaging although Dr. Del Beccaro says that they sometimes use the non-secure e-mail if sending a more general message to a patient, one that does not contain any identifying information or HIPAA-related issues.

If the person receiving the medical information via e-mail or text is not authorized to receive it, the physician may be violating the patient’s privacy rights, especially when there’s enough information in the message to identify the patient, Mr. Kern says. Breaching HIPAA regulations is the most serious concern, but certainly not the only legal problem that may be encountered if sensitive information is disclosed. For more tips, see “Using E-mail for Physician-Patient Communication” and “Medico-legal and Administrative E-mail Guidelines.”

If a message is sent concerning a sensitive issue, such as the results of a test for a sexually transmitted disease or a drug or alcohol screening, and that information is accessed by a spouse or employer, for example, that disclosure could result in a divorce or loss of a job. “If somebody’s personal information

Medicolegal and Administrative E-mail Guidelines

The following tips are from the AMIA's white paper, "Guidelines for the Clinical Use of Electronic Mail with Patients":

- Consider obtaining patient's informed consent for use of e-mail; written forms should do the following:
 - Itemize terms in communication guidelines;
 - Provide instructions for when and how to escalate to phone calls and office visits;
 - Describe security mechanisms in place;
 - Indemnify the healthcare institution for information loss due to technical failures and;
 - Waive encryption requirement, if any, at patient's insistence;
- Use password-protected screen savers for all desktop workstations in the office, hospital, and at home.
- Never forward patient-identifiable information to a third party without the patient's express permission.
- Never use a patient's e-mail address in a marketing plan.
- Do not share professional e-mail accounts with family members.
- Use encryption for all messages when encryption technology becomes widely available, user-friendly, and practical.
- Do not use unencrypted wireless communications with patient-identifiable information.
- Double-check all "To:" fields prior to sending messages.
- Perform at least weekly backups of e-mail onto long-term storage; define "long-term" as the term applicable to paper records .
- Commit policy decisions to writing and electronic form.

gets out and the patient winds up losing a job, you've got a potential lawsuit," he says.

Preventing Legal Headaches

To prevent legal problems resulting from e-mail communication, experts advise the following:

- **Get the patient's approval in writing** before beginning any

online communication with them concerning their medical care. You don't know who has access to the phone number you text or the address you e-mail.

- **Use a secure site** as another option, placing patient information there and allowing patients to access that information by using a pre-assigned password.
- **Don't leave a message beyond** saying, "This is Dr. X. Please call my office," unless you have written authorization from the patient.
- **Written authorization** can be as simple as "I hereby authorize Dr. X to communicate any information concerning my healthcare to me at the following secure e-mail address. This authorization is valid for one year unless revoked by me in writing." However, since certain state laws may require additional information, and since federal rules are subject to change, consult a healthcare attorney before finalizing any authorization for communication of protected healthcare information.
- **Remind patients** not to use their employer's e-mail account to send healthcare-related messages to their physician, because it's not secure.
- **Let patients know that certain symptoms or conditions**, such as those related to breathing difficulties or the heart, are not suitable for e-mail; instead, the patient must be seen in the office or go to the nearest emergency department.
- **Contact your medical liability insurance provider** to be sure that this type of interaction is covered under your policy and that your practice is following state board guidelines.
- **Ask your vendor to set up online technologies** to ensure that such communication is automatically attached to each patient's EMR.

Other Risks

Other risks can lead to legal problems when you communicate online. If you choose to delegate online communication to another person in the office, perhaps a nurse or assistant, in many jurisdictions you can be held liable for the content of that communication. Since education standards and legal torts vary from state to state, you must be sure that such communication is reviewed and approved—and if necessary—promptly corrected

Using E-mail for Physician-Patient Communication

These guidelines are adapted from the American Medical Informatics Association's (AMIA) "Guidelines for the Clinical Use of Electronic Mail with Patients":

- Establish turnaround time for messages; do not use e-mail when urgent matters are involved.
- Inform patients about privacy issues. Patients should know who (besides the addressee) processes messages
 - during addressee's usual business hours
 - during addressee's vacation or illness
 Include that information in the medical record.
- Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) that are and are not permitted over e-mail.
- Instruct patients to put the category of transaction in the message's subject line for filtering: "prescription," "appointment," "medical advice," or "billing question."
- Request that patients put their name and patient identification number in the body of the message.
- Configure an automatic reply to acknowledge receipt of messages. Print out all messages, along with replies and confirmation of receipt, and place them in the patient's paper chart.
- Send a new message to inform the patient that his or her request has been completed.
- Request that patients use the auto reply feature to acknowledge that they read the provider's message.
- Maintain a mailing list of patients, but do not send group mailings in which recipients are visible to each other; instead, use the "blind copy" option.
- Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages.

by you. Thus, many physicians elect to do these communications themselves, Dr. Saylak notes. If you're going to offer electronic visits via e-mail (preferably through a secure patient portal), then it's your responsibility to handle these visits in a manner to avoid legal potential legal exposure, i.e. just as if the patient were to

come into your office for medical treatment.

Mr. Ryan acknowledges that in medical practices, just as in business office settings, some physicians or staff members may not be technologically advanced or enthusiastic about online communication. But, he cautions, "I think everyone has to agree that if they're going to use electronic communication, they need



"[Answering e-mails from patients and their parents] is the way life is going."

Mark Del Beccaro, MD

Professor, Vice Chair for Clinical Affairs
Pediatrician in Chief
Department of Pediatrics
Seattle Children's Hospital
Seattle, Wash.

to agree on how they're going to use it." That means they have to agree on which technology to use and how to ensure that it is compliant with regulations like HIPAA. To stave off other problems, create policies and procedures that spell out when you will answer e-mails and who will answer e-mails when you are not in the office (e.g., when you are on vacation).

Despite the potential pitfalls, many physicians are using electronic communications. Dr. Del Beccaro says he spends more time than ever these days answering e-mails from patients and their parents. "This is the way life is going. Social media will have a greater place in the future. Online communication is definitely becoming the prevalent way of doing things.