eRisk for Providers

Understanding and mitigating Provider Risk Associated with Online Patient Interaction

March 2001

Medem, Inc.
333 Bush Street, 24th Floor
San Francisco, CA 94104
www: www.medem.com/erisk
e-mail: erisk@medem.com

DISCLAIMER/LIMITATION OF LIABILITIES

MEDEM, INC. and the eRisk Working Group for Healthcare ("the Working Group) have compiled the information in this document from sources believed to be reliable, and have suggested for further discussion certain proposed operational steps and standards with respect to physician-patient electronic communications. However, **Medem, Inc. and the Working Group do not make any warranties whatsoever regarding this document, and hereby disclaim all warranties whatsoever, either express or implied, that the information contained in this document is complete or accurate, or that the operational steps and standards suggested in this document would be sufficient to avoid legal liabilities. Medem, Inc. and the Working Group hereby exclude all implied warranties of merchantability and fitness for particular use or purpose with respect to the information and suggestions contained in this document.** Medem, Inc. and the Working Group make no warranty as to the reliability, accuracy, timeliness, usefulness, adequacy, completeness, or suitability of the information and suggestions in this document. The information and suggestions contained in this document are not exhaustive, and do not cover or address all legal or operational issues or standards. **This document is not a substitute for consultation with your own legal counsel, and does not constitute legal advice**. **You may not rely on this document as being sufficient to create for you your own compliance plan or regime with respect to physician-patient electronic communications**. This document is provided on an "AS IS" basis. Further, Medem, Inc. and the Working Group explicitly disclaim any responsibility for the accuracy, content, or availability of information from third parties or found on websites of third parties mentioned in this document.

UNDER NO CIRCUMSTANCES SHALL MEDEM, INC., THE WORKING GROUP, OR ANY OTHER PARTY INVOLVED IN CREATING, PRODUCING, OR DISTRIBUTING THIS DOCUMENT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSSES WHATSOEVER, INCLUDING BUT NOT LIMITED TO THOSE FOR LOSS OF PROFITS, LOSS OF GOODWILL, OR OTHER INTANGIBLE LOSSES (EVEN IF ONE OR MORE OF THE PARTIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) THAT RESULT FROM THE USE OF INFORMATION CONTAINED IN THIS DOCUMENT, OR FROM FOLLOWING SUGGESTED OPERATIONAL STEPS OR GUIDELINES CONTAINED OR SUGGESTED IN THIS DOCUMENT.

Overview

eRisk – The potential malpractice risk that a physician or other health care provider faces, when conducting patient communications, education and care over the Internet.

Background: Patients, and their physicians, are flocking to the Internet. In a recent survey by Medem, Inc., nearly half of all physician practices indicated that they had or planned to build a Web site for their practice. Consider that there has been a doubling of provider/practice Web sites and a tripling of provider-patient e-mail use in the 12-month period ending May 2000. A Cozint report in May 2000 demonstrated that, far from their inaccurate portrayal as technophobes, physicians were using the Internet at rates double the population at large. In a report published in February 2001, the Institute of Medicine urgently recommended that Congress create a $1 billion "innovation fund" to help subsidize promising health care information technology projects, for "many patients... could have their needs met more quickly and at a lower cost if they had the option of communicating with health care professionals through e-mail."

Physician-to-patient, (P2P) Internet-based interactions are an inescapable and increasingly prominent feature of the modern health care environment.

The Internet holds forth a tantalizing vision of improved patient outcomes, efficiency, satisfaction, and enhanced patient education. These beneficial effects can only be realized through the fullest utilization of the Internet's potential for communications.

The present challenge for all – patients, providers, technology developers, and health care system administrators – is determining the most effective uses of the communications technologies. We must proceed deliberately but not recklessly, grounded to the time honored traditions of the doctor-patient relationship.

eRisk Working Group in Healthcare – In August 2000, representatives of the leading medical malpractice insurers, representing more than 70 percent of covered U.S. physicians, began working with Medem and medical societies to identify the issues and liabilities associated with online physician-patient interaction and to develop guidelines to address these concerns. In October 2000, the working group, with the help of the law firm Foley and Lardner, gathered to discuss the current and future state of P2P Internet communications and review and refine a set of guidelines based on the collective input of all participants. The working group produced hundreds of proposed guidelines and recommendations for large provider organizations, individual physicians, and technology vendors and published them in a *Detailed Guidelines* document.

This document, *eRisk for Providers,* captures many of the important issues and conclusions reached by the group pertaining to individual physicians and their practices.

More information about eRisk including sample policies and disclaimers and information about ordering the *Detailed Guidelines* is available at www.medem.com/erisk

Major Considerations

Is there reason to be concerned about risk and liability from online physician-patient interactions?

A significant body of case law regarding online physician-patient communications has not yet been established. Because of this, the risks and liabilities are ill defined. Many physicians are likely conducting Internet-based communications and transactions with patients that carry considerable malpractice risk, even as they are unaware of what they are.

The Internet represents at least four areas of risk to providers and their insurance carriers:

- Liability for online malpractice.
- Liability associated with the expansion of the physician's office and the patient-physician relationship onto the Internet.
- Liability associated with the inadvertent creation of a physician-patient relationship (or other licensed provider-patient relationship).
- Liability for failures of process and/or supporting technology resulting in misuse, inappropriate disclosure, loss, or inappropriate access to patient information (including issues of HIPAA and other regulatory compliance).

Can a doctor-patient relationship be established online?

Case law has not yet determined when a patient-physician relationship begins, when the only contact is online. There is case law regarding telephone contact. Some tests have been:

- Whether the physician and patient ever saw each other.
- Whether the physician knew the patient's name.
- Whether there was ever a physical examination.
- Whether the physician ever saw the patient's medical records (including individual test results or images).
- Whether the patient compensated the physician.
- Whether the physician accepted the patient's request for an appointment (whether or not the parties actually kept the appointment).

Online interaction, depending upon its nature, might be held to offer a more 'information rich' interaction than telephone. For instance, if there is both a messaging capability (whether interactive or asynchronous) supplemented by availability of access to an online record of health information, availability of online photographs of the parties, and so forth, the likelihood is probably increased that the courts would establish existence of a relationship based exclusively on "cyber-contact."

There is also no existing case law regarding malpractice liability for exclusively online interactions. On one hand, if the interaction is exclusively online then perhaps no patient-physician relationship has been established in which case the physician should be in the clear. On the other hand, there are new areas of exposure relative to online interaction, assuming that a relationship is somehow established. Hence, the particular need for careful informed consent and expectation setting in cases where it is believed that a patient-physician relationship has been established.

The rest of the document is organized into five major sections:

1. General Guidelines
2. Privacy, Confidentiality and Security
3. Publication of Web Sites
4. Messaging Services
5. Clinical Content

Within these sections, guidelines are generally grouped around:

- Choosing third-party services or building your own (i.e., product features).
- Using these services (i.e., policies and procedures).

The information and suggestions contained in this document are not exhaustive, and do not cover or address all legal or operational issues or standards. This document is not a substitute for consultation with your own legal counsel, and does not constitute legal advice. Do not rely on this document as being sufficient to create your own compliance plan or regime with respect to physician-patient electronic communications.

Where no broader organizational policies apply, you should develop your own policies and procedures, doing so with the advice of your local legal counsel.

1. General Guidelines

1.1 Using Online Services to Interact with Patients

Develop and maintain a written internal policy for your staff regarding online patient interaction ("Staff Policies and Procedures") including:

- Advice to your practice staff that there may be increased risk associated with online interactions with individuals who are not established patients or who are in states other than where the physician is licensed.
- Your policy, guided by local legal counsel and/or your state licensing board and/or the state licensing boards of other states, regarding conduct of online interactions with:
  - Individuals who are not established patients:
  - Established patients who are, at the time of the communications, residents of a state other than those in which you are licensed to practice.
  - Established patients who are, at the time of the communications, temporarily in a state other than those in which you are licensed to practice.
- Advice that particular care should be taken to avoid de facto establishment of provider-patient relationships, particularly in a role as the primary medical decision maker.
- That your practice's use of online sites and services should be limited to those services on your "acceptable" list. If you do not have such a list, evaluate sites and services against these guidelines to decide which you are comfortable utilizing.
- That before establishing an online relationship, patients must read your policies, disclaimers, and terms of use, and also those of any third party online service being used, and have accepted (online or in writing) an informed consent to risks of online interaction.
- Whether parents will be permitted access to any information resulting from online interaction between practice staff and the parents' adolescent children as patients.
- The specific types of online interactions that are permissible for each staff person or job function. Other online patient interactions should not be engaged in, such as participation in any type of "online medical services auction" where providers submit bids for the performance of medical procedures.
- Where (clinic, hospital, home), for what purposes (routine, emergency), and by whom (categories of jobs or preferably to specific jobs) each third-party online service can be acceptably used).

Develop, maintain, and provide a notice to your patients describing your personal policies for online interaction (a "Personal Online Patient Policy") including:

- That you reserve the right to refuse online communications with any patient who uses the online services in a manner contradictory to your communicated policies or abuses such services.
- That you reserve the right to refuse to base conclusions of diagnosis or decisions regarding course of treatment upon information that is communicated to you by the patient online, in the absence of in-person encounter(s) regarding the condition(s) or complaint(s) in question.
- Disclosure of any fees that you charge and insurance payments that you will accept for online consultations.

- Disclosure of any extents to which your office and/or support staff might also see and process online communications of various types, stating the nature of those staff persons' involvement (e.g. reviewing and forwarding messages based on subject matter or type of request).
- Any criteria you set for maintaining an established online patient relationship such as: patient must be seen in person in the last 180 days.
- How the patient will be notified in case you decide to discontinue further online interactions with him/her.

Before beginning an online relationship, have each patient:

- Acknowledge their understanding of your "Personal Online Patient Policy."
- Accept a disclaimer that protects you with regard to use of the online services.

Maintain a verifiable record of patient acceptances of your "Personal Online Patient Policy."

2. Privacy, Confidentiality and Information Security

2.1 Choose Third-Party Online Services to Interact with Patients that:

- Post an online Privacy and Confidentiality Policy for consumers/patients that addresses all of the five Fair Information Practices (Notice, Choice, Access, Integrity, and Redress) regarding the service's own operations. This should include exhaustive and detailed notice of information handling practices and information security provisions:
  - Users should be fully informed regarding:
    - What information is captured
    - How it is kept, used, and disclosed
    - Whether and how they can access it
  - Discussion of information security provisions should address:
    - Physical security
    - Authentication and access control
    - Encryption
    - Audit trails
    - Disaster recovery and business continuity
    - Data integrity
    - And internal policies and procedures
- Operate in full accordance with posted its posted Privacy and Confidentiality Policy.
- Require Web site visitors to read and accept terms of its online Privacy Policy before accepting any personally identifiable information from them.
- Provide contact information so that users of its services can ask questions regarding their privacy and the confidentiality and security of their information.
- Ensure that a user's acceptance of the privacy policy is logged, documented, or otherwise verifiable.
- Present all online services that collect personally identifiable information on an optional basis.
- Disclose all uses of third-party online ad services to site users.
- Disclose all uses of cookies, Web bugs, or other tracking techniques to site users.
- Assure users' privacy and confidentiality and the security of their information, by addressing all of the following:
  - Authentication of users and verification of their access privilege are required before granting access to any personal identifying information or personally identifiable health information.
  - All personal identifying information and personally identifiable health information is encrypted in transit using 128-bit or stronger encryption.
  - Persistent storage of all personal identifying information and personally identifiable health information is on database servers that are not visible to the Internet.
  - Hosting environment is firewall-protected.
  - Applications provide robust audit trails and are otherwise designed to support non-repudiation in an application-appropriate manner (for instance, a messaging service must ensure that messages, once sent, cannot be altered or denied).

- Applications are designed to provide healthcare provider organizations with the means to control, in a job function-appropriate manner, their staff persons' access privileges with respect to specific application functionality and/or specific types of information.

- Do not permit direct access to the health information of adolescents by their parents, without intervention by the adolescent's physician.
- Comply with all relevant Health Insurance Portability Act (HIPAA) requirements.

2.2 Use of Online Services to Interact with Patients

For any third party-online service used, review changes in their policies and terms of use at some maximum interval (e.g., 6 months or 12 months).

Do not disclose any patient identifying or health information to third parties for their use in direct marketing.

Store copies or printouts of the electronic messages in a manner that is consistent, in terms of information security and confidentiality protections, with your treatment of medical records.

Comply with all relevant Health Insurance Portability Act (HIPAA) requirements.

3. Publication of Web Sites

These guidelines pertain to providers that produce and publish their own Web sites, and to independent commercial enterprises that provide tools and hosting services that permit provider organizations to construct and publish Web sites.

Patients are going to the Internet for clinical information. Many are asking their physicians for guidance. Physicians are either providing this information on their own Web sites or directing their patients elsewhere for it. In both situations, issues arise regarding the content source and responsibility for, and frequency of, updates. There are also potential risks of conflict of interest associated with delivery of advertising/sponsorship along with the clinical information.

3.1 Produce Your Own Provider Web Site or Choose a Third-Party Service That:

- Provides users direct access to your Web site without passing through a third party "portal" site.
- Requires users of your provider site to read and accept terms of service and a medical disclaimer prior to inputting or exchanging personal health information, and that the medical disclaimer extends legal protection to you and your organization.
- Allows you and your organization to review the available third-party content and select specific articles that you wish to post on your own site.
- Notifies you when there are significant changes to accepted standards/protocols that could impact the third-party content published on your sites.
- Allows you to adapt or modify the third-party content that you post to your site, or allows you to selectively suppress this content and post your own.
- Provides you a means to rapidly and conveniently publish, unpublish, and edit your site.
- Displays links on each third-party content page to a description of the editorial policy governing the production and/or selection of the content.
- Serves intermediate "buffer" pages or uses similar notification tools for any links to external third party sites, notifying users they are about to interact with another site that may have different privacy, security, sponsorship, editorial, and other policies than your site, and whether or not there is any endorsement of the third party site.

3.2 Use of Your Provider Web Site

If you use a third-party service for your Web site that requires patients and other visitors to pass through a central portal for access to your site, then post a notice on your site stating whether you do or do not endorse the third party, its 'portal' site, the portal site's content and editorial policies, and any products or services that the portal site offers.

To the extent that a visitor might optionally reach your site via a portal site, ensure that there is no undesired appearance that you endorse the portal site.

Clearly state on your site:

- Your credentials
- Where (in what States) you practice

Clearly attribute authorship and dates of publication and revision for any locally authored content.

Develop and maintain a written internal policy for your staff regarding online patient interaction ("Staff Policies and Procedures") including:

- An internal protocol for periodic review of your site for timeliness and accuracy of health information and ongoing conformance to local or generally accepted standards of care.
- A list of "trusted content sources" and individually review all content on your site from other sources or else block or delete it from the site. Examples of "trusted sources" might include the NIH, the CDC, the medical professional societies, peer-reviewed journals, nationally/internationally respected clinics and teaching hospitals.
- A policy/recommendation regarding what portions of the site(s) (if any) shall be accessible by individuals who are not established patients of your practice.
- Requirements that you and your staff do not make any false, exaggerated, or unsupportable claims regarding specific services that you provide, nor make unsupportable claims regarding overall standards or quality of care that you can provide, nor appear to make any implied warranties regarding any specific services or overall quality of care.

4. Messaging Services

Physicians and patients are increasingly using e-mail to exchange confidential health care information. The difficulty is that adoption of new technologies is outpacing the development of standards that dictate proper use. The eRisk group supports the concept of electronic P2P communications but cautions that the provider is at increased risk if he/she uses an unauthenticated, unencrypted, non-secure communications network. ***Most readily available e-mail clients do not meet this standard.***

4.1 Choose a Third-Party Messaging Service That:

- Permits patient communication only with healthcare providers that have explicitly accepted the patient's request to establish an online relationship.
- Allows providers to selectively block communications from specific patients, and can block and unblock at will.
- Appropriately encrypts all communications in transit and thereby protects them against 'snooping' attacks.
- Provides safeguards to ensure that messages cannot be accessed by individuals other than the sender and intended recipients
- Restricts forwarding of messages regarding specific medical conditions (by the original addressee) to other users of the service that have 'healthcare provider' credentials within the system.
- Prevents forwarding of messages to non-secure messaging modalities such as standard e-mail. However, such non-secure modalities may be used to notify addressees of the existence of incoming secure messages.
- Protects against e-mail-borne computer viruses being introduced into the secure messaging environment from any interfaces with standard e-mail.
- Provides a capability for categorizing messages according to type or purpose and for indicating type or category within a message header (e.g., a message template for prescription renewal requests).
- Provides a means for a healthcare provider organization to control staff access to specific categories of messages if appropriate.
- Provides senders with reliable means to know their messages have been delivered.

4.2 Use of Online Messaging Services

Develop and maintain a written internal policy for your staff regarding online patient interaction ("Staff Policies and Procedures") including:

- The procedures to follow for establishing the identity of a message sender, and the minimum criteria to be relied upon in conclusions about identities of message senders.
- The types of transactions that are:
  - *Acceptable to conduct online* (e.g. appointment request, prescription renewal, general questions, billing questions, clinical questions regarding a condition for which patient **has** been seen in person in the prior 180 days).
  - *Not acceptable to conduct online* (e.g. new prescriptions, clinical questions regarding a condition for which patient **has not** been seen in person in the prior 180 days).

- The specific types of message-oriented inquiries that are permissible for each staff person or job function to:
  - Access
  - Process
  - Respond to
- Procedures to incorporate copies or printouts of your provider-patient online messages into the existing (paper and/or electronic) medical record.
- Procedures to ensure that messages and audit trails are retained and stored in a manner that fulfills applicable state and Federal regulations.
- Procedures you would follow to ensure orderly transfer of custody of, and/or access privileges to, the historical records of online messages left behind by individuals who are leaving your staff, or brought in by individuals who are joining your staff.
- A policy regarding acceptable conditions for processing of electronic messages by staff other than the specific addressee (e.g. processing of messages to physician by physician's staff or answering service).
- Instructions that any message sent that contains specific medical advice should include an explicit statement to that effect, and should clearly state whatever follow up treatment is needed.
- Instructions that any message sent that does not contain specific medical advice (e.g. a referral to additional general information on a condition or procedure) should include a disclaimer to that effect.

Develop, maintain, and provide a notice to your patients describing your personal policies for online interaction (a "Personal Online Patient Policy") including:

- What the patient should expect in terms of:
  - Timeliness of response to online communications.
  - Appropriate and inappropriate subject matters for discussion using the online messaging service (e.g. not for "online therapy", not for emergency situations).
  - Whether and how messages are to be incorporated into the existing medical record
  - The procedure the patient should follow when online communications are not responded to in accordance with those documented expectations.
  - That you may refuse to respond online to a patient who you believe needs to be seen in person, how you will notify a patient that s/he needs to be seen in person, and that records of such notifications will be added to patients' medical records.
  - Disclosure of any cases when someone other than the actual addressee may process patients' messages.

5. Clinical Content

The eRisk working group felt that if a physician puts clinical information on his/her Web site, that there was an affirmative obligation that it should be of high quality and be appropriately updated.

5.1 Choose a Third-Party Online Clinical Content Provider That:

- Makes available a description of the underlying editorial standards and process for all content available for its consumers to review.
- Offers consumer/patient-oriented content conforming to generally accepted standards of care and/or derives from "trusted sources" such as the NIH, the CDC, the medical professional societies, peer-reviewed journals, nationally/internationally respected clinics and teaching hospitals.
- Has an editorial process that enforces standards for timeliness of periodic review and update of the entire content library (e.g. such that no article in the library has gone without review for a period exceeding 12 months).
- Ensures every item of content includes a clear and prominent disclaimer (or a link to one) that addresses at least these issues:
  - All clinical content is for informational purposes only and not to be used for diagnosis or treatment.
  - The advice of a healthcare provider should always be sought.
  - No therapeutic relationship is established as a result of the patient's access and viewing of the content, with or without specific referral from a clinician.
- Presents content at a reading level and in language(s) appropriate to the intended target audience(s).
- Explicitly discloses, or makes easily discernable to the reader within the text, whether all claims, opinions, or conclusions are based upon study, consensus, or personal professional experience.

5.2 Use of Online Clinical Content

Develop and maintain a written internal policy for your staff regarding online patient interaction ("Staff Policies and Procedures") including:

- A list of those health information content sites/sources that you consider acceptable for you and your staff to refer patients to.
- A policy that referrals to content sites should only go to sites on your "acceptable" list.
- An internal protocol for periodic review of information referral site recommendations.
- A policy/recommendation detailing mechanisms and minimum standards for responding to patients' questions arising from their use of online content, and for documenting the resolution of those questions.
- A policy/recommendation that unless the intent is to incorporate online content as part of treatment, patients are to be referred to online content only with explicit instruction that they are to consider the content as "health education" and not as specific medical advice.

If you publish any self-authored content on your site then:

- Attribute yourself as its source
- Include the original publication and last revision date
- Maintain an archive of the revision histories of all such articles