eRisk Working Group for Healthcare's Guidelines for Online Communication

October 2006

The *eRisk Guidelines* have been developed by the eRisk Working Group for Healthcare, a consortium of professional liability carriers, medical societies and state licensure board representatives. These *Guidelines* are meant to provide information to healthcare providers related to the use of online communication and services with patients. They are reviewed and updated regularly. These *Guidelines* are not meant as legal advice and clinicians are encouraged to bring any specific questions or issues related to online communication to their legal counsel.

General Principles

The legal rules, ethical guidelines and professional etiquette that govern and guide traditional communications between the healthcare provider and patient are equally applicable to email, Web sites, list serves and other electronic services and communications, including the use of Personal Health Records (PHRs) with patients. A Personal Health Record (PHR) is established, owned and controlled by the patient or their caregiver. An Electronic Medical Record (EMR) is a practice-based clinical record that is established, owned and controlled by the practice. However, the technology of online communications introduces special concerns and risks as follows:

1. **Confidentiality.** The healthcare clinician is responsible for taking reasonable steps to protect patient privacy and to guard against unauthorized access to and/or use of patient healthcare information. This responsibility extends to the use of network services that have an appropriate level of privacy and security as required under HIPAA. Following are key considerations:

    a. **Privacy and Security.** Online communications between healthcare clinicians and patients should be conducted over a secure network, with provisions for privacy and security, including encryption, in accordance with HIPAA. Standard email services do not meet the requirements under HIPAA. Healthcare clinicians need to be aware of the full range of potential privacy and security risks and the requirements under HIPAA designed to mitigate those risks, and develop policies and procedures accordingly.

    Note: With respect to email specifically, clinicians should add a disclosure to the bottom of their standard, non-secure email service stating that "this email is not secure, and is not for use by patients or for healthcare purposes in general".

    b. **Authentication.** Healthcare clinicians have responsibility for taking reasonable steps to authenticate the identity of correspondent(s) in electronic communication and to ensure that recipients of information are authorized to receive it. Patient authentication, or authentication of an authorized patient proxy (i.e., parent of a minor, authorized family member, etc.) for patient–provider online communication including the delivery of patient data is important in order to ensure patient privacy and confidentiality. Clinicians are encouraged to follow the following guidelines for patient authentication:

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.

i. Have a written patient authentication protocol for all practice personnel and require all members of the staff to understand and adhere to the protocol.

ii. Establish minimum standards for patient authentication when a patient is new to a practice or not well known. Examples include requiring the production of a government-issued photo ID prior to first granting online communication or data sharing services to new patients. For new patients without government—issued IDs, other measures should be taken to confirm their identity; these could include mailing a postal card or letter to the patient's address which asks them to call the practice to confirm receipt of the letter and their online information and communications options with the practice.

iii. Keep a written record, electronic or on paper, of each patient authenticated for online communication or data exchange. The record should include the following:

1. Name of the patient
2. Date of authentication
3. Name of practice staff authenticating the patient
4. Means used to authenticate the patient

iv. Providers should take care not to offer, promote or encourage patients to participate in online healthcare services where patient authentication is not addressed to at least the level offered by the provider in his/her own practice.

2. **Unauthorized Access to Computers.** Unauthorized physical access to computers can immediately compromise patient information or put that information at risk through compromise of the security of the computers. Practices should establish and follow procedures to guard against unauthorized access to computers with technologies such as automatic log-out and password protection.

3. **Informed Consent.** Prior to the initiation of online communication between healthcare clinician and patient, informed consent should be obtained from the patient regarding the appropriate use and limitations of this form of communication. Clinicians should develop and adhere to specific written guidelines and protocols for online communications with patients, such as avoiding emergency use, heightened consideration of use for highly sensitive medical topics, setting expectations for response times, etc. These guidelines should be documented in the clinician's practice policy manuals, in patient terms of service or disclosures, or in the medical record when appropriate.

   Clinicians should exercise discretion when selecting patients for the use of online services to ensure that they are capable of electronic communication and will be compliant. Practices should consider developing patient use guidelines to help clinicians decide who uses these services on a patient-specific basis.

4. **Pre-Existing Clinician-Patient Relationship.** Healthcare clinicians may increase their liability exposure by *initiating* a clinician-patient relationship online. Payment for online services may further increase that exposure. Online communications of any kind are best suited for patients previously seen and evaluated in an office setting.

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.

5. **Licensing Jurisdiction.** Online interactions between a healthcare clinician and a patient are subject to requirements of state licensure. Communications online with a patient, outside of the state in which the clinician holds a license, may subject the clinician to increased risk. For example, pathologists, radiologists and other clinicians interpreting specimens, slides or images sent through interstate commerce for a primary diagnosis that becomes part of the patient's medical record, should have a license to practice medicine in the state in which the patient presents for diagnosis or where the specimen is taken or image is made. Intra-specialty consultation does not require in-state licensure, provided the consultation is requested by a physician licensed within the state and is referenced in a report they issue.

6. **Highly Sensitive Subject Matter.** Clinicians should advise patients of potential privacy risks associated with online communication related to highly sensitive medical subjects, such as issues of mental health, substance abuse, HIV status, etc.

   Some states have laws about special classes of health information, such as HIV or mental health. Clinicians should follow state law in obtaining approval from the patient to exchange those classes of information with patients, unless the clinician is sure they can differentiate between the two types for both transmitting and receiving information.

   Note: As interoperability between technology-based services (such as an EMR and a PHR) become more common, it will become even harder to control the distribution of these different classes of data, especially since states classify them differently. To avoid unforeseen issues, clinicians should follow state law to get approval from the patient to exchange ALL classes of information.

7. **Patient Education and Care Management**. Healthcare clinicians are responsible for the information that they make available to their patients online. Information that is provided to patients through a PHR, automated patient education programs, care management and other online services should come either directly from the healthcare clinician or from a recognized, credible and authoritative source.

8. **Emergency Subject Matter.** Healthcare clinicians should advise patients of the risks associated with online communication related to emergency medical subjects such as chest pain, shortness of breath, bleeding during pregnancy, etc. Clinicians should discourage the use of online communication to address medical emergencies and instead instruct patients to call the office or go to the emergency room. In addition, patients should be referred to the Online Consultation Terms of Service where they have accepted the condition that the Online Consultation service is not to be used for emergency issues.

9. **Medical Records.** A permanent record of online communications relevant to the ongoing medical care of the patient should be maintained as part of the patient's medical record, whether that record is paper or electronic. Online clinician-patient and clinician-clinician communications (including email) should be clinically-relevant as they are a permanent part of the medical record. Accurate and thorough documentation is effective risk management.

   Providers and patients should be aware that email and online information, including PHRs and consultations, are not erased from the hard drive when deleted and are potentially discoverable in litigation. Therefore all communicated information should be accurate and professional.

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.

As interoperability between technology-based services (such as an EMR and PHR) become more common, if a patient is allowed to electronically transmit information to a clinician, that information should be quarantined until the clinician has reviewed and commented on the data, to avoid introducing inappropriate or incorrect information into the clinicians' medical record.

10. **Practice Web Site Considerations.**

    a. **Authoritative Information.** Healthcare clinicians are responsible for the information they make available to their patients online. Information that is provided on a medical practice Web site or provided to a specific patient via secure email or other online services should come either directly from the healthcare clinician or from a recognized and credible source.

    b. **Commercial Information.** Web sites and online communications of an advertising, promotional or marketing nature may unrealistically raise patient expectations and subject clinicians to increased liability, including implicit guarantees or implied warranty and potential violation of consumer protection laws designed to protect against deceptive business practices. This is particularly true when cosmetic procedures, off-label drug use, and non-FDA approved procedures are promoted.

    c. **Links to Third Party Web Sites and Other Sources of Information.** Clinicians are encouraged to post a disclaimer page between their Web site and a link to any third party Web site/information that advises patients and other viewers that they are leaving the clinician practice Web site and that the clinician and the practice does not assume any responsibility for the content or the privacy of other Web sites to which the practice Web site links.

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.

Online Clinical Consultations

An Online Clinical Consultation is a clinical consultation between a clinician and a patient, similar to an office visit or a call that would be documented in the patient's chart, but conducted online via a secure messaging service. In an online clinical consultation, the clinician has the same obligations for patient care and follow-up as in face-to-face, written and telephone consultations. An online consultation should be substantive and specific to the patient's personal health status.

In addition to the 10 guidelines stated above, the following are additional considerations for fee-based online consultations:

1. **Informed Consent.** Prior to initiating an online consultation, the healthcare clinician should obtain the patient's informed consent to participate in the consultation, including discussing appropriate expectations, disclaimers and service terms,, and any fees that may be imposed. This consent can be presented as part of a Terms of Service the patient must accept either online or in writing before engaging in online consultations.
2. **Fee Disclosure.** Prior to an online consultation, patients should be clearly informed about any charges that might be incurred, and be made aware that the charges may not be reimbursed by the patient's health insurance.
3. **Identity Disclosure.** Clinical information that is provided to the patient during the course of an online consultation should come from, or be reviewed in detail by, the consulting clinician whose identity should be made clear to the patient.
4. **Available Information.** Healthcare clinicians should state and document, within the context of the consultation or clearly within the patient terms of service agreed to in advance of requesting an online consultation, that the consultation is based only upon information made available by the patient to the clinician during, or prior to, the online consultation, including referral to the patient's chart when appropriate, and therefore may not be an adequate substitute for an office visit.
5. **Online Consultation vs. Online Diagnosis and Treatment.** Clinicians should distinguish between an online consultation related to a known pre-existing condition (concerning ongoing treatment, follow-up questions, etc.) - - and the diagnosis and treatment of new conditions addressed for the first time online. The diagnosis and treatment of new conditions online may compromise patient safety and increase liability exposure. When clinicians decline to diagnose a new condition online, they should communicate the importance of immediate office follow-up to the patient and document this in their office medical record. When the patient presents at the office, clinicians should document the time lapse between their deferral of the online consultation and the patient's arrival in the office.
6. **Follow-Up Plans.** An online consultation should include an explicit follow-up plan, as clinically indicated, that is clearly communicated to the patient, in keeping with established protocols for in-office visits.
7. **Internet Pharmacies.** There are potential risks when patients are referred to on-line pharmacies, since some employ "cyberdocs" who dispense drugs and medical devices without a valid doctor's order and others may be involved in the illegal importation of prescription drugs. The National Association of Boards of Pharmacy has a Verified Internet Pharmacy Practice Sites (VIPPS) program (http://www.nabp.net/vipps/intro.asp). Pharmacies in compliance with their standards show the VIPPS seal of approval on their home page.

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.

Personal Health Records

Personal Health Records (PHRs) -- the electronic storage and exchange of patient information, which may include electronic patient education, FDA and medical device warnings, disease management, and other programs -- have the potential to improve care quality and efficiency. PHR and related information technology services are now being promoted by the government, health plans, employers, patient advocacy groups and others.

The technology of PHR and other patient-specific information technology services introduce special concerns and potential risks. When clinicians offer a PHR service to their patients, the patients/caregivers should be required to accept a PHR Terms of Service, either online through the PHR service provided or in writing from the practice, which at a minimum should include the following:

1. The PHR service is provided to patients for their convenience only, and is distinct from the medical record maintained by the physician or healthcare provider. Entries in the PHR do not become part of the medical record unless and until they are formally accepted for inclusion by the clinician.
2. It is the patient's responsibility to notify their healthcare clinician(s) if they have a PHR.
3. The PHR is not a substitute for directly communicating the patient's medical information to his or her physician in a traditional format (in-person, by telephone, etc.). Patients should not assume that their Personal Health Record has ever been seen or reviewed by their clinician(s).
4. It is the patient's responsibility to notify their healthcare provider(s) when new information appears in their PHR – whether they personally update it or it is automatically updated by third parties (health plans and other insurers, pharmacies, laboratories, etc.). Entering information into this record does not guarantee that their clinician will see it.
5. The provider should make it clear that the responsibility for the accuracy of the information in the PHR remains with the patient or caregiver as the owner of the record.
6. Developing and maintaining a PHR on a clinician practice Web site requires that patients have a pre-existing relationship with that clinician.
7. Materials and information available through the PHR are for informational purposes only and are not a substitute for professional medical advice.
8. Patients/caregivers should agree that they will contact their clinician if they have any questions about their medical condition, or if they need medical help.
9. Patients/caregivers should agree that if they need emergency medical help, they should immediately call 911, their local emergency number, or their physician.
10. Patients/caregivers should agree that their User ID and Password are their responsibility to protect from unauthorized access and use by third parties.

All clinicians are advised to have Terms of Service and other legal documents, including Informed Consent, etc. reviewed by their legal counsel.

Copyright © 2006 Medem, Inc. This document is intended as a guideline for the use of online communication and services between clinicians and patients, and is not establishing a standard of care, Any use of this document, in whole or in part, is subject to this Terms of Use. You agree to attribute the source of all utilized portions of this document as follows: "[Portions] Used with the permission of Medem, Inc. and the eRisk Working Group for Healthcare." You agree that you will not and may not rely on the attached eRisk documents as being sufficient to create your own policies, compliance plans, or regimens with respect to physician-patient electronic communications and that you will not and may not consider any of their contents to constitute legal advice. You agree that any transfer or distribution by you of the attached documents shall be made subject to these Terms of Use. All other uses are prohibited.