



E-Mail with Patients

The use of e-mail as a means of communication continues to grow in popularity. Messages can be exchanged by e-mail and SMS Text through many cellular phones. Physicians who choose to use this as a means of communicating with patients need to be aware of the risks associated with e-mail and SMS text.

This guideline provides helpful information on what is appropriate with e-mail communications between doctors and patients.

E-Mail is Forever

First and foremost, e-mail users should be aware that with few exceptions, e-mail is forever. Messages sent are typically stored on internet routers and servers, and forensic data specialists can retrieve these messages with surprising ease. Here are a few rules that can assist in avoiding embarrassment with e-mail:

- a. E-mail is not guaranteed to be a private communication. Never say anything in e-mail you don't want distributed. E-mail is easily forwarded and shared with vast numbers of people.
- b. E-mail should not identify a patient's name and personal health information in the same communication or communication string of messages. Due to the ease of distribution – and the possibility of improper distribution – it is very easy to violate HIPAA privacy protections by releasing names and medical conditions in the same message or message string.
- c. E-mail is accepted as evidence in courts of law. E-mail messages between doctor and patient should be treated as official communication and

Risk Management Guideline

copies should be included in the medical record.

d. Any e-mail message sent by a Physician should include a strong disclaimer, such as:

This e-mail is intended to be a private communication between doctor and patient. If you have received this message in error, please alert the sender immediately. Do not rely on this or any e-mail message for medical advice. This message is not offering medical advice or establishing a standard of care, and should not be substituted for appropriate medical care from a licensed professional. If you are experiencing an emergency medical condition, call 911 or visit your nearest emergency room immediately. E-mail messages may not be sent or received in a timely manner or may be delayed by networks and servers. We assume no responsibility for the misuse or inappropriate use of this e-mail message or its' contents.

When is E-Mail NOT appropriate?

E-Mail should NOT be used in the following circumstances:

- a. To communicate test results that are abnormal or require follow up.
- b. To disclose a negative change in the patient's health condition.
- c. To disclose an adverse medical event or unexpected outcome.
- d. To disclose a medical error.
- e. As a substitute for a face to face meeting regarding medical errors, adverse events, or unexpected outcomes.
- f. As a means of prescribing medications.
- g. As a means of giving medical advice.
- h. As a means of diagnosing patient conditions.



When can medical practices use E-Mail?

E-mail should only be used when requested by a patient. A simple request form signed by the patient should be included in the medical record, documenting that the patient has authorized use of e-mail messages as a means of communication.

- a. To schedule or confirm routine appointments for non-emergent conditions.
- b. To share information such as practice hours, phone numbers, holidays, or special news.
- c. To share practice newsletters.

Medical Advice and E-Mail

Medical advice should not be provided in e-mail messages. Many opportunities exist for miscommunication. A physician may be held responsible for medical advice rendered a patient via e-mail, and may even face some liability if the patient shares the information with others who then follow the advice.

If e-mail is used by a patient to report a medical condition, the treating physician should follow up with a phone call, appointment, and medical examination and / or treatment as needed.

Establishing E-Mail policy

Practices are best protected by establishing set policy and procedure with regard to the use of e-mail. At a minimum, such policy should include the topics discussed in this guidance.

E-Mail and Electronic Medical Records

Electronic Medical Record (EMR) systems allow the use of intranet (a secure network between offices) and internet (which may be an unsecured or secured use of the World Wide Web)

Risk Management Guideline

communications. Typically these are envisioned as means of communicating between offices or providers. Few envision communication between doctors and patients due to the potential liability issues.

If your EMR system has e-mail capability, ensure that appropriate security measures are in place including 'firewalls' designed to prohibit outside penetration of the system. Messages sent between doctors may contain information that is not suitable for distribution or release. Users should always be aware of the possibility that EMR systems may be accessed by unauthorized users, and the contents of messages distributed to the public.

The Best Suit of E-Mail Armor

The best suit of risk management armor with regard to e-mail messages is simple but restricts use of this communication medium.

- a. Do not offer any medical advice via e-mail. If a patient messages with a medical problem, schedule an office visit.
- b. Do not share medical information by e-mail. You do not know who is receiving the e-mail message or where it may be forwarded.
- c. Do not say anything in an e-mail message you would not want published on the front page of the local newspaper. This concept illustrates the fact that e-mail is permanent, accessible, and may be widely distributed beyond intended recipients.

This guideline is informational in nature. It is not intended to constitute legal, accounting, or medical advice. It is not intended to establish a standard of care. It does not constitute an insurance company policy. For specific assistance, consult a qualified expert in the area of concern.