



Email and the Clinical Practice

A primer to help you understand the requirements, risks, and opportunities of using email — plus tools to help you get started.

Prepared for clinical practitioners and their staff by HealthyEmail

Advisory Board Members

William Braithwaite, MD, PhD
National Director
HIPAA Advisory Services
PricewaterhouseCoopers LLP

John R. Christiansen
Attorney
Preston Gates & Ellis LLP

Emily Freeman
Vice President Western Region and
Executive Director of Consulting
American Insurance Group, Inc.

Stephen Harri
Managing Director
AON Health Alliance

Daniel S. Nutkis
Vice President
Strategy and Products
Zix Corporation

Daniel Z. Sands, MD, MPH
Clinical Director of
Electronic Patient Records
and Communication
CareGroup Healthcare System
and Beth Israel Deaconess
Medical Center

Assistant Professor of Medicine
Harvard Medical School

Joseph Scherger, MD, MPH
Professor
Florida State University
College of Medicine

Paul C. Tang, MD
Chief Medical Information Officer
Palo Alto Medical Foundation

Richard W. Whitten,
MD, FACP, MBA
Carrier Medical Director
for AK & WA Medicare
Noridian Administrative Services

Introduction	2
Section 1 The Opportunity for Using Email	3-5
Current usage of email	3
Benefits of using email	4
Managing the use of email	4-5
Section 2 Regulatory Requirements and Risk Management Issues	6-9
How HIPAA applies to email	6
Making decisions under HIPAA	7-8
HIPAA is not the only concern	8-9
Section 3 Use of Email in a Secure Environment	10-11
Section 4 HealthyEmail Guidelines	12-14
HealthyEmail program guidelines	12
Recommended administrative policies	12-13
Recommended patient policies	13
Improving the effectiveness of your email program	14
Section 5 The HealthyEmail Program	15



This primer is divided into five sections:

1. An overview of the opportunities for using email in healthcare
2. A review of the regulatory and risk management issues related to using email
3. A discussion on what comprises secure email communications
4. A guide for managing your electronic communications program, including policies, and procedures
5. Information on the HealthyEmail program

Introduction

Protecting the privacy and confidentiality of patient information has always been a hallmark of the healthcare industry in the United States. It is an important part of the foundation of trust for which our profession is known.

Until recently, communication of patient health information has been on paper or orally, either in person or over the telephone. The introduction of electronic mail – email – combined with the distribution capabilities of the Internet is revolutionizing the way patients, clinical practitioners, and other providers are communicating.

Clinical practitioners, in general, have been slow to jump on the email bandwagon; but use of email by healthcare professionals is growing, and those who use it say it is becoming a key communications tool for them and their staff.

That's good news because email is a valuable communications tool. Email is easy to use for all parties and offers many opportunities to improve the distribution, speed, comprehension, and tracking of communications. Patients, in particular, are becoming more interested in improving communications with their healthcare providers through use of email for non-emergency communications.

Various regulations, such as those issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), impose requirements applicable to email communication of patient health information transmitted over the Internet. HIPAA does not prohibit the use of the Internet or email to communicate private health information, but does require the individuals and organizations it regulates to assess the risks of using email and to take steps to reduce or eliminate those risks.

Entities regulated by HIPAA include all healthcare providers, health plans,

and clearing houses. HIPAA does not specifically regulate physician-to-patient communications but it is just good business practice to extend the procedures you implement for regulatory compliance to all of your business communications.

A lack of resources, time, and skills can make it difficult for already busy clinical practices to adequately address the issues of privacy and security of email. The increasing number of proprietary secure email systems many hospitals and insurers are promoting only aggravates this problem. It is easy to become confused by the complexity of the new regulations, technical issues of available systems, and the lack of standards.

We've launched HealthyEmail to address these issues and bring the industry together to develop and adopt best-in-class universal standards and practices. We also want to help guide you through the complexity and inconvenience that often comes with searching for the right security solution. Therefore, we've written this primer to specifically help you and your staff make an informed decision about the use of email in your practice, to help improve the effectiveness and efficiency of your electronic communications, and to help you comply with the HIPAA regulations. In future communications, we will be providing additional updates and information relating to topics such as reimbursement for doctor/patient consultation over the Internet, and integration of email into electronic medical records.

Whether you or your office utilizes the secure communications solution provided by HealthyEmail, we believe this primer will help you better understand the issues, benefits, and risks of using email in a clinical practice setting.



SECTION 1 The Opportunity for Using Email

Current usage of email

Using email to communicate with patients, partners, and other providers can be a practical, inexpensive, and convenient way to improve care giving and practice management.

However, nothing in the electronic world is as simple as it first appears – and use of email brings both a learning curve and a reminder of our tremendous responsibility to ensure the privacy and security of the information entrusted to us. You should consider using email only when you are comfortable with the idea and the technology. We think you will quickly be glad you made the decision to do so.

Most of the healthcare industry has readily embraced email with insurance companies communicating with its members and hospitals communicating with patients. Clinical practitioners, however, have been slower to adopt this communications tool. For example, while estimates of the number of clinical practitioners in the United States who use email already vary widely, it is likely that fewer than 15 percent of all clinical practitioners use email in their practice regularly.

This is in direct contrast to the explosion in consumers' use of email for a wide range of purposes. Email is widely popular among consumers and used by millions on a daily basis. More than 75 percent of American adults now access the Internet from their home, office, school, library, or elsewhere. Email usage makes up a large part of the time people spend online.

It is becoming more difficult for clinical practitioners to avoid adopting a communications tool preferred by so many of their patients. In a recent Harris InteractiveSM study, 90 percent of people already online said they would like to be able to communicate with their doctors online. More than two-thirds of them would like to be able to do each of the following:

- Ask questions when no visit is necessary (77%)
- Fix appointments (71%)
- Refill prescriptions (71%)
- Receive the results of medical tests (70%)

More than half of the online respondents said their ability to communicate online would influence their choice of doctors.

Why aren't more clinical practitioners using email regularly? It isn't easy to change routines in an already busy work environment and some simply don't feel they need it. Many see the addition of new technology as an uncomfortable burden, and are also often concerned about time and reimbursement issues.

In reality, healthcare professionals who use email regularly find the time commitment is not great and that email helps improve the work processes in their office. Email is an asynchronous technology – meaning you and the recipient of the communication do not need to be communicating at the same time, like you would in a telephone conversation. Use of email can help bring about an end to "telephone tag." And you can respond to email at a time when it is convenient to you. Email also provides an automatic record of the communication, so you do not have to create separate notes to document it.

“Currently, half the population in the United States uses email, and yet only 15 percent of physicians use email regularly to communicate with their patients.”

Dr. Daniel Sands
Advisory Board member

Some of those who do not use email may feel using it creates a legal liability issue. There is no case law to this effect and doctors who use email often say the reality is likely to be quite the opposite. The ability to easily put a copy of an email into a patient's medical file provides a much more accurate record of what was communicated than handwritten notes created after a conversation. A complete and accurate record of communications with a patient removes doubt about what was communicated and can help avoid malpractice claims. And, patients with whom we communicate more may feel their concerns are being addressed more personally and effectively, and be less inclined to resort to lawsuits to address issues.

Benefits of using email

Healthcare professionals already using email to communicate with patients, other doctors, payers, and hospitals say email:

- Improves patient, doctor, and staff understanding and satisfaction; strengthens patient relationships; and encourages more patient participation
- Provides immediacy of communication; no need to wait for the mail or connect for a telephone call
- Increases opportunities for information sharing; allows easy attachment of other electronic documents
- Reduces number of telephone calls and pages made and received
- Saves time; email can be quicker than an in-person conversation or a telephone call; some doctors say you can expect to receive about one email a day for every 100 patients you have using email
- Allows for communication at more convenient and calm times for both sender and recipient
- Frees up schedules and improves access for patients who really need to see the doctor by reducing non-essential office visits of other patients

- Avoids illegibility problems of handwritten communications
- Allows for easy routing to the most appropriate responder on your staff
- Saves patients from having to take notes on such things as names, contact information, instructions, and test results; they, therefore, don't need to repeat the same questions later; they can also review your messages later and discuss them with family and friends, thereby increasing their comfort and understanding
- Contributes to more cost-effective patient care
- Improves staff communications and allows for ease of communications with other providers using email
- Allows for the development of new business through online consultations for which a fee can be charged

Managing the use of email

As with any new practice, especially a technical one, there are risks that need to be understood and managed. The important risks that may arise in using email for clinical purposes include:

- Potential breach of confidentiality, such as interception by hackers or by unauthorized people seeing emails on a computer screen or printed copies in your office or in the patient's home or workplace
- Delayed response because the recipient hasn't checked his or her email
- Possible inequity of communications practices for patients who do not use email
- Outdated information issues, especially old email addresses
- State licensing issues when communicating with someone outside of your state; state laws may further restrict what information can be communicated via email
- Reduced revenue through fewer in-person consultations



- Increased number of hours of work
- Inappropriate use of email for emergency or time-sensitive issues
- Lack of patient understanding that can result from the lack of nonverbal cues
- Need for enough identifying information in the email to allow it to be filed in the medical record (paper or electronic)
- Inability to know whether the email was read by the intended recipient

Because of these kinds of risks, you should not try to adopt email for clinical purposes unless you first:

- Establish proper policies and procedures to safeguard patient information
- Properly train yourself and your staff
- Establish informed consent before communicating with a patient electronically
- Address technical security issues by using a secure network or encryption

The benefits of email usage generally outweigh the risks and all clinical practices should consider using email – if not today – at least in the near future.

SECTION 2

Regulatory Requirements and Risk Management Issues

These days, every healthcare practitioner and organization has to be concerned with privacy and security issues affecting patient information. New Privacy Regulations are coming into effect under HIPAA (the Health Insurance Portability and Accountability Act of 1996), and final HIPAA Security Regulations have recently been published. At the same time, news reports about healthcare organizations experiencing computer system security breaches and patient privacy violations have become all too common.

HIPAA compliance and more general privacy and security concerns are important factors for clinical practices considering adoption of email. Unfortunately, too much of the discussion about HIPAA privacy and security is superficial and even misleading, and provides no useful guidance. Therefore, it is important to clarify how HIPAA compliance, and other privacy and security risk management needs, apply to the use of email in healthcare.

How HIPAA applies to email

When people talk about HIPAA they are usually referring to both the HIPAA legislation, which was passed in 1996, and to a number of other regulations issued by the U.S. Department of Health and Human Services (HHS) as directed by the legislation. HIPAA is a complex set of laws that covers many subjects, most of which are not important to the use of email. Two sets of regulations, the Privacy Regulations and the Security Regulations, do matter to email.

The Privacy Regulations have had the most attention, and were published in a series of proposals and amendments over the last two to three years. They are now in their final form (though they could be amended in the future) and compliance is required by April 14, 2003. A draft of the

Security Regulations was published in 1998, and the final version has just been published. Compliance with the Security Regulations will be required no later than April 2005.

The Privacy Regulations do not specifically deal with email, and the Security Regulations do not address it in specific terms. The way that these regulations apply to email is by their requirement that healthcare organizations "safeguard," that is, protect, patient information. This requirement applies to all information that can be identified to an individual patient and has anything to do with his or her health care. Information subject to this requirement is called Protected Health Information or PHI.

The Privacy Regulations do not specify the exact safeguards that must be adopted to protect PHI. This decision is left to the informed, reasonable judgment of the healthcare organization based on the services it provides, the technologies it uses, the risks to PHI created by use of those technologies, and the organization's financial and administrative resources. Organizations are expected to take these kinds of factors into account to make "scaleable" decisions about the safeguards they will adopt.

The requirement for this kind of analysis is spelled out in more detail in the Security Regulations. The Security Regulations specifically require healthcare organizations to assess their PHI-related security risks, and implement appropriate safeguards to address those risks. These requirements apply to PHI in all electronic systems, including email.

The Security Regulations do not state that email encryption is mandatory, but do specify that encryption is an



"addressable specification" for controlling access to PHI. An "addressable specification" is a safeguard which is not required, but which must be considered, and implemented if it is a reasonable and appropriate safeguard. If a decision is made not to implement an addressable specification, the organization must "document why it would not be reasonable and appropriate to implement" and "implement an equivalent alternative measure if reasonable and appropriate."

An organization considering the use of email must:

1. Identify and assess the risks associated with using email,
2. Decide whether encryption is a "reasonable and appropriate" safeguard given the identified risks, and either
3. Adopt encryption, or
4. If encryption is not adopted, identify the reasonable and appropriate alternative means of addressing which solution will be adopted, and document the reasons why the alternative was a better option than encryption.

This analysis is consistent with the informed decision-making process required for safeguards under the Privacy Regulations. While compliance with the Security Rule will not be required until April 2005, its standards and required approach to compliance is good guidance for making decisions for Privacy Regulation compliance as required starting April 2003.

Making decisions under HIPAA

In deciding how to manage email risks to PHI, your first consideration is whether your clinical practice should adopt email to provide or support services to patients. If you do not adopt the technology, you will not be exposed to the risks. Therefore,

if you are not willing to invest at least some amount of time, money, or attention to establishing practice standards and policies for managing your email, this may not be a service you should provide. Only if you have decided email would be a worthwhile service and only if you are willing to make some investment to do it right, should you move on to the next consideration.

Second, once you have decided to adopt email you need to consider the risks it poses and how you will address them. Generally speaking, the main risk in using email is that an unauthorized individual can intercept the message. This interception might happen deliberately while the message is being transmitted, for example by a hacker, who might read or even change the message. More often it happens by accident when the message is sent to the wrong email address or an unauthorized person, like a spouse or co-worker, gets access to an email account.

These kinds of risks were well known to the drafters of the HIPAA regulations. The draft Security Regulations in particular addressed these risks by requiring Internet email users to encrypt their messages, and establish processes to "authenticate" message contents (i.e., to make sure they have not been altered). This was changed to a non-mandatory "addressable specification" in the final Security Regulations, with commentary from HHS indicating that the adoption of practices and technologies posing risks to PHI would call for encryption:

... Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. Covered entities are



encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet.

As business practices and technology change, there may arise situations where electronic Protected Health Information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.

The adoption of email for routine healthcare communications is precisely the kind of new business practice and technology adoption which leads to situations creating risks of unauthorized PHI access. Therefore, while encryption is not mandatory, it is clearly strongly favored by HHS. A decision not to encrypt email will need to be documented and very well-reasoned, especially as encryption solutions, such as the one offered as part of the HealthyEmail program, become interoperable, more affordable, and simpler to use.

Compliance with the Security Rule is not yet required, but it would be prudent to use its approach in developing the "safeguards" required for compliance with the Privacy Regulations as of April 2003. The Privacy Regulations have a specific provision requiring the use of "appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information." A failure to comply with this provision could expose an organization (or individual healthcare professional) to civil penalties, and could even be a basis for potentially even severe criminal penalties if the failure to comply leads to an unauthorized use of disclosure of PHI.

Use of encrypted email is a prudent practice for HIPAA Privacy and Security Regulations, even if it is not technically required. It represents a "technical safeguard" which the drafters of the HIPAA regulations have already recognized as appropriate for sending PHI over the Internet. Under the "addressable specifications" approach required by the Security Regulations you should adopt email encryption unless you have determined that it is not reasonable and appropriate, adopt any alternative which you believe is a more reasonable and appropriate means of addressing the same risks, and document the basis for your decision.

This leads to the third consideration in determining whether encryption is the right solution to email risks: Whether there are encryption products or services that are reasonable and appropriate given your organization's financial and administrative resources. A cost-effective solution which delivers strong encryption and reliable delivery to the correct addressee within the scope of your available resources can be an acceptable HIPAA compliance solution. The point is to maintain an "appropriate technical safeguard" against known risks of Internet email.

HIPAA is not the only concern

HIPAA compliance is not the only regulatory or risk management consideration in the use of email with patients. State laws may apply and might impose different or additional requirements, though to date it appears this is not an issue in the area of email use. Clinical practices that use computers, especially computers connected to the Internet, need to recognize and manage financial and operational risks associated with these technologies quite apart from email or HIPAA compliance considerations.

This kind of risk management would generally include prudent system access controls, such as passwords or other



solutions for authorized user access, firewalls to keep out hackers, anti-virus software, computer use policies and the like, which are important issues but beyond the scope of this primer.

However, there are some risks specific to clinical care uses that need to be taken into account.

In particular, clinical practices need to avoid using email for uses that might compromise the quality of patient care, such as diagnosis or emergency advice. It would simply not be prudent medical care, for example, to try to diagnose the reason for chest pain and an appropriate treatment based on email rather than an actual examination. Patients need to know and understand the limitations of email. While it may be a valuable service for many uses, there are some situations

in which it is not appropriate. As a risk management and patient relations matter, it will be important to manage patient (and practitioner) expectations in using email.

HIPAA and state law compliance and computer system and clinical risks can and should be managed by adoption of appropriate policies and procedures by any practice that chooses to adopt email. Email users need to understand how the systems work and what they are good for, and how to work with them to safeguard PHI.

Technologies such as encryption are a necessary part of this solution, but they are not sufficient. Informed decision making and establishment of suitable policies and procedures are needed as well.



SECTION 3 Use of Email in a Secure Environment

While the ubiquity and cost effectiveness of using email is enabling clinical practitioners to extend their communications reach, improve response times, and save capital and operational budget, these activities also pose both privacy and security risks.

These risks include:

- Unauthorized interception of messages in transmission
- Receipt or retrieval of messages by unauthorized persons
- Inappropriate physical security measures
- Destruction of data via electronic attack or viruses

The fact that risks exist does not mean the Internet cannot be used for the transmission of information, including Protected Health Information (PHI). But as with all other areas covered by HIPAA's Privacy and Security Regulations, it does mean appropriate safeguards must be used.

HIPAA regulations are specific about the end result required if you use email – health information sent via email must be protected against unauthorized access. However, the rules are less specific about the technologies to be used to accomplish this. No particular technology is required, so a wide variety of options have emerged.

Choosing among the alternatives is a matter of your using properly informed business judgment based on your particular circumstances, resources, and needs.

In general, you should select a secure email solution that:

- Ensures privacy by allowing you to send information securely to anyone with an email address, regardless of their platform or software
- Is consistent with HIPAA requirements for protection of PHI in electronic communications by providing prudent safeguards, such as encryption and authentication
- Works universally with all of the individuals and entities with whom you communicate
- Ensures messages arrive unaltered and can only be opened by the intended recipient
- Is interoperable with other existing technologies
- Causes no disruption to operations and works seamlessly with your existing email software
- Is inexpensive, easy to install, and easy to use
- Will grow with you as your practice grows; this is known as scalability
- Helps you to develop your risk assessment and provides a process for identifying and addressing your security risks
- Provides technical support you can count on

“I believe that if healthcare practices are not offering an email option, they will not be attractive to an increasing number of patients. Having secure email and the ability to communicate at the patient’s convenience is going to be critically important.”

Dr. Joseph Scherger
Advisory Board member



The available alternative solutions include closed networks, Virtual Private Networks (VPN), Public Key Infrastructure (PKI), outsourced PKI, passphrase encrypted mail, and symmetric key services. While all of these options provide adequate and appropriate message security, the disadvantages of these options individually far outweigh the benefits. Disadvantages of all of these technologies include lack of interoperability and scalability, expense, maintenance, and complexity.

We believe the most appropriate solution is a blend of two of the alternatives, outsourced PKI and symmetric key services. These two technologies together meet the broadest range of secure external communications. This combination of services is the only massively scalable solution that delivers the best configuration of cryptography, or encryption, solutions to reach the broadest audience of recipients.

The solution offered by HealthyEmail delivers the best-in-class blend of encryption technologies and ease of use benefits to meet the needs of every clinical practitioner and is already widely adopted by the healthcare community. The HealthyEmail solution is being offered free of charge for two years so that you can explore the benefits of email in everyday communications without obligation. For more information on the HealthyEmail security solution visit our Web site at www.healthyemail.org.

SECTION 4

HealthyEmail Guidelines

This section presents the first version of our guidelines for establishing a HealthyEmail program. We will update and expand these guidelines and our recommended policies, procedures, and patient education materials on a frequent basis over the coming months as we continue to develop best-in-class standards and tools. Adopting these tools should significantly simplify and accelerate the process of implementing a comprehensive and prudent email program.

HealthyEmail program guidelines

Following these guidelines will help you establish prudent safeguards and help ensure you are in compliance with all privacy and security regulations.

- Establish procedures to minimize the risk of unauthorized access and distribution of patient information. This includes policies about who receives and distributes emails in your office and how you protect the privacy of those communications.
- Gain the informed consent of patients interested in communicating with you by email and document the fact that you have explained your safeguards, policies, and procedures.
- Address all state laws on the maintenance and filing of clinical communications and records that apply to your practice. Be aware that communicating via email with a patient outside your licensing jurisdiction may pose a risk.
- Add physical safeguards to your computer equipment and network, including back-up systems. Make sure computers are locked up; passwords are in place, not shared and are changed frequently; and that systems auto log users after periods of inactivity.

- Create clear, written administrative procedures for use of email between you and everyone you will be communicating with – patients, other doctors, consultants, payers, and other third parties.
- Never use a patient email list for group promotional mailings or other unsolicited email. Never give or sell the list to a third party.
- For fee-based online consulting activities, establish separate and clear guidelines for the type of consulting you will do and the fees you will charge. Hold an informed consent meeting with patients before beginning such a relationship.

Recommended administrative policies

- Decide how many email addresses you want to use. You can have one email address and assign one person to handle all emails; or you can have one email address and use a “triage” approach, whereby the person who receives all the emails distributes them to others on your staff who can best address the issue. Another option is to have several email addresses that go directly to the appropriate responder, such as yourself, your office head, and your billing person. Remember that having several email addresses and/or distributing email among various computers can increase your security risks. Create very specific policies about the flow of emails, who has access to them, and the safeguards you are establishing about the routing of emails in your office.
- Determine your standard for turnaround time for responding to emails, such as “within two business days” and communicate that goal to your patients. One recommended practice is to read emails at a set time every day, such as the same time you return telephone calls.

- Build accountability for all email administration into your staff job descriptions. Add email privacy and security statements to the confidentiality agreements your employees sign. Be clear about who will answer, print, file, delete, redirect, back-up, maintain, and protect the emails you receive and send. Set up contingency procedures for when people are out of the office, including you. Train your staff on your new email procedures and make sure they understand the consequences for not following the procedures.
- Save a copy of all emails you send and receive in the patient's medical file, whether your files are paper-based or electronic.
- Clear out your email system frequently by archiving important messages and deleting old messages.
- Create a master address list of all patients with whom you exchange emails and store in a secure place.
- Avoid leaving email messages on unattended computer screens. Use password protected screen savers.
- Decide with your staff the topics that should never be communicated via email. Also communicate this information to your patients.
- Do not deliver bad or sensitive news or complex information via email.

Recommended patient policies

- Always discuss with interested patients the opportunities email presents. Ask patients about their communications preferences and note it in their file.
- Discuss with a patient in person the benefits of the new federal requirements for privacy and security and your email policies, procedures, and safeguards. This is an "informed consent" discussion that should be documented in the patient's clinical records. You can document this discussion in one of two ways. You can create a pre-printed form that you sign, date, and place in the patient's file.

Or, you can have the patient sign an informed consent agreement to be placed in their medical file.

- Produce a sheet of guidelines to give or send to patients who wish to communicate via email with you. The sheet should explain the safeguards of participating in the HealthyEmail program, your policies and procedures, and tips on when to use email.
- Tell patients specifically who will see and process their emails on a routine basis and on a special basis, including when you or staff are out of the office or on vacation.
- Secure a patient's permission before sending an email about that patient to a third party.
- Take special precautions if you answer email from home. Do not allow family members to see messages and do not print messages at home and store them there. Do not send email from an unsecured home account, as the information will not be protected and the different address could confuse patients who might reply directly to that address thinking it had gone to your office. Do not allow your staff to send or receive business emails at home.
- Inform patients if they do not follow the policies and procedures you have established, you will terminate the email relationship with them.
- Make sure information you provide is truthful and credible. This is especially important if you are attaching documents created by other people or are suggesting a patient read information on a Web site link. You are responsible for the information you communicate.
- Don't hesitate to escalate an email discussion to a telephone call or office visit. Email is no substitute for a physical exam.
- Ask patients to inform you of changes in their email address.

Improving the effectiveness of your email program

The following tips are provided to help improve the effectiveness of your email communications:

- Create descriptive and professional email addresses that are intuitive – dr.janejohnson@email.com or dr.johnson.officemanager@email.com
- Take all reasonable precautions to ensure your email goes to only the person you intend. Double-check any email address you type. Remember that some email programs will “complete” email addresses for you, by inserting the address closest to the first several characters you type before you are done; this may or may not be the person with whom you wanted to communicate.
- Put a short descriptive statement in the subject line of the email, such as “Your prescription has been refilled.”
- Start the body of the message with the word “Confidential,” the date, patient’s full name, address, and medical identification number.
- Close all emails with an “electronic signature” that includes your name, address, telephone number, and email address.
- Create a closing statement that reminds recipients of the importance of privacy and that email is to be used for only non-emergency communications. Also indemnify yourself by informing recipients you are not responsible for loss of information due to a technology failure.
- Set up an automatic reply, so the patient will know you’ve received the message. In the automatic reply, state your turnaround policy. Ask the patient to send a reply email to acknowledge they have read your message.
- Send another reply message when a request has been completed.
- Reply with the prior message attached or quote it so the patient knows what specific message you are replying to.
- Take the time to compose a concise message. Write as simply as possible avoiding complex terms or medical jargon. Always be professional in tone.
- Create passwords if they are not already required by your network or encrypted email system.
- Use attachments judiciously and be sure the electronic format you send them in allows the patient to easily view the attachments. Most medical documents are not in electronic form and have to be scanned or retyped. Be aware that scanned documents can take up a lot of space on your computer system.
- Send group messages only if there is a need to alert patients to something important, such as a change in your office hours or a system shutdown. Put your own name in the “To” section of the email and put all of the patients’ names in the “bcc” section. This ensures the recipients will not see each other’s names.

SECTION 5 The HealthyEmail Program

HealthyEmail is an outreach program for clinical practitioners created to address everything we've discussed in this primer. Our goal is to diminish the complexity of the issues and risks surrounding the discussion on email in the healthcare profession; and to develop and adopt industry standards to help guide clinical practitioners and their staff in all areas of email usage – from the email security solution to education tools and recommendations on how to create and implement an email program that is right for you.



Posters for your waiting room to help educate your patients.

Patient education brochures give your patients an overview of the "do's and don'ts" of communicating with you via email.

HealthyEmail benefits include:

- Access to an award-winning secure email application, ZixMail™, and full technical support. Up to three free licenses are available to every physician in the United States for two years. This secure email application adheres to the guidelines outlined in the HIPAA Privacy and Security Regulations. It provides a mechanism to send secure email from your existing email address to any receipt with an email address, including patients, other doctors, payers, and hospitals, regardless of their own email platform or software. Patients who wish to send you secure emails may sign up at <http://messages.healthyemail.org>.
- A range of education materials, including this primer
- Best-in-class guidelines for establishing your email program

For more information on all that HealthyEmail offers you, visit our Web site at www.healthyemail.org.

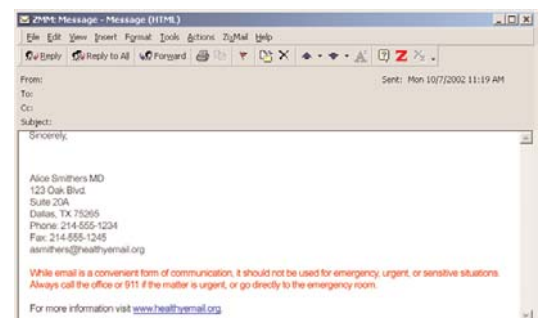
Dr. Alice Smithers
Internal Medicine

123 Oak Blvd.
Dallas, TX 75265
asmithers@healthyem

Email guidelines:

1. Only use email for non-emergency situations
2. Be concise
3. Include a descriptive topic in the subject line (i.e. appointment request, medical question)
4. Include your name and patient record number in the first line of the message body
5. All email exchanges will be filed in your record
6. Other appropriate staff members may read your email messages

Use this label on the back of your business or appointment cards to reinforce the guidelines for email.



Email signatures are provided to remind patients of the importance of privacy and that email is to be used only for non-emergency messages. Your contact information also appears at the close of every email.