physician connection

PSIC | Professional Solutions INSURANCE COMPANY

Protecting Reputations ... One Doctor at a Time®

PROFESSIONAL SOLUTIONS INSURANCE COMPANY BRINGS YOU PRACTICAL TIPS FOR AVOIDING A MALPRACTICE ALLEGATION ISSUE 1 • 2013

E-mail, Internet, Texting … Oh My!

New options for communicating in a physician's office often mean new risks.

The HIPAA Security Standards require practices to protect the privacy of patient health information (PHI). However, patient safety and privacy can easily be jeopardized through electronic devices. Consider the following examples:

Scenario 1: A long-time patient emailed her cardiologist to report a potentially serious side effect of a newly prescribed cardiac medication. The physician had told the patient to contact him *immediately* if she experienced any symptoms after starting the drug therapy.

This patient and her cardiologist had routinely communicated via email between office visits. However, the day she emailed him, the cardiologist was out of town attending a conference. The practice had no system in place for checking the physician's incoming emails in his absence.

The patient had been found nonresponsive the evening she sent the email and rushed to the hospital by ambulance *in extremis*. By the time the cardiologist returned and read her email, the patient had been hospitalized. She never fully regained consciousness and died four days after the physician returned.

Scenario 2: A student nurse in a family practice clinic was observing a suture removal by a nurse practitioner as part of her on-the-job training. Unbeknownst to the nurse practitioner, the student was videotaping the procedure with her cell phone. She later sent it to another student in her class just to show him: "How cool is this?!" That student posted it on Facebook.

Regrettably, the student/videographer had taken no precautions to conceal the patient's identity, and the patient's face was clearly shown. The online video eventually was seen by the patient who sued the practice for breaching his privacy and confidentiality, and he filed a HIPAA violation complaint.

Scenario 3: An on-call pediatrician was called by the ED about a 10-month-old boy who had a seizure-like spell earlier that evening. The parents witnessed that the child's body had suddenly stiffened, and he had a fixed stare for more than one minute. The pediatrician responded with verbal orders, and he reported that he was on his way to the ED, arriving in approximately 10 minutes.

The patient began to deteriorate, and the staff sent a text to the physician to let him know. Due to confusion at the front desk, the staff mistakenly texted this message to *both* the pediatrician and the patient's mother.

While the pediatrician was still en route to the hospital, he received a frantic phone call from the boy's mother. She screamed at the physician asking why he wasn't at the hospital with her son but rather driving around in his car. She demanded that another physician intervene on the boy's behalf before the pediatrician arrived at the ED.

Email Communications with Patients

As the first scenario shows, parameters must be established in the practice for how email will be used. For example, this situation might have been avoided had the physician had an out-of-office message reply on his email.

It is essential that PHI remain secure, patient care and safety is uncompromised and practice policies are communicated with staff. There should also be a disclaimer on emails that patients should not rely on emails to communicate time-sensitive matters.

Just as patients are asked for their contact information, they should be asked at their first visit whether the practice may communicate with them via email. These preferences should be checked regularly to ensure the patient's email address or communication preferences have not changed. It can be helpful to address the following issues before allowing email for patient communication:

Continued on Page 2

Continued from Page 1

Smart phones have raised the potential for breaching patient confidentiality.

SAMPLE POLICY/CONSENT FORM FOR PRACTICE EMAIL

XYZ MEDICAL GROUP
PHYSICIAN-PATIENT EMAIL COMMUNICATION POLICY

To better serve our patients, XYZ Medical Group has established an email address our patients may use to communicate with the practice and its physicians. It is just one of several communication options we make available to our patients.

Our Policy: Patients of XYZ Medical Group have the option of communicating with our physicians, physician assistants and nurse practitioners (list names as appropriate) by email. Prior to doing so, we ask that you review this policy sheet and sign it below.

Please note that copies of all email communications between you and this practice will be placed in your medical records and treated like other information contained there.

When sending an email to this practice, use our email address, info@xyzmedicalgroup.com. Please include your full name and patient ID. (Many email programs don't automatically include your name.) In addition, please include the subject of your message in the subject line, so your email may be processed and routed efficiently.

You may email us for routine matters that do not require an immediate response. Do NOT use email communication in emergency or urgent situations. Please use the office phone, XXX-XXX-XXXX, or dial "9-1-1." Also, for your privacy, some issues (e.g., AIDS or HIV, mental health, substance abuse, work-related injuries or disability) are not appropriate for email discussion. Communication appropriate for email include: scheduling, billing or insurance questions, test and lab results, prescription refill requests, and non-urgent medical advice.

XYZ Medical Group will send you an automatic notice when your email has arrived. If you don't receive this notice within ____ (specify applicable length of time, e.g., two business days), please call the main office. Also, any email sent to you by XYZ Medical Group will arrive with return receipt requested, so we will know when you received it. Our physicians generally answer emails within ___ (specify length of time, e.g., two business days). If you need a quicker answer, please call the main office rather than emailing us. If the physician you are emailing is out of the office and unable to answer your email in the normal timeframe, we will automatically alert you.

XYZ Medical Group is committed to keeping your medical information private, including any information sent to us by email. However, email security cannot be guaranteed as messages are transmitted via the Internet. For that reason, please do not use email for anything you want kept confidential.

If you have any questions about these policies, please ask _____ (Dr. X, the office manager or one of the other staff, as appropriate). If you understand our email policy and would like to add email to the ways you communicate with us, please sign and date below and return it to our office staff.

Signed _____ Date _____

[Note: this sample form reflects the AMA Guidelines for Physician-Patient Electronic Mail, AMA Policy: H-478.997.]

- Which members of the staff will be permitted to use email for patient communication.
- Who will be allowed to see patient emails (other than the intended recipient).
- What will be the information the patient is required to include in emails to the practice.
- What hours will emails to the practice be answered (e.g., will emails be read only during normal office hours?).
- When and how will patient consent to communicate via email be obtained and stored.
- What will be the practice turnaround time for emails, including confirmation of receipt and response.
- What issues may or may not be addressed via email.
- When should the practice be contacted via alternative methods (e.g., in emergencies or situations that require a prompt response).
- What systems need to be in place to protect patient confidentiality and security of PHI (e.g., passwords, encryption and patient authentication).
- What email communication will become part of the patient's medical record, and how will this information be backed up, stored, retrieved and retained.
- How can patients be educated to protect their own confidential patient information, e.g., do not share their email address and/or electronic device with others.
- What will be the consequences of patient noncompliance with the practice's email policies and procedures.

Once a practice decides to allow physician/patient emails, the practice should modify its internal policies and procedures to include responsibilities for:

- Monitoring the practice's email account.
- "Triaging" or routing emails to the intended recipient.
- Assuring patient emails are answered within the practice's published turnaround time.
- Archiving the emails to include email communications to and from the patient in the record.

Smart Phones/Electronic Devices

Some physician practices provide their physicians and administrative staff with smart phones and unlimited-use plans as an employee benefit.

Policies for the staff's personal use of these e-communication devices are often broadly structured, e.g., sometimes limiting it to "reasonable use." Other practices specifically state that noncompliance—especially for breaches of patient confidentiality—will result in disciplinary action, including immediate dismissal.

The use of these devices raises the potential for breaching patient confidentiality and violating HIPAA greatly. The most obvious threat is associated with the physical loss or theft of a device. The National Institute of Standards and Technology considers cell phones at "high risk for loss, theft, disposal and unauthorized access." The Institute has developed "Guidelines for Cell Phones and PDA Security" (see Resources). Once lost or stolen, patient confidentiality is at risk if these devices contain PHI and encryption is not in place. This can result in a HIPAA violation.

The importance of the physical safekeeping of electronic devices containing PHI cannot be overstressed. Devices not in use but containing PHI should be kept in the practice under lock and key. Employee policies regarding these devices should include what to do in case of loss or theft of any device that contains PHI.

In addition, as shown in the second scenario, there are security risks when personal devices are brought into the practice. As such, the following questions should be addressed before allowing employees to use electronic devices on the job:

- Are policies in place that establish who owns the device?
- Are policies in place to safeguard patient privacy? This should include policies to secure the device (password/access numbers are enforced).
- Are devices protected against viruses, hacking and malware?

- Do they have encryption features if PHI is accessed and transmitted?
- Can data be wiped remotely if a device containing PHI is lost or stolen?

Texting

Texting has obvious appeal in that it is fast, easy, available, inexpensive and succinct. Studies have demonstrated that unlike email, most text messages are read by the recipient and responded to quickly (usually within three to five minutes of receipt). And, text messages are viewed as much less obtrusive and annoying than a phone call.

A recent study by the Pew Research Center and the California Health Care Foundation reported that the use of cell phones to obtain health information is expected to grow rapidly.[1] Although only nine percent of users currently receive health information via text, this is likely to change as text messaging becomes universally accepted.

Physicians have quickly embraced texting as an easy way to communicate with colleagues and staff. Many are using texting with patients for appointment reminders, medication reminders, preventive health notices and other health information.

However, as illustrated by the third scenario, there are obvious limitations and potential risks to consider with text messaging. These include:

- A lack of encryption, for both sending

SAMPLE POLICY CHECKLIST FOR E-COMMUNICATIONS

The following checklist, though not all inclusive, may be incorporated into the practice's confidentiality policies or adapted as a stand-alone e-communications policy.

Email

- ☐ Obtain patient consent for email communications. Keep on file and reconfirm it at least annually. [See Sample Practice Policy/Consent Form for Email.]
- ☐ Develop a confidentiality statement to include with all emails. For example:
  The information in this email may be privileged and confidential, containing protected health information, which is protected by federal privacy regulations. It is intended only for the individual to whom this email is addressed. If you are not the intended recipient or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If this communication has been received in error, please notify the sender at XXX-XXX-XXXX or by replying to this email to arrange for return or destruction of the information received.
- ☐ Include an auto-reply, receipt verification system to ensure the intended person has received incoming and outgoing emails and will obtain a timely response. The system should stamp the date and the time of the receipt and response. If the recipient is unavailable, the system should send an out-of-office message, along with the contact person for immediate assistance. Out-of-office messages are also recommended, with instructions on who to contact if the intended recipient is unavailable, or if the patient's email is received when the office is closed.
- ☐ Implement a process for routinely check emails in compliance with the practice's turnaround time policies.
- ☐ Require staff to print out and file patient email correspondence (to and from) in the patient's medical or billing record, as applicable.
- ☐ Advise staff that practice emails may be monitored and accessed at any time, disclosed to law enforcement providers or other third-parties, and discoverable in a malpractice or professional discipline action.

Smart Phones and Electronic Devices

- ☐ Place encryption and antivirus security software on practice-owned devices. Password protect and include a recovery mechanism on these devices.
- ☐ Establish policies for downloading PHI or other sensitive information on any devices not practice-owned.
- ☐ Establish policies for the use of practice-owned devices for anything non-practice related, whether in the office or during personal time.
- ☐ Consider a policy prohibiting photography or videotaping at least in patient areas. The policy should apply to patients, visitors, vendors and staff and be prominently posted in waiting and patient areas.
- ☐ Address the use and safekeeping of these devices in HIPAA educational programs. Practice staff should understand how PHI confidentiality breaches occur and what to do in the event of a breach.
- ☐ Require any cell phones or electronic devices be placed on vibrate or silence mode during patient encounters or in situations where a ring tone could be viewed as rude, intrusive and/or unprofessional.
- ☐ Caution staff to abide by all regulations for practice-owned cell phones while driving (e.g., hands-free devices only, texting while driving prohibitions, etc.).

Texting

- ☐ If the practice elects to provide texting as a patient communication choice, include the option on the initial patient intake form and train staff to regularly reconfirm the patient's communication preferences. If possible, include an "opt-out" option on all texts sent from the practice.
- ☐ Use devices equipped with encryption and other safeguards. Keep in mind, however, that for encryption to work both sending and receiving devices must have encryption in place.
- ☐ Do not send patient-specific information or identifiers in e-communications. Keep information generic and vague to prevent a HIPAA violation if the message is read by someone other than the intended recipient.
- ☐ Caution staff to abide by all regulations on practice-owned devices while driving (e.g., texting while driving prohibitions, etc.).

Social Media

- ☐ Establish clear guidelines for the use of social networking sites, such as Facebook and Twitter, to protect the reputation and privacy of the practice, its physicians, and staff. The guidelines should apply both to on-the-job and after-hours use.
- ☐ Encourage employees to use their personal email address rather than the practice's email. Remind employees that the practice will monitor web access and emails sent and received on its electronic devices.
- ☐ Advise staff not to post photos or any information about a patient (even without naming the patient) or any practice-related event involving a patient or a staff member.
- ☐ Prohibit employees from revealing confidential or proprietary practice information and consider banning even the use of the practice's name or logo in a post.
- ☐ Caution employees that their personal activity on social networking sites must be clearly distinguishable from their professional life (must not be perceived as representing the practice or its physicians).
- ☐ Encourage staff to report any postings or photographs about the practice, physicians, staff or patients.

General

- ☐ Have a back-up communication plan for all patients, and make sure contact information includes more than phone numbers and email addresses. Contact information can change, not be in service, and power and Internet outages can disrupt patient communication efforts.

Six Tips for Safer Texting

By observing the following safeguards, physicians can help minimize the risks associated with text messaging and maximize the benefits for their practices:

1. **Use a secure text messaging service.** Companies like TigerText and Doximity provide secure text messaging services. Both the sender's and the receiver's phones must be equipped with encryption capabilities to comply with HIPAA.
2. **Avoid including PHI in your text messages.** This includes patient identifiers, diagnostic information or test results. For messages to patients, follow the HIPAA guidelines for voicemail messages (e.g., leave only the appointment time and the clinic phone number). For medication reminders, consider simple messages like "remember your regimen."
3. **Ask patients to opt-in to receive your text messages.** Require patients to sign a written authorization for you to text message them, and be sure they understand regular text-messaging fees will apply.
4. **Delete, delete, delete.** Though the messages may still remain with the service provider, having them removed from your phone reduces the risk of unauthorized access to patient information.
5. **Review before sending.** This simple step helps ensure your message is received as intended.
6. **Set boundaries.** Explain that you may not be able to respond to texts immediately.

Source: Podolsky, L. Physician Texting: pitfalls & pointers. Medical Office Today (online) March 6, 2012. ©2012 Feral Chick Media LLC
www.medicalofficetoday.com/article/physician-texting-pitfalls-pointers?page=0,1

and receiving messages, can result in PHI breaches and HIPAA violations.
- Unlike emails, there is no retrievable record of a text message exchange to enter into the patient's record.
- There is an inherent expectation that text messages are read and responded to promptly.

Most text messages are read and responded to quickly.

- Text messaging is not secure—messages can be intercepted and read during transmission.
- Size limitations may impede the inclusion of sufficient clinical information.
- The use of abbreviations in a text may be misinterpreted.
- Texting is inherently casual and personal—not necessarily good features for a physician/patient relationship.
- Spell checks and auto-correction features can create problems, particularly with medical terminology or drug names that are not recognizable by the device software.
- The device used to text is prone to loss or theft.

Risks with All E-Communication

The AMA Guidelines for Patient-Physician Electronic Mail states: *"New communication technologies must never replace the crucial interpersonal contacts that are the very basis of the patient-physician relationship. Rather, electronic mail and other forms of Internet communication should be used to enhance such contacts.*

In this regard, the practice should assess its potential benefits and risks, and then determine which e-communication would be most efficient and effective. Once the issues have been analyzed, the practice can develop policies and procedures that best meet the needs of the practice while protecting patient confidentiality.

[1] Pew Internet/CHCF Health Surveys. Mobile Health 2012. November 8, 2012. www.pewinternet.org/~/media//Files/Reports/2012/PIP_MobileHealth2012.pdf

Resources

American Medical Association
https://ssl3.ama-assn.org/apps/ecomm/PolicyFinderForm.pl?site=www.ama-assn.org&uri=%2fresources%2fdoc%2fPolicyFinder%2fpolicyfiles%2fHnE%2fH-478.997.HTM

AMA Policy: E-9.124 Professionalism in the Use of Social Media
www.ama-assn.org/ama/pub/meeting/professionalism-social-media.shtml

Centers for Disease Control & Prevention
Social Media Tools, Guidelines & Best Practices
- Facebook Guidelines and Best Practices
- Twitter Guidelines and Best Practices
- Button and Badge Guidelines and Best Practices
- Health-e-Card Guidelines and Best Practices
- Text Messaging Guidelines and Best Practices

www.cdc.gov/SocialMedia/Tools/guidelines/?s_cid=tw_eh_78

Federation of State Medical Boards
Model Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice, Report of the Special Committee on Ethics and Professionalism, 2012
www.fsmb.org/grpol_policydocs.html#2012

National Institute of Standards and Technology (NIST)
NIST Guidelines for Cell Phone and PDA Security (S.P. 800-124)
http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

NIST Guidelines Updates for Mobile Device Security (S.P. 800-124, Revision 1). Proposed update to Guidelines for Cell Phone and PDA Security released for comments July 2012.
http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Ohio State Medical Association
Social Networking and Medical Practice: Guidelines for Physicians, Office Staff and Patient
www.osma.org [Search "social media"]

Scan to visit the risk management section of psicinsurance.com

PSIC | Professional Solutions INSURANCE COMPANY

Send all inquiries, address changes and correspondence to:
Physician Connection, P.O. Box 9118, Des Moines, IA 50306
Toll-Free 1-888-336-2642
Internet – www.psicinsurance.com
Email – riskmanagement@psicinsurance.com