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.

PSIC | Professional Solutions INSURANCE COMPANY

www.psicinsurance.com

P.O. Box 9118, Des Moines, IA 50306