Table of Contents

Introduction .................................................................................................................. pg.3

Policies for Your Practice ............................................................................................. pg.4

1. Sample Social Media and Electronic Communications Policy ................................pg.4
   Provides guidelines for your employees who use social media and social
   networking websites, and who communicate with patients by email or text.
   It incorporates criteria set forth by the AMA and additional guidance from other
   health care sources.

2. Sample Patient Portal Policy .............................................................................. pg.6
   Provides parameters for communicating with patients via a patient portal.
   Also provides enforcement terms to ensure employees’ compliance with
   the policy.

3. Sample Patient Portal User Agreement and Informed Consent ...................... pg.7
   A plain-English policy to help you inform your patients about the portal and
   explain the requirements for their participation in using the portal.

4. Sample Electronic Communication User Agreement and Informed Consent .... pg.9
   Practices should provide this policy to patients when the practice does not have
   a patient portal, but has the ability to communicate electronically with patients.

5. Sample Social Media Policy for Practice-Sponsored Social Media ............. pg.10
   Contains all the provisions of the first policy plus additional prohibitions to serve
   as notice to practice employees.

Example Scenarios ...................................................................................................... pg.12
These examples illustrate a variety of social media scenarios you may encounter when
you incorporate social media into your practice.

Social Media Scenarios ............................................................................................... pg.12

Patient Portal Usage Scenarios .............................................................................. pg.13

No Patient Portal Scenarios .................................................................................... pg.14
Introduction

The Illinois State Medical Society (ISMS) has developed five social media policies and sample workplace scenarios to help guide you as you incorporate new media to promote your brand, disseminate information, and remain current with patient needs and wants.

Social media applies to user-created video, audio, text, photo, or other media that are published and shared in a social environment, such as a blog or micro blog, wiki, social network, instant messaging, video hosting site or other communication platforms.

The information presented here is intended to assist you with protecting your patients’ interests and applying principles of ethical medicine when using social media. Also addressed is how your medical practice staff should be advised to handle communications with patients, colleagues and employers when using social media.

Due to the largely unsecured nature of social media, confidential information can reach a wide audience, and health care professionals and patients alike may be unaware of inappropriately crossing boundaries. These policies are not intended to minimize a practice’s current communication or behavior standards and policies, but rather augment such policies with a framework for using technology and social networking in the delivery of health care.

Use of Social Media, Patient Portals and Text Messaging in Your Practice

To ensure that your patients’ private health data is protected as you incorporate social media into your practice, ISMS recommends that you keep the following in mind:

- Social media sites do not have HIPAA compliant services.
- Staff must follow existing rules and laws on privacy and ethical behavior.
- Enforcement of the policies provided in this document will limit risk to patients and your practice.

With regard to communications taking place through a patient portal, via text messaging or email, ISMS recommends that:

- You consult with your EMR vendor and reach a decision concerning the issue of recording, maintaining and storing these communications as part of the patient’s medical record. Please note that we recommend electronic communications related to patient care be maintained as part of the medical record.
- If you do allow email communications with patients or sponsor a portal, those communications should be considered part of the patient medical records and subject to all applicable law.
- Email communications with patients and staff containing medical data be conducted over a secure, encrypted system.

With respect to text messages, please note that as of 2011 the Joint Commission disapproved use of text messages to relay orders from physicians to hospitals. Text messaging is inherently unsafe if it is conducted on personal devices that may not be secured in compliance with the data security policies of your practice. For this reason and others, we recommend that no clinical information be used within any text messaging system.

The issue of text messaging is directly related to the use of mobile devices (cell phones, tablets) for communications and data storage and transmission. Be aware that cell phone cameras, risk of loss of mobile devices, limited keyboard functionality impacting complex passwords and a general failure in the health care industry to encrypt mobile devices must be anticipated and risks managed. Capabilities to remotely wipe data, use of app-specific virus protection and authentication should all be addressed to assist your practice to mitigate risk. It is important to realize that your patient’s devices may have none of the security or privacy protections you require for your practice staff.

Patients do have the right under HIPAA to identify alternative means of communication. Consult your legal counsel if you receive a patient request for an alternative with which you are uncomfortable, such as use of unencrypted email or text messaging.

Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice is an instructive document provided by the Federation of State Medical Boards, written especially for those with a minimal understanding of social media. Physicians may access a copy of this additional resource at http://www.fsmb.org/pdf/pub-social-media-guidelines.pdf.
SAMPLE Social Media and Electronic Communications Policy

PURPOSE

[Practice name] supports the use of social media and electronic communications, but wishes to use this media consistent with ethical principles governing the patient-physician relationship, confidentiality, privacy and respect. In observing these principles, PRACTICE will minimize the risk to the company and its employees. At all times, employees of [practice name] shall use social media in a manner consistent with this organization’s mission, values, administrative policies, and all applicable laws, privacy regulations, and confidentiality standards. It must be clear that the information provided by [practice name] on these platforms is intended for educational purposes only. It is not an endorsement, nor is it a substitute for professional medical advice, diagnosis, or treatment.

NO INFORMATION POSTED ON ANY SOCIAL MEDIA IS PRIVATE. USE OF PRACTICE SPONSORED SOCIAL MEDIA IS SUBJECT TO A SPECIFIC POLICY.

“Social media” should be understood to include any internet websites that allow users to connect, comment, reply, rate or post information, including pictures or videos, in addition to social networking, blogging, online forums, media sharing sites, cell phone photography, electronic searching, texting, and e-mailing. Examples of such websites include but are not limited to Facebook, Twitter, YouTube, Vimeo, LinkedIn, Yelp, Spoke, and blogs in general. Social media does not include patient portals.

“Electronic communications” means e-mail or text messaging with patients outside of a patient portal.

The term “patient portals” refers to the part of [practice name’s] information system that provides access to patients’ health information and allows for secure communication, including prescription, referral and appointment requests.

BEST PRACTICES

1. Use common sense – anything you say can be discovered.
2. Remain vigilant – monitor your personal page.
3. Be respectful and transparent – you represent your practice and the medical profession.
4. Maintain boundaries online as you would in the office, and do not interact personally or socially with patients through unsecured electronic communications.

POLICY

All employees of [practice name] agree to:

1. Comply with standards of patient privacy and confidentiality. Employees shall not post any identifiable patient information online except in a practice sponsored communication, such as a patient portal. At no time may the employee disclose any patient identifiers, such as name, date of birth, geographical information, etc. Breaches of patient confidentiality must be reported immediately to [practice name’s] Compliance Officer.

2. Maintain separate personal and practice social media content. [Practice name’s] employees should not connect with patients or the patients’ families on their personal social media websites. Accepting invitations to connect with patients or patients’ families through the employee’s professional social networking website is acceptable. Employees should refrain from sending out invitations to connect. This is not meant to prevent employees from connecting with patients who are also family members of employees. In those instances, employees should refrain from engaging in discussions about the patient family member’s health care over social media.

3. Use privacy settings for their personal and professional social networking websites. Note: A professional social networking page is one that represents the person as a professional and employee of [practice name]. Content on such pages should be strictly related to that employee’s role at [practice name].
4. Observe all ethical boundaries and guidelines while connecting with patients through the employee’s professional social media websites.

5. Never post in response to unfavorable comments on health care rating websites. Do not post anonymous comments supporting [practice name] in response to patient grievances. If a defamatory comment or complaint is posted, bring the matter to the attention of the Compliance Officer. Leadership with [practice name] will decide on the response or action, if any, such as contacting the host site advising them of the defamatory comment or contacting the patient directly. Responses should be objective, and an attorney should be contacted when appropriate.

6. Use disclaimers when posting about health care topics on personal and professional social media websites. An example of a proper disclaimer: “The views expressed here are solely the author’s and do not represent the opinions of [practice name].” Additionally, if you list [practice name] as your employer on a personal social media website, you will need to add that disclaimer as well.

7. Inform the Compliance Officer if a colleague’s social media behavior is inappropriate.

8. Recognize that behavior on social media websites reflects not only on the individual, but on their colleagues, [practice name], and the medical profession.

9. Never refer to financial or other relationships you may have with professionals of products or services, and never refer to products or services of third parties that you discuss or review online.

10. Refrain from discussing patients anonymously even if you are able to disguise references to symptoms, conditions etc. DO NOT PROVIDE MEDICAL ADVICE OR COMMENT ON MEDICAL ISSUES THROUGH SOCIAL MEDIA WEBSITES OR OTHER WEBSITES SUCH AS HEALTHTAP. This could be construed as practicing medicine and forming a doctor/patient relationship. Additionally, this behavior potentially violates HIPAA.

11. Recognize that anything said or otherwise posted on social media websites is in the public domain and potentially subject to discovery.

12. Never post anything that is defamatory, profane, libelous, threatening, harassing, abusive, obscene, knowingly false or otherwise inappropriate.

13. Never comment on legal issues involving [practice name].

14. Post only your original creations. Do not share copyrighted publications, logos or other trademarked images, unless by express, written consent. Providing a link to the creation of another is acceptable, as long as the employee does not misleadingly present the content as his/her own.

15. Never email or text message a patient from a personal email address or phone number. Emailing a patient should only be done through [practice name’s] patient portal or practice email. This is not meant to apply to personal communications with family members or friends done through a personal email address or phone number. The patient’s medical care should not be discussed over personal text or email.

16. Use email only when in compliance with the Practice’s security and/or encryption technology requirements, for communications between providers within and outside the Practice.

17. Use common sense: If in doubt, do not post it.

ENFORCEMENT

All employees of [practice name] agree to adhere to this policy. Violation(s) of this policy are grounds for disciplinary action and may include termination of employment and reporting to law enforcement or professional regulators.

Employee name

[Practice name] President or CEO

Employee signature

[Practice name] Pres/CEO signature

Date

Date
SAMPLE Patient Portal Policy

PURPOSE

[Practice name] understands the need for communication between health care professionals and patients. [Practice name] is committed to providing patients and other authorized personnel the ability to use a secure and confidential patient portal that provides access to [detail what will be available here. Optional: medical records, appointment desk, secure communication with health care professional]. The [portal name] utilizes technology to deliver secure communications between patients and [practice name].

The term “patient portal” refers to the part of [practice name’s] information system that provides access to patients’ health information and allows for secure communication, including prescription, referral and appointment requests.

“Electronic communication” means email or text messaging with patients outside of a patient portal.

POLICY

1. Correspondence via patient portal is supplemental to health care professional/patient encounters.
2. Reasonable care must be taken to authenticate the identity of the correspondent(s) and ensure the recipients of information are authorized to receive it.
3. Before using the patient portal, health care professionals must obtain informed consent from patients regarding appropriate usage, limitations and risks inherent with this technology.
4. Secure email messaging with patients is for non-emergent situations.
5. Discussion of sensitive subject matter is not permitted (HIV/AIDS, STDs, mental health, behavioral health, drug treatment, genetic information, etc.).
6. All electronic communication with patients should occur through a practice sponsored patient portal.
7. Responses to communication received from a patient through the portal or other electronic communication method should be sent within two business days.
8. Information about a positive or abnormal test result must be discussed directly with the patient, either over the phone or in person and not through a patient portal.
9. The use of patient portals is only appropriate with established patients who have given informed consent.
10. A health care professional must determine the physical location of a new patient before engaging in discussions, either through the patient portal or other electronic communications.

ENFORCEMENT

All employees of [practice name] agree to adhere to this policy. Violation(s) of this policy are grounds for disciplinary action and may include termination of employment or criminal or professional sanctions.

Employee name [Practice name] President or CEO

Employee signature [Practice name] Pres/CEO signature

Date Date

This is for educational purposes and is not intended as nor should be considered legal advice © 2014 Illinois State Medical Society
Patient information

<table>
<thead>
<tr>
<th>Name</th>
<th>DOB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email address</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Patient portal basics

[Practice name] understands the need for communication between health care professionals and patients. [Practice name] is committed to providing patients and other authorized personnel the ability to use a secure and confidential patient portal that provides the following functionality:

1. Access to [detail what will be available here. Optional: medical records, etc.]
2. Ability to contact the appointment desk.
3. Secure communication with health care professional.

The [portal name] utilizes technology to deliver secure communications between patients and [practice name].

The term “patient portal” refers to the part of [practice name’s] information system that provides access to patients’ health information and allows for secure communication, including prescription, referral and appointment requests.

“Electronic communication” means e-mail or text messaging with patients outside of a patient portal.

Patient portal policy

The following policies and limitations apply to the use of [practice name’s] patient portal.

1. Patient portal communication is not for emergency purposes. If you are having an emergency, dial 911 or go to your local hospital.

2. Correspondence via patient portal is supplemental to physician/patient encounters. [Practice name] will not provide patient portal-based diagnosis and treatment.

3. Sensitive subject matter, such as HIV/AIDS, STDs, mental health, behavioral health, drug treatment, or genetic testing information cannot be discussed through the patient portal.

4. Other electronic communication with the health care professional, such as non-patient portal email or text messaging is prohibited.

5. Communications sent via patient portal must be courteous, respectful, appropriate, fact-based and truthful.

6. Communications should be responded to within two business days. You agree not to use this portal if you need a response sooner or on an urgent basis. If your need is urgent you must contact the practice directly.

Patient portal policy continued next page
Patient portal policy continued

7. You agree not to share your password with anyone and that you are solely responsible for protecting your password.

8. You agree that access to the site is provided on an “as is available” basis and that our practice cannot guarantee you will be able to access the portal at any time. Internet based communications are inherently insecure since no technology guarantees privacy or security of information sent over the internet. You agree to use caution when providing information via this portal, and acknowledge that keeping messages secure is your responsibility.

Conditions of participation

Access to [patient portal name] is restricted to the above-named patient. This service is optional, and we reserve the right to suspend or terminate the service and/or your access to it at any time. If the practice suspends this service, you will still have access to copies of your medical record and other health information, upon request.

The patient acknowledges that he/she agrees to comply with the [practice name’s] Patient Portal Policy outlined above.

Patient name:__________________________________________________________

Patient signature:______________________________________________________

Date:______________________________________________________________
SAMPLE Electronic Communication User Agreement and Informed Consent

Purpose

Completion of this form is necessary prior to engaging in electronic communications with [practice name]. At current time, [practice name] does not have a patient portal through which [practice name] and patient may securely communicate.

Patient information

Name
DOB
Address

Email address
Telephone number

Electronic communication policy

“Electronic communication” means unsecured e-mail or text messaging with patients outside of a patient portal.

The following policies and limitations apply to the use of [practice name’s] electronic communication:

1. Electronic communication is not for emergency purposes. If you are having an emergency, dial 911 or go to your local hospital.

2. Correspondence via electronic communication is supplemental to physician/patient encounters. [Practice name] will not provide electronic communication-based diagnosis and treatment.

3. Sensitive subject matter, such as HIV/AIDS, STDs, mental health, behavioral health, drug treatment, or genetic testing information, cannot be discussed through electronic communication.

4. Communications sent via electronic communication must be courteous, respectful, appropriate, fact-based and truthful.

Conditions of participation

Electronic communication with [practice name] is restricted to the above-named patient. This type of communication is optional, and we reserve the right to suspend or terminate it at any time. If the practice suspends access, you will still have access to copies of your medical record and other health information, upon request.

The patient acknowledges that he/she agrees to comply with the [practice name’s] Electronic Communication Policy outlined above.

The patient also acknowledges and understands that any information conveyed using unsecured electronic communication is not protected and may be viewable in the public domain.

Patient name: ________________________________

Patient signature: ________________________________

Date: ________________________________
A practice-sponsored social media site typically allows patients to exchange comments among each other, for example, as part of a support group for cancer or bereavement. The fact that distinguishes public social media from private or sponsored social media is the control exercised over content. If the practice controls access to and content of the site, then it would be considered sponsored. In addition, the practice may sponsor sites that it does not control completely, such as a Facebook page. Controls over certain aspects of this format should still be exercised by the practice.

PURPOSE

[Practice name] sponsors social media and electronic communications, but wishes to use this media in a manner that maintains ethical principles governing the patient-physician relationship, confidentiality, privacy and respect. In observing these principles, PRACTICE will minimize the risk to the company and its employees. At all times, employees of [practice name] shall use practice-sponsored social media and electronic communications in a manner consistent with this organization’s mission, values, administrative policies, and all applicable laws, privacy regulations, and confidentiality standards. It must be clear that the information provided by [practice name] on these platforms is intended for educational purposes only. It is not an endorsement, nor is it a substitute for professional medical advice, diagnosis or treatment.

NO INFORMATION POSTED ON ANY SOCIAL MEDIA IS PRIVATE. USE OF PRACTICE-SPONSORED SOCIAL MEDIA IS SUBJECT TO THIS POLICY.

All employees of [practice name] agree to refrain from:

1. Postings of any kind except with approval of the Practice.
2. Posting material that infringes on the rights of any third party, including intellectual property, privacy or publicity rights.
3. Posting material that is unlawful, obscene, defamatory, threatening, harassing, abusive, slanderous, hateful or embarrassing to any other person or entity as determined by the Practice.
4. Posting of non-practice related advertisements or solicitations of business.
5. Posting chain letters, spam or pyramid schemes.
6. Impersonating another person.
7. Allowing any other person or entity to use your identification for posting or viewing comments.
8. Posting any confidential or proprietary information of the practice.
9. Posting solicitations for fundraising or charity purposes unless they comply with applicable HIPAA rules.
10. Posting content that is not their own without proper attribution. Employees should post only original creations. Do not share copyrighted publications, logos or other trademarked images, unless by express, written consent. Providing a link to the creation of another is acceptable, as long as the employee does not misleadingly present the content as his/her own.

BEST PRACTICES

- Use common sense – anything you say can be discovered.
- Remain vigilant – monitor your personal page.
- Be respectful and transparent – you represent your practice and the medical profession.
- Maintain boundaries online as you would in the office and DO NOT interact personally or socially with patients online.
The practice reserves the right (but is not obligated) to do any or all of the following:

- Remove communications that are abusive, illegal or disruptive, or that otherwise fail to conform with these policies.
- Terminate a user’s access to the social media upon any breach of these policies.
- Edit or delete any communications posted on the social media, regardless of whether such communications violate these standards.

In addition, all the elements of the Social Media and Electronic Communications Policy apply to the conduct of staff of the practice with respect to any social media sponsored by the practice.

**ENFORCEMENT**

All employees of [practice name] agree to adhere to this policy. Violation(s) of this policy are grounds for disciplinary action and may include termination of employment and reporting to law enforcement or professional regulators.

<table>
<thead>
<tr>
<th>Employee name</th>
<th>[Practice name] President or CEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee signature</td>
<td>[Practice name] Pres/CEO signature</td>
</tr>
</tbody>
</table>

| Date | Date |
The social media policy emphasizes prudence when both interacting with patients and developing a business identity over social media platforms. This approach will help physicians avoid ethical dilemmas and minimize risk.

The following examples are meant to provide real-life scenarios that may be encountered in a medical setting.

Social media scenarios

1. A patient “friends” his physician on Facebook. The physician only maintains a personal Facebook page, not a professional one. Is it appropriate to accept the friend request?

   No. The physician should ignore or reject the friend request, due to ethical implications. A solution to this issue is to set up a professional Facebook page. Additionally, the physician should update the privacy settings on his personal page to decrease the likelihood that a patient could find his personal page.

2. A patient posts a scathing review of a physician and her office staff on a doctor rating website, alleging incompetence and rudeness. An office staff member sees this review and decides to respond to this post. The staff member posts a polite response, apologizing for the unpleasant visit and inviting the patient to return to the office to discuss the incident further. Is this an appropriate response?

   No. Neither physicians nor their office staff members should respond to patient comments on websites of any kind. Although the response was polite, it was inappropriate to respond. Instead, defamatory content should be brought to the attention of the website where the review was posted. The practice may also choose to contact the patient directly to further discuss the incident.

3. Outside of work hours, a physician maintains a blog where he posts on a variety of topics, ranging from politics to pop culture to health care issues. In one post, the physician discusses a reality TV series on the recent rise in super morbid obesity and mentions that this issue has begun to affect his practice – just today, an 52-year- old obese man from Hammond came in and broke an examining table due to his size. Is this an appropriate post?

   No. The post contains a fair amount of detail about the patient and does not appropriately hide his identity. Additionally, blogs such as this are viewable by the public and casual or overly personal remarks can undermine trust in the profession.

4. A plastic surgeon posts before and after pictures of reconstructive surgery. The patients’ faces are obscured. Are these appropriate to post?

   Yes, as long as there is no identifiable patient information embedded in the picture, such as a file name that contains patient identifiers, and the patient gives his or her written permission.

5. On her professional Facebook page, an oncology nurse posts links to articles relevant to her area of practice. The links are to articles from sources such as the AMA and American Cancer Society. Is this appropriate?

   Yes, provided she is not representing the written works as her own.

6. Doctor X and Doctor Z are partners in the same practice and also friends on Facebook. Doctor X notices in her newsfeed that Doctor Z is now friends on Facebook with a current patient. Additionally, it is evident that Doctor Z has made inappropriate comments on some of the current patient’s photographs and writes suggestive comments on her wall. Doctor X mentions what she has seen to Doctor Z. Is this appropriate or an invasion of his privacy?

   This is appropriate. Unacceptable behavior on social media outlets should be discussed with the source. In this situation, Doctor Z does not have a fair expectation of privacy – he is holding out himself in a public arena.
Patient portal scenarios

The patient portal policy was developed in response to the need for secure communication with patients. It acknowledges that while a patient portal is a useful tool, it should only be used to supplement the traditional physician-patient relationship for active patients; patients who do not maintain an active, face-to-face relationship should not be allowed to communicate using a portal. If an inactive patient asks for permission to communicate through a portal that request should be denied. Note that an “active” patient is dependent upon specialty. While the general figure is two years, surgical specialties, for example, consider active patients as those seen within the past six months.

1. Main Street Medical uses a patient portal to schedule appointments, send reminders to patients, and notify them about the availability of test results. The office is constantly busy, and the portal makes it quick and easy for the staff to communicate with patients, as opposed to the slow process of using the telephone. Since they are so backed up, they have started notifying patients about all test results – negative, abnormal, positive – through the patient portal. Is this appropriate?

No. Although they are busy, abnormal and positive test results must be conveyed directly to the patient, either over the phone or in person. This is to prevent a failure to notify the patient, to assure that the patient is thoroughly informed about the results and has an opportunity to speak with a practitioner about the impact of the results and to schedule follow-up care.

Negative test results may be posted to the patient portal.

The patient must specifically consent to having his or her test results available through the patient portal.

2. A patient was recently seen at Main Street Medical and was diagnosed with an STD. When he got home, he realized he had more questions about his condition and sent them to his health care professional over the patient portal. The health care professional discussed his condition and treatment over the portal. Is this appropriate?

No. Discussion of highly sensitive information, including sexually transmitted diseases, is inappropriate through a patient portal.

3. A longtime patient of Main Street Medical is not feeling well and uses the patient portal to send questions to her health care professional regarding her current condition. The professional declines to answer her specific questions and instead recommends she come into the office for an appointment the following day. Is this appropriate?

Yes. Medical advice should not be dispensed over the portal.

4. Main Street Medical encourages patients to sign up for its patient portal, but in order to use it, patients must fill out an informed consent document. Some patients have complained about the number of documents they have to fill out at the practice, and claim that a verbal acknowledgement is good enough. Is it appropriate to use an informed consent document for patient portal use?

Yes, it is appropriate for the practice to have patients fill out an informed consent form; a verbal acknowledgement should not be utilized. This consent should be specific to the use of the patient portal, and should not be confused with other informed consents signed for other purposes.
No patient portal scenarios

Numerous practices have yet to acquire a patient portal service, and thus a policy on the use of unsecured patient communication is required. The policy delineates what qualifies appropriate communication.

1. Everytown Medical Group is located in a small, rural community and cannot afford to purchase a patient portal system. Some of the physicians in the group have email addresses, but they are not encrypted. Physician A’s wife is the office manager and patients often email her at her practice’s email address to set up appointments. Is this appropriate?

It is appropriate to book appointments this way, however, care and treatment cannot be discussed. Additionally, email encryption is encouraged. The practice should also have a signed Electronic Communication Use Agreement and Informed Consent form (see page 9).

2. Physician B is well liked and has numerous friends and acquaintances in Everytown, many of whom are patients. One of her patients is Patient 1, who is also her brother-in-law. Physician B texts Patient 1 to remind him about his upcoming visit. Is this appropriate?

While treatment of family members is not recommended, it is appropriate to text a reminder. The physician should follow the same procedure for all patients, including requiring a signed electronic communications policy agreement.

3. Patient 2 is a longtime patient of Physician C. Patient 2 will email Physician C to set up appointments. Physician C or his wife will respond, and in the response email will often ask about Patient 2’s family, recent vacations, recipes, etc. Is this appropriate?

No. There should be a distinction between professional and personal communications. Physician C should set up a professional email address and limit correspondence to business questions. For professional communications with patients regarding PHI, the evolving standard is to use encryption for email.

4. Patient 3 is a client of Everytown Medical Group and was recently diagnosed with schizophrenia. She does not know much about this condition and sends an email to Physician D with questions specific to her care. Physician D responds in a timely manner, gives her a basic outline of her care and treatment, and provides some helpful links to articles. Is this appropriate?

No. Discussion of sensitive medical information, such as mental health issues, is inappropriate over both email and patient portal. Instead, the practice should contact the patient and schedule a follow-up appointment.