the newsletter for physician office administrators

medical office manager™

volume XXVII, number 10 october 2013

HIPAA COMPLIANCE UPDATE

How to self-audit your compliance with the HITECH final rule … before feds do

Now that the Sept. 23 deadline has passed for compliance with the Omnibus Final Rule implementing the HITECH Act, you may think your job is done. But HITECH calls for audits of covered entities.

You shouldn't wait for a government audit to make sure you have done everything needed to comply with the final rule's changes. It's best to do your own self audits to check that you've done everything you need to do to bring yourself into compliance with the new rules.

Self-auditing is also a good way to spot potential compliance issues before they become problems. We've provided a handy checklist to make sure you've met all the requirements you needed to meet for Sept. 23.

Here, we'll explain why the final rule changes mean you should be auditing the items in our checklist.

reviewing the rule

As you know, the Omnibus Final Rule issued in January 2013 became effective in March with a Sept. 23, 2013 deadline for compliance with the obligations under the rule.

That rule expanded covered entities' obligation to protect patient's protected health information (PHI), imposed direct liability on business associates for violations of privacy and security rules and increased penalties for violations. Those increased penalties are a big reason you should be double-checking your compliance with the requirements.

Founder and president of First Healthcare Compliance, **Julie Sheppard** suggests practices need to focus on three things to make sure they satisfied their obligations for that Sept. 23 deadline: Notice of Privacy Practices (NPPs), Business Associate (BA) agreements and breach notification protocols. In a nutshell, that means you should review your compliance efforts to be sure:

1. Your updated NPP is disseminated and posted as required.
2. BA agreements are compliant and agreements needing updates were updated or are scheduled to be updated as required.
3. Breach Notification protocols are current.

(continues on page 3)

in this issue

Medical Office Manager (ISSN 1052-4894) is published monthly by Plain Language Media, LLC, 15 Shaw Street, New London, CT, 06320.

Subscription rate: $267/year; back issues are available at $10 each. Periodicals postage paid at New London, CT 06320. Postmaster: Send address changes to **Medical Office Manager**, P.O. Box 509, New London, CT 06320.

Opinions expressed are not necessarily those of **Medical Office Manager**. Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

this month's idea

Front desk moves its phones into a communications center

A Colorado manager has taken the telephones off the front desk and set up a communications center.

The noise, commotion and staff burnout at the front desk have ended. As a result the four-doctor, 16-staff office is able to see more patients in a day.

Before the change, the front desk was nothing short of frustrating. It was noisy with phones ringing. Worse, staff had to deal with never-ending interruptions. As they checked patients in and out, they had to answer calls. And then they had to put callers on hold to help patients at the desk.

So the manager of this practice cleared out a small room at the back of the office that's nowhere close to the reception area and put in three phones, three computer terminals and three staffers. One staffer answers the incoming calls and routes them. The other two are nurses. They triage calls, schedule appointments and handle prescription refills.

Setting up the center created staffing changes all down the line, but it also created efficiencies.

For example, the number of front desk staff was reduced from three to two. But because those staffers no longer answer any phones, they took on the job of posting daily charges and payments. The billing staffer who originally did the posting now has time to follow up on billing problems.

The manager also moved one nurse from lab and x-ray to the communications centre. The office found that lab and x-ray could be managed by only one person with the other nurse acting as backup.

Still another change was a new hire – the second nurse in the center. That means the nurses who work directly with the physicians don't have side work that keeps them from patient care. That means in turn the doctors can see more patients.

The patients benefit from the new communications center too. They say the waiting area is calmer and that they get more personal attention from the desk staff. When they call, there is no waiting for callback from a nurse.

If you have a system that makes your office run smoothly, **Medical Office Manager** *would like to write about it. Contact the editor:* barb@plainlanguagemedia.com.

We pay $100 for every idea we write about in this column ◆

(continued from page 1)

amended notice of privacy rules

Several omnibus final rule's provisions impact NPPs. So you need to make sure you covered all those items in your practice's revised NPP. "Definitely, the NPP is at the top of my list," says Sheppard, regarding issues that she addresses with clients when discussing compliance with the omnibus final rule.

For example, your updated NPP should address changes in the final rule regarding breach notification, disclosures to health plans, marketing and sale of PHI, and fundraising. Using the revisions to the rules and the discussion in the preamble to the rule, published in January, we've come up with the following items that you should be sure your NPP addresses so it is updated to incorporate the latest changes, clarifications and guidance in the final rule.

1. A statement that authorization is required for a) most uses and disclosures of psychotherapy notes, b) uses and disclosures of PHI for marketing purposes, and c) disclosures that constitute a sale of PHI.

2. Notice that individuals can opt out of fundraising communications (the fundraising communication will tell them how to opt out but your NPP could include those instructions as well).

3. Explanation that patients have the right to restrict disclosure of information to a health plan if the patient pays out-of-pocket in full for the health care item or service.

4. Notice that individuals have a right to be (or will be) notified of a breach of unsecured PHI (this statement doesn't have to include explanation of how the risk assessment will be conducted or other details of this obligation to provide notification breach but NPPs can include such information).

After you modify your NPP to comply with the new final rule, there are three more steps Sheppard advises practices must complete:

1. Make sure the revised NPP is visible in your waiting room.
2. Ensure your office has hard copies available to hand to patients.
3. Be sure to post the revised NPP on your website.

The preamble to the rule adds that providers can post a summary of the notice in a "clear and prominent location" if the full notice is "immediately available" for patients to pick up without having to ask for a copy. These are "basic but important steps," says Sheppard. That's because the changes in the final rule affecting the NPP are declared material changes which require distribution of new NPPs. As HHS noted in the preamble to the rule: "The modifications to [NPP requirements in] §164.520 are significant and important to ensure that individuals are aware of the HITECH Act changes that affect privacy protections and individual rights regarding protected health information."

Business Associate Agreement modifications

The big change with regard to business associate agreements is that now there are new groups that must enter into business associate agreements with covered entities:

1. Patient safety organizations and others involved in patient safety activity.

2. Health information organizations (e-prescribing gateways or health information exchanges) that transmit and maintain PHI).

3. Personal health record vendors.

So you need to ask the following questions to ensure you are complying:

1. Do you have relationships with vendors that didn't previously require a BA agreement but now do? If so, do you now have a BA agreement in place?

2. Did you make sure all BA agreements needing modifications were amended to comply with current final rule?

3. Did you check existing agreements for dates/renewals (if the agreement existed before Jan. 25, 2013, you may have until it is renewed or modified or until Sept. 22, 2014, whichever is earlier, to revise the agreement).

Your BA agreements must have been modified to include the following:

- A provision requiring assurances that business associates will comply with the HIPAA security rule and safeguard protected health information.
- A requirement that business associates report any security incident of which the BA becomes aware, including "breaches of unsecured protected health information."
- A mandate that BA's subcontractors enter into agreements requiring they protect security of PHI and report security incidents.

Breach notification analysis

After the NPP, some of the most significant changes address breach notification. Julie Sheppard warns that breaches are "now presumed reportable unless you completed a risk analysis." That risk analysis requires you consider four factors. If that analysis reveals a "low probability of PHI compromise" the presumption doesn't apply. This presumption is new, says Sheppard.

So you need to adjust your breach notification protocols to make sure you adhere to that presumption rule.

The four factors are:

1. Type and extent of PHI involved in the breach (sensitivity of information either financially (say for identity theft risks) or clinically (personal health information) and how likely is it the information can be identified or linked to a person;
2. Who gained unauthorized access to the information (and whether they have their own obligation to maintain confidentiality);
3. Whether the information was accessed or acquired (taken); and
4. What mitigation efforts were made—for example, did you get the unauthorized recipient to agree to maintain confidentiality?

Prior to the final rule, a subjective test evaluated whether there was "significant risk of financial, reputational or other harm." The final rule's preamble explaining the changes indicates you don't need to get a third party to do your risk analysis and you don't need to do the risk assessment if you decide to just give a notice of the breach. But the preamble indicates it wouldn't be wise to omit the risk analysis because you may be just leaving open the door to further breaches. Additionally, the preamble advises that patients only need to receive one breach notification so the notice can be coordinated by you and any business associate involved.

Policies and procedures addressing other rule changes

Complying with Nondisclosure Requests

Related to the breach obligations is a new requirement that providers honor a patient's request to not disclose PHI to a health plan if the patient agrees to pay out of pocket. Sheppard notes that, previously, physicians could refuse such requests but now the final rule says physicians must agree to the request. "You need procedures and protocols to make sure it in fact never gets reported," she recommends. For example, patients who come to the ER drunk may not want that visit reported and patients coming for STD tests or women coming for pregnancy tests may not want that reported, Sheppard explains.

This new requirement creates an opportunity for improper disclosure if your procedures or protocols make it easy for such information to be inadvertently or accidentally disclosed against the patient's wishes. Sheppard advises that your procedures should flag such information so it is never reported and track to make sure the restriction isn't violated.

Security vulnerabilities

"Get IT help to check for vulnerabilities in your security," suggests Sheppard. The final rule made technical revisions with regard to security but it's important that your practice obtain an IT specialist to review your systems for compliance. The rules clarified that security measures must be reviewed and amended when necessary to ensure compliance.

Marketing communications

New limitations on marketing communications prevent physicians from giving out marketing information to patients unless patients provide written consent. You can only tell patients about third-party products and services without consent if:

1. The physician isn't compensated for the communication.
2. The communication is face-to-face between patient and physician
3. The patient is already being prescribed the drug or biologic and physician only gets paid a reasonable reimbursement of the costs of communicating with the patient.
4. The communication is a general health promotion rather than promoting a specific product or service.
5. Communication involves government or government-sponsored programs.
6. This doesn't prohibit promotional gifts of nominal value (pamphlets).

The preamble explains that patient authorization is needed for all "treatment and health care operations communications" if the physician receives compensation from a third party relating to a product or service marketed. Given the difficulty in distinguishing "treatment versus a health care operations communication," the preamble recommends that patient authorization be obtained for "all subsidized communications that market a health related product or service." Although the NPP no longer must notify patients that the practice may contact individuals about appointment reminders, treatment alternatives or other health related benefits and services, if those actions involve financial compensation from a third party, the individual's authorization must be obtained, the preamble advises.

Permitted disclosures

The rule discusses and clarifies permissible disclosures in two circumstances which should be addressed in your policies and procedures:

- Providers can disclose childhood immunizations to schools if an informal agreement is made regarding the disclosure
- Providers can disclose information to deceased patients' families and friends if they could have disclosed that same information when the decedent was alive and the recipient of the information was someone who provided or paid for patient's care and the physician was not aware of a preference for nondisclosure.
- Providers can disclose PHI concerning a patient 50 years after patient's death.

RESOURCES

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, Jan. 25, 2013, Federal Register, Vol. 78, No. 17, pages 5566-5702

- http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

HHS Model NPP notices and instructions:

- http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

HHS Security Rule Guidance (conducting risk analysis, implementing safeguards)

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule

Audits

- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

Sample Business Associate Agreement

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Breach Notification Guidance Page

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

September 19, 2013 Compliance Delay for Laboratories:

- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/clia-labs.html

September 19, 2013 Refill Reminder guidance:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketingrefillreminder.html

September 19, 2013 Guidance on Decedents:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketingrefillreminder.html

September 19, 2013 Guidance on Student immunizations

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/studentimmunizations.html

Patient access to PHI

The rules have also addressed patients' right to access their PHI. So you should ensure your policies and procedures are up-to-date on these requirements.

- Providers must respond to requests for PHI within 30 days with one 30-day extension. There is no longer a 60-day period for providing PHI when records are offsite.
- Providers must provide PHI in electronic health record format or other electronic record form or format requested if "readily reproducible" in that format (or other mutually agreeable format). Hard copies are only acceptable if individual refuses all readily reproducible e-formats
- Providers can email requested PHI only if they advise the requesting party of the security risks of email transmissions and the party still wants it emailed.
- Costs charged for copies can now include labor costs (even skilled technical labor for electronic PHI) and supply costs for paper copies or portable media costs such as USB or CDs (unless state law sets lower reimbursement rate). Providers can also charge for providing an affidavit of completeness.

HIPPA

Compliance Checklist

Use this checklist to make sure you have complied with all the new and modified requirements in the HIPAA final rule:

Notice of Privacy Practices

☑ Addresses breach notification rules

☑ Discusses uses for which authorization is required

☑ Advises patients they can request nondisclosure to health plan if they pay out-of-pocket

☑ Addresses sale of PHI

☑ Advises patients they can opt out of fundraising related disclosure

☑ Explains right to notice of breach of unsecured PHI

☑ Amended NPP posted on website

☑ Amended NPP is posted in delivery site in "clear and prominent" location [or summary is so posted with full NPP available without request]

☑ Copies of NPP are available in office to provide patients requesting same.

Business Associate Agreements

☑ BAAs are entered into with all patient safety organizations and entities involved with patient safety, health information organizations (e-prescribing gateways or health information exchanges that transmit and maintain PHI), and personal health record vendors

☑ Require assurances that BAs will comply with HIPAA security rule and safeguard PHI

☑ Mandate that BAs report any security incident and breaches of unsecured PHI

☑ Require BAs to have breach notification policies and procedures

☑ Require BAs obligate subcontractors to comply with HIPAA and report any security incidents or breaches of unsecured PHI

☑ Require BAs to coordinate with your practice on provision of breach notification

☑ All agreements needing amendment prior to September 23 were amended

☑ Any agreements not required to be amended prior to September 23 are identified for modification before September 22, 2014

Security

☑ Review security measures to ensure continuous protection of PHI

☑ Check policies and procedures to be sure security efforts are documented

Breach Notification

☑ Check breach notification procedures to ensure they require risk analysis for any breach using four factors required

☑ Ensure BA agreements require BAs to have breach notification policies and procedures

☑ Ensure your BA agreements require BAs to coordinate with your practice on provision of breach notification

☑ Policy and procedure for flagging information patients request not be disclosed to their health plan (ensure information is segregated and tracked so can be sure it is never reported inadvertently)

Marketing Policies/Procedures

☑ Ensure policies/procedures require patient consent before marketing information is provided patients unless conditions satisfied (face-to-face, no compensation received by physician, etc.)

Access/Copies

☑ Do you have procedures for providing requestors access to their PHI, and for providing in the form required/requested

☑ Procedures require access/requested copies within 30 days

☑ Procedures require requested PHI be provided in format requested if readily reproducible in that format; hard copies only permissible if requestor rejects all readily reproducible formats

☑ Procedures prohibit email communication of PHI unless requestor is warned of risk of email security and still requests disclosure via email

☑ Procedures clarify permissible charges include labor, supply costs (to extent permitted by state law) and affidavit of completeness

Permitted Disclosures

☑ Do policies and procedures address disclosure of childhood immunizations to schools

☑ Have procedures regarding sharing information with deceased patients been updated to clarify disclosures can be made to family/friend of deceased regarding PHI related to the death

☑ Do disclosure policies indicate PHI may be disclosed 50 years after patient's death

BILLING

10 accurate acronyms ensure you get paid

Medical coding is primarily numbering, but acronyms are also important for accurate billing. Here are 10 of the most common. Keep this list handy for reference:

CMS (Centers for Medicare and Medicaid Services)—Division of the United States Department of Health and Human Services that administers Medicare, Medicaid and the Children's Health Insurance Program.

EDI (Electronic Data Interchange)—Electronic systems that carry claims to a central clearinghouse for distribution to individual carriers.

EOB (Explanation of Benefits)—Document, issued by the insurance company in response to a claim submission, that outlines what services are covered (or not) and at what level of reimbursement. Each payer has its own EOB form.

HIPAA (Health Insurance Portability and Accountability Act-Law)—sometimes called the Privacy rule, outlines how certain entities like health plans or clearinghouses can use or disclose personal health information.

HMO (Health Maintenance Organization)—Health management plan that requires the patient use a primary care physician who acts as a gatekeeper.
INN (in-network)—A provider who has a contract with either the insurance company or the network with whom the payer participates.

OON (out-of-network)—An out-of-network provider is one who does not have a contract with the patient's insurance company.

POS (Point of Service-Health insurance plan)—Offers the low cost of HMOs if the patient sees only network providers.

PPO (Preferred Provider Organization)—Health management plan that allows patients to visit any providers contracted with their insurance companies. If the patient visits a non-contracted provider, the claim is considered out-of-network.

WC (Workers' Compensation)—U.S. Department of Labor program that insures employees who are injured at work.

ELECTRONIC WORKPLACE

Why you need an employee social networking

THIS STORY WILL HELP YOU … Prevent employee blogging, texting, tweeting,

At least some of your employees are into blogging, tweeting, Facebook and other social networking. What employees do with their free time is their own business.

Or is it?

What about employees who social network during work time? And how about employees whose blogs, tweets and Facebook postings come from home but still do damage to your doctors, patients and practice? As manager, it's incumbent on you to protect the medical practice from harmful social networking by employees. Here's how:

Defining the Terms—What is Social Networking?

Social networks are services that use software to build online communities of people who share common interests. Members typically create their own profiles and interact with each other via chat, messaging, video, file sharing, blogs, discussion groups, etc. There are two basic kinds of social network:

- An internal social network (ISN) is a closed, invitation-only community whose members usually come from the same company, society, association, school or organization; and
- An external social network (ESN) is a public community open to web users. The best known social networks, including Facebook, Twitter and Pinterest, are ESNs.

The "social networks" we talk about in this article are ESNs, not ISNs.

8 Ways Employee Social Networking Can Hurt Your Practice

Employee social networking can actually be a positive thing to the extent employees use it to exchange professional guidance and pick up tricks of the trade that help them do their jobs better. But, it can also do a lot of harm:

1. Productivity Losses

The greatest risk to business posed by social networking is lost productivity. Anyone who has at least dabbled in the experience can understand how addictive social networking can be and how easily it can suck up your time. What may be intended as a simple exchange can suddenly turn into a day-long interaction. And, of course, many employees choose to do their social networking at work.

The productivity losses resulting from these diversions are only beginning to be measured. For example, a 2007 BBC report cites a recent study that reveals that social networking could be costing UK employers an average of about £130 million in lost productivity – per day!

2. Threats to Business Confidentiality

One of the things people like to talk about is their jobs. And in a social context, they tend to speak candidly. When such conversations occur face-to-face or on the phone, they're generally kept private. But keeping such interactions private is more problematic when they occur online, especially within an ESN. Just about anybody who has access to the Internet can join an ESN and get in on the conversation. Consequently, work-related conversations by employees on social networks can create big problems for employers.

One of the most serious risks is that employees will disclose confidential information about the practice or the business. For example, the employee might express concern to her Facebook chum that her clinic is talking to a hospital about selling off the business unit she works for. The disclosure may not be a deliberate attempt to disclose a business secret. The employee may simply not know that the negotiations with the hospital are highly sensitive and must be kept secret. But even if the indiscretion isn't ill-intentioned, once the information is out in cyberspace, the damage is done.

policy to help protect your practice

emailing and other social networking abuses

3. Undermining of Management

Complaining to friends about work, bosses and colleagues is an ancient and largely harmless social tradition. But when it happens online, it's not so harmless, even if the whole conversation takes place while the employee is off duty and at home. In a cyberworld, gripes get expressed in the form of inappropriate postings, pictures and jokes about doctors, patients, colleagues and the like online where anybody can see them.

In addition to harming morale and collegiality, such communications can expose the practice to risk of liability for harassment, discrimination and other violations. They also can be a form of insubordination or insolence.

Example: In her blog, a hospital RN referred to the nurse who supervised her as "Nurse Ratched"—the nurse from hell in *One Flew Over the Cuckoo's Nest*. Although the employee didn't use her name in the blog, she didn't bother to hide the fact that she worked as a nurse for a hospital in a particular county that had only one hospital. Result: It was pretty easy to figure out the identity of the blogger and the supervisor the "Nurse Ratched" comment was directed at. An arbitration board ruled that the hospital had just cause to fire the employee for insubordination.

4. Harm to Practice's Reputation

Employees might also say unflattering things or post inappropriate material or videos on their networking page about the medical practices, doctors or patients they serve. The negative things employees say on social networks and blogs can undo your practice's reputation and standing in the community.

5. Violations of Patient Privacy

Employees may disclose patient records and other protected information in the course of their social networking. In addition to violating HIPAA, these transgressions can undermine the doctor-patient relationship.

6. Discrimination and Harassment of Other Employees

Employees don't only talk about their bosses and employers in their blogs or social network posts; they also talk about their co-workers. Comments made about co-workers in an employee's blog could constitute harassment or discrimination and expose your practice to liability. For example, an employee may make inappropriate sexual comments about or use a racial epithet to describe a co-worker.

Employees may also download, view or transmit pornographic, racist and other offensive material from the Internet at work in violation of your harassment or discrimination policies. Many a practice has had to deal with the situation of employees emailing, tweeting or texting pornographic or objectionable material to a colleague. And, of course, simply working in a cubicle next to a co-worker who views porn or exchanges smut with co-workers can be extremely offensive.

7. Liability for Illegal Activities

Employees may conduct illegal activity on the Internet at work, such as distributing child pornography or downloading material in violation of copyright law. And there's no shortage of legal theories that can be used to hold your practice liable for such activities especially when employees use your computer and network to conduct them.

Explanation: Prosecutors may argue that your practice, by providing the opportunity and the means to engage in illegal activity, condoned it and so is "vicariously liable" for it. That argument is particularly compelling if you knew about the employee's activities and did nothing to stop them.

8. Harm to IT Infrastructure

Employees who use the Internet for unauthorized purposes often introduce viruses, worms, Trojan horses and the like into the practice's information network, causing serious problems for the IT infrastructure. Use of the office network for personal business—especially when many employees do it at the same time or when an employee downloads a large file—can also slow down the system and make it harder for other employees to use the network to do their jobs.

3 Ways to Prevent Social Networking Abuses

In addition to establishing the legal grounds for discipline, establishing clear and specific social networking policies will deter misconduct in the first place. Three effective strategies used by cutting edge employers:

1. Address Social Networking in Confidentiality Agreements

Like many practices, you may ask employees to sign confidentiality agreements banning them from disclosing confidential information. If it doesn't already say so, add language to your agreement requiring employees to abide by their confidentiality obligations while engaging in social networking and other forms of online activity. Spell out that revealing sensitive organization information on an online social network at home is just as unacceptable as doing it in a business communication during work.

Example: A skilled nursing facility has a confidentiality agreement banning employees from talking about facility residents outside the facility and warning of discipline for revealing names or information that could be used to identify residents. A caregiver is fired for discussing personal information about facility residents and even posting a photograph of a resident on her personal blog. An arbitrator dismisses her grievance, finding that the caregiver's conduct constituted insubordination and violated the facility's confidentiality policy as well as the standard of conduct for employees caring for nursing home residents.

2. Address Social Networking in Codes of Conduct

Most practices have standards of conduct banning forms of unacceptable behavior, both on and off-duty, such as harassment, bullying and bad mouthing bosses, customers and the organization. Indicate that these forms of misconduct are equally unacceptable and subject to discipline on a social network or other online activity.

Example: The arbitrator in the above case found the caregiver's blogging about residents "unbefitting" and a violation of the facility's standard of conduct requiring caregivers to respect the privacy and confidentiality of residents.

3. Set Specific Policy on Employee Social Networking

The centerpiece of your effort to curb social networking and blogging abuses is to establish and consistently enforce a Social Networking Policy that addresses these activities.

What to Say in Your Social Networking Policy

Make sure your policy is realistic. Simply banning employees from using social networking sites or blogging altogether is impossible to enforce, especially to the extent it applies to what employees do off-duty. Although each practice must tailor its policy to its own, the Model Policy is a pretty good template. Like the Model, your social networking policy should spell out that:

- All organization computers, IT equipment and Internet access is intended for practice use only and that employees can't use them for non-work-related purposes;
- Employees are expected to work while they're on duty and to do their personal social networking outside the workplace;
- Employees may not post or say anything on a social networking site that harms the practice's reputation and good standing in the community;
- Employees may not insult, offend or demean the practice or its doctors, employees and patients;
- Employees may not divulge confidential or private information about the practice and its doctors or patients; and
- The content of any employee postings must comply with all practice policies, including its code of conduct and discrimination and harassment policies.

Conclusion

The law governing your right to discipline employees for the things they say on blogs and social networks is still in its infancy stages. But even from the early cases, it has become clear that online conversations are *not* simply private matters. There's a big difference between bad mouthing a company, supervisor or colleague to a friend in a bar over a glass of beer and making those remarks in a blog or correspondence on an ESN.

The bottom line: You have the right to take action against employees for social networking and other online activities, even if those activities take place while the employee is off-duty and at home. Having the right social networking policy will help you exercise this right effectively. Better yet, it should help you prevent employees from engaging in social networking abuses in the first place.

POLICY BANK

Model policy on social networking by employees

Here's a Model Policy you can adapt for your practice to limit employees' social networking activities.

Employee social networking

The purpose of this policy is to outline acceptable and unacceptable use of any computer equipment and other technology by all "employees" (as defined below) of XYZ Medical Practice (the "Practice") as such use relates to blogs and/or social networking Websites. These rules and restrictions herein are in place for the protection of all employees and the Practice. Violation of this policy exposes the Practice to risks and legal liability.

1. Scope

a. **Who This Policy Covers:** This Policy applies to all permanent, probationary and temporary employees; contractors; consultants; and other workers at the Practice, collectively referred to as "employees."

b. **What This Policy Covers:** For purposes of this Policy, "social networking" refers to online interactions with individuals of common interests via chat, messaging, video, file sharing, blogs, texting, Twitter messaging, email, discussion groups and other methods on external social networks, including but not limited to sites open to all web users such as Facebook, Twitter and Pinterest.

2. Prohibited and/or Restricted Uses

a. **Practice Owns Computer Equipment:** All equipment and technology purchased or leased by the Practice (regardless of its location) that is accessed by its employees, including without limitation, computers, Internet access, PDA, is intended for work-related use only. Employees may not use any Practice equipment or technology for personal purposes, including, but not limited to, maintaining, accessing or using a personal blog or social networking website.

b. **No Social Networking during Work:** While at the workplace during work hours, employees are expected to be working, not handling personal matters. Employees must keep their outside interests and activities, including, but not limited to, the maintenance, access or use of a personal blog or social networking website, outside the workplace.

c. **No Negative Communications on Social Networks:** Employee social networking communications, including, but not limited to, postings on blogs and social networking websites, must not negatively impact the Practice's reputation or standing in the community Any communications that are insulting, demeaning, or offensive to the Practice, its employees, doctors, patients or affiliates, or that the Practice otherwise deems harmful or damaging are a violation of this Policy.

d. **No Publication of Private or Confidential Information:** Employee social networking communications must not include any information which the Practice deems is a trade secret or other sensitive or confidential information related to the Practice, its doctors, employees or patients.

e. **Social Networking Subject to Other Practice Policies:** The content of employees' social networking communications must comply with all Practice policies, including, without limitation, the Code of Conduct and any policies related to discrimination and harassment in the workplace.

3. Violation of this Policy

Any employee who violates this policy will be subject to disciplinary measures up to and including dismissal.

4. Acknowledgement

I hereby acknowledge that I have received, read and understood this Policy and promise not only to follow it in all key respects but also help to enforce it by reporting to my supervisor or the Practice HR manager any or potential violations committed by other persons that I become aware of.

Name: ___________________________

Date: ___________________________

About this Model Policy

The law governing your right to discipline employees for the things they say on blogs and social networks is still in its infancy stages. But even from the early cases, it has become clear that online conversations are not simply private matters.

Having the right to take action against employees for social networking and other online activities, even if those activities take place while the employee is off-duty and at home, is one thing; exercising it effectively is another.

The Model Policy illustrates what to include in a computer use and social networking policy. But you'll need to modify to reflect the rules, standards, and procedures followed at your own practice.

IN A NUTSHELL

HR law & employee social networking

Can you discipline employees for social networking offenses?

Answer: It depends.

Explanation: Frittering away time, disclosing patient records, bad mouthing the practice and other offenses are grounds for discipline when they occur "off line."

So why should it make a difference if employees do these things online while social networking?

In theory, it shouldn't.

The problem, of course, is that the HR laws were forged in a different era and haven't yet caught up with the realities of social networking. Eventually they will. But until then, you face the challenge of applying 20th century employee discipline rules to 21st century employee misconduct.

One of the biggest challenges of discipline for social networking is that it so often takes place after work at the employee's own home.

While an employer generally doesn't have authority over employees after the shift, off-duty conduct *can be* grounds for discipline if it undermines the employment relationship and/or impairs the employee's ability to do the job.

Courts and arbitrators have upheld disciplinary actions for conduct outside of the workplace that:

- Harms the employer's reputation;
- Interferes with the employee's ability to perform job duties;
- Creates a situation where other employees won't work with the employee;
- Violates the law and thus affects the company's reputation;
- Constitutes insolence or insubordination; and
- Interferes with the company's management of its operations or workforce

SCORECARD

Employees fired for social networking offenses

Here are just a few examples of cases in which a court or arbitrator upheld the decision to fire an employee for social network abuses. Note that the existence of a clearly written, specific social networking policy was a factor in each of these cases:

OK to fire employee for:	Why termination upheld:
Disparaging Co-Worker in Blog: Nurse makes highly unflattering remarks about supervisor—calling her "Nurse Ratched"	Blog is not a private communication and even though nurse didn't use her name, she gave enough info to figure out who she was, who she worked for and who she was talking about
Posting Inappropriate Work Conduct on YouTube: Inspired by the movie *Jackass*, construction workers bare their genitals in lunch room and engage in other idiocy, all of which is captured on video and posted on YouTube	Even though it was a first offense, the conduct was egregious
Viewing Porn on His Work Computer: The offense was especially egregious because the employee was a supervisor	Supervisor had been warned twice
Sending Harassing Emails: Employee sends threatening emails to his co-workers	Conduct violates organization's violence and harassment policy
Ridiculing Boss on Facebook: 2 car dealers make negative comments on Facebook about boss and the dealership they work for including "don't buy from" them	Arbitrator treats Facebook postings as public communications
Excessive Personal Texting: Employee constantly uses his personal cell phone to text friends and family during work hours	Conduct violates written policies and employee received at least 2 warnings
Junior High Teacher Has Child Pornography: Teacher found to have naked pictures of his 15-year-old student on the hard drive of his work computer	Teacher knew IT department had access to his hard drive and had no reasonable expectation of privacy
Badmouthing Product in Blog: Employee mocks the city she's supposed to help promote in her blog	"Polar Penny" was no ordinary employee—she was in charge and served as the face of the campaign to bring tourists to the city
Praising Hitler in Blog: Employee calls Hitler a genius and makes other racist statements on his personal blog	Co-workers knew employee had posted the blogs and refused to work with him

RECRUITING

The best ways to find and hire qualified office staff

Do you struggle to find qualified office staff who are also a good fit for your practice?

It can be very difficult to figure out which methods are best for attracting the qualified job candidates you seek. Trial and error can be time consuming, and all too often results in a costly hiring mistake.

Fortunately, research conducted by staffing and recruiting consultancy CareerXroads provides insight into recruiting and hiring best practices. For the past 12 years, the firm has been conducting annual surveys on the best sources for finding and hiring staff for offices like yours.

Looking within

The CareerXroads Sources of Hire 2013 study finds that last year nearly 42 percent of open positions were filled by internal movement and promotion.

There are multiple advantages to considering current staff for new assignments. You already know what skills they possess, and you're familiar with their work habits; plus, they know the practice. Assuming the people you would consider are great workers, it's already been determined they're a fit for the organization.

In addition, upward mobility reflects positively on the practice. Furthermore, "hiring" from within is less costly than recruiting and hiring a new staff member.

Nevertheless, there are considerations

In order for current staff to succeed in a new role, is additional training required? If so, can the practice support the transition, from both a financial and time standpoint? For instance, a promotion to the coding department from general clerical staff might involve off-site training.

Would your internal job candidates welcome a new opportunity? Keep in mind that not everyone responds positively to the prospect of change. Don't push someone into a supervisory role if they believe they will be happier doing billing data entry for another person in charge.

What about the positions left vacant? If the jobs are entry-level, they might be easier to fill than the current job opening or openings. On the other hand, if by creating internal movement you create openings in jobs that are highly specialized, you may be needlessly adding to your staffing challenges. For example, moving a clinical employee into administration might leave a spot difficult to fill.

Relying on external sources

When it's time to turn to external sources to fill open positions, there are numerous choices. Yet, three stand out among the others.

The CareerXroads study finds these are the top three sources of external hires:

1. Employee referrals, 24.5 percent
2. An employer's own careers site, 23.4 percent
3. Job boards, 18.1 percent

Additional external sources of hire from the CareerXroads survey include direct sources; colleges; rehires; social media; temporary workers who convert to hires; career fairs; and walk-ins, among others.

Let's first take a look at the top three sources, and how you might use them.

Tapping the power of employee referrals

There's a reason employee referrals account for almost one-fourth of all external hires. A member of your staff, who is presumably a terrific worker, highly recommends someone for a job. What could be a better way to hire?

Unfortunately, this method can have a downside as well, particularly in a small office environment. Hiring a staff member's relative or close friend, for example, has the potential for problems and should be avoided.

Nevertheless, because referrals are a proven source, and less expensive than other recruiting methods, don't let any initial concerns deter you. Establish referral guidelines (e.g., no relatives or close friends if yours is a small office), and of course carefully screen these job candidates as you would any others.

Using your practice's website for employee recruitment

Many large employers have a full-blown careers site, which includes an array of information presented on multiple web pages, along with job listings. However, smaller employers often also have a careers site, although it usually consists of a single web page.

If your practice has a website but doesn't have a careers site, you may want to consider creating one, especially if yours is a large to mid-size practice.

Today's job seekers spend a lot of time online, and they research potential employers. A careers site, even a single page, will provide potential hires with information about open jobs – and, while at your website, they will learn more about the practice.

Don't underestimate the value of driving job seekers to your website, where they can learn more about the practice. If when perusing your site they decide the practice isn't a fit, they will self-select out of the application process, saving everyone time, and the practice the cost associated with additional candidate screening – or, worse, the cost associated with a bad hire.

Posting at job boards

Job boards are another popular and successful source of hire. Of course the question is what job boards to use.

There are large, well-known job boards like CareerBuilder and Monster, which get many site visitors, as well as niche job boards.

When it comes to niche job boards, take a look at industry-specific sites. However, you'll want to check them out before you pay to post your open positions. Things to consider include number of jobs advertised, site traffic, and geographic region.

And speaking of geographic region, don't overlook job boards aimed at specific areas of the country. Some of these are highly popular; but again, make sure you conduct a little research before you commit to advertising.

Finally, most newspapers have both a print and an online edition, and often you have the option of advertising jobs in both. Newspapers, print and digital, still have plenty of readers, many of whom are job seekers.

Considering other methods

Two of the less popular sources in the CareerXroads study might also be worth considering: temporary workers who convert to employees and rehires.

Today's temporary workers include people with skills ranging from entry to executive level. In addition to providing a quick solution, a temporary work relationship offers another important advantage. It's an opportunity for both parties to see if the relationship is a fit.

Rehiring someone who previously worked for the practice, on the other hand, has an advantage in that the person is already a fit for the practice. Or so it seems. Considerations with regard to rehires include length of time since the person last worked for the practice; if day-to-day operations have changed considerably, the former employee may no longer be a fit. Of course, it's also important to revisit why the person initially left and determine if she or he is now able to commit to the job, at least for the foreseeable future.

Recruiting and hiring are not easy tasks. But by relying on proven sources, you can find the staff you need to keep your practice running smoothly. ◆

coding update

Subluxation of radial head – "nursemaid's elbow"

By Aimee Wilcox, MA, CST, CCS-P

Subluxation is an injury caused when the normal position of a joint (or other part of the body) is partially or incompletely dislocated.

Subluxation can be caused by injuries and impact to the joint or from instability of the joint due to laxed muscles, tendons, or ligaments that usually support or hold the joint in place.

Although not a complete dislocation, subluxation can be as painful and disruptive as a dislocation. Diagnosis occurs after x-ray of the painful joint is reviewed and treatment for sublimation is the same as dislocation with one exception, which may include manipulation, to put the joint back in its normal anatomical location and immobilization such as a sling or brace to hold the joint in place while healing occurs.

However, healing time for a sublimation may be less than it is for an actual dislocation.

If repetitive sublimation of the same joint is a problem, physical therapy may be ordered to strengthen the surrounding muscles, ligaments, and tendons to create an atmosphere of support rather than weakness.

The radial head is the most proximal aspect of the radius bone. This area is mobile within the annular ligament and allows probation and supranational of the forearm.

Nursemaid's elbow

Nursemaid's elbow is another term for sublimation of the radial head or a pulled elbow. This is the most common upper extremity injury in infants and young children presenting to the ER or Urgent Care.

Although it can be seen in infants as young as six months, it is rare.

Cause: A quick tug of the arm, swinging the child around by their hands, or picking them up by their hands can very easily cause a sublimation of the radial head. The annular ligament is not fully fused in young children, which makes it easy for the radial head to slip or tear through this ligament and become subleased or dislocated. It is more common than you think. Caregivers rarely understand what caused the patient to have a sudden onset of pain in the arm because there is no obvious etiology. The funny thing, is that the majority of radial head sublimation occur on the left side and this is thought to possibly be because the caregivers are right handed, holding the child's left arm.

Diagnosis: Patients with sublimation of the radial head may complain of wrist pain, won't use the wrist or arm, and tend to hold their wrist with their good hand. All indications are that there is a wrist injury, when in fact, there is an elbow injury. If swelling is present then x-rays must be done to rule out a more serious injury, but as this is a very common injury, it is generally easily diagnosed.

Treatment: Mild but constant traction of the arm with supranational and then probation with flexion and extension should return the radial head to its proper anatomical location. There is an excellent You Tube video showing a toddler having her radial head reduced. We have provided a link to this video below.

To see this technique demonstrated, go to the YouTube link: http://www.youtube.com/watch?v=tJb5rGOFiTY

CPT Coding: 24640 ICD-9-CM: 832.2