



IN THIS ISSUE

Pay For Performance:
Are You In the Game?

Don't Forget The Basics

Vital Signs

Physicians And The AMT



*Member of the
Wolf Financial Group*

Healthcare

Better Ways ▲ Better Results

A NEWSLETTER FOR THE HEALTHCARE INDUSTRY

WINTER 2008

Data Security: Why You Should Care



HIPAA security rules say you must implement safeguards to protect the confidentiality, integrity and availability of any patient data that is either stored in an information system or transmitted.

Data security is important for several reasons. First and foremost, privacy breaches can and do happen in medical practices with frightening regularity. Of privacy violations tracked by the consumer advocacy organization Privacy Rights Clearinghouse (<http://www.privacyrights.org>) in 2006, some 16 percent occurred in healthcare organizations. That figure could be up another 5 percent to 6 percent this year if trends continue.

Second, it would be a mistake to view protecting patients' privacy and security as simply a "compliance issue." Any breach that is made public could have long-term repercussions, including damage to your reputation.

The Importance Of An IT Review

Also known as an "information systems audit," this is quite simply an examination

of the controls within your practice's IT infrastructure (your computer system, billing software, EMR, intranet and Internet sites, etc.). At its most basic, such a review seeks to address three critical areas:

Availability. Will your computer systems be available for the business at all times when required? Computers won't be available, for example, if they are disabled by a virus or if a hard drive fails and data was not backed up properly.

Confidentiality. Will the information in the systems be disclosed only to authorized users? Passwords, firewalls and other security features come into play here.

Integrity. Will the information provided by the system always be accurate, reliable and timely? Integrity certainly cannot be ensured if your computers are vulnerable to hackers or manipulation by personnel within the practice.

What To Do

You can take measures to protect yourself, your patients and your practice without spending an arm and a leg. Most of the measures suggested by security experts call for investing time, not money.

Put someone in charge. HIPAA requires practices to name a security officer as the point person for implementing the regulations. Assign security to one person — preferably someone with real authority, such as a doctor or office supervisor — and give him or her the resources and time to do the job. This may include conducting a risk analysis, creating procedures and policies, training

Pay for Performance: Are You In The Game?



Love it or hate it, pay for performance, or P4P, appears to be the next big thing in U.S. healthcare, says Steve Lutz, partner-in-charge of the Healthcare Services Group at Wolf & Company LLP.

Advocates say P4P addresses concerns that traditional payment structures reward volume rather than quality. Critics say it's just another bureaucratic jumble of numbing regulations and paperwork.

What It's All About

At the heart of P4P is the concept of evidence-based medicine and an attempt to reward positive outcomes and adherence to best practices. The most notable example is Medicare's new Physician Quality Reporting Initiative (PQRI), which establishes a financial incentive for physicians who participate in a voluntary quality reporting program.

Medicare has identified 74 metrics for quality measures, such as risk assessments, screenings, specific interventions, medication management and lab test orders. The reported data will be used by Medicare to generate confidential reports to physicians on their performance.

Is This The Tip Of The Iceberg?

While PQRI and other P4P programs are limited in scope and application, all indications are that they will evolve and expand. This is perhaps best evidenced in current legislative proposals in the House of Representatives to boost the Medicare bonus from 1.5 percent to 3 percent in 2008.

Third-party payers, which have historically followed the lead set by the Centers for Medicare & Medicaid Services (CMS), are likely to follow with their own programs. Already, some organizations are rating physicians on both quality and cost measures, assigning star and numerical ratings for meeting efficiency and quality measures. As more sophisticated capabilities to use claims and administrative data are developed, it appears likely that public and private payers will use that data to profile physicians and provide feedback on their quality and efficiency.

Should You Jump Onboard?

There are certainly numerous reasons to participate in P4P programs. Participation in P4P initiatives may make sense in terms of increased professionalism or in order to receive feedback for performance improvement. You may also decide that it's a wise investment in the future of the practice. And, of course, there's the potential for bonuses. But make no mistake, participation in P4P programs can require a significant change in practice operations.

Patient base — You'll need to understand the nature of your patient base and the types of quality measures that are relevant.

Current compliance — You'll need to have a general idea of your current compliance with quality standards. (The practice may feel it has a high compliance rate, but the real picture may vary from patient to patient and provider to provider.)

Current operations — You'll need to understand the efficiency and effectiveness of your internal operations — and that you may need to make changes in staff assignments, patient flow and other patient care activities to comply with quality standards.

Continued on page 4

Splitting It Up

Deciding how to divvy up pay-for-performance rewards within the practice presents another set of challenges altogether.

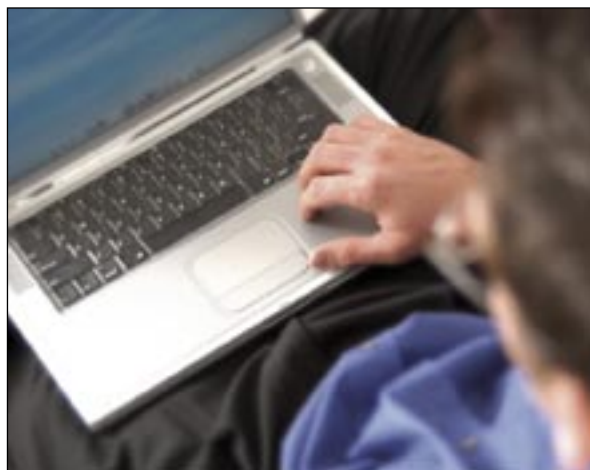
Current physician P4P initiatives concentrate on performance at the medical group level. So what happens to the individual who shirks, knowing that rewards are based on group, rather than individual, performance? Or what about an individual physician who does not have enough patients with a given condition (e.g., diabetes) to yield reliable measures of performance? Are you still going to share with everyone equally, or share based on proportion of Medicare billing?

While there is no right or wrong answer, the decision will need to rest on the practice's overall philosophy of compensation. The key is to discuss it before the first performance bonus arrives. ■

employees and ensuring that all computers are kept up to date with security patches.

Conduct an analysis. HIPAA requires practices to conduct a formal risk analysis as a first step to developing a security program. A basic risk analysis consists of asking yourself common sense questions about how you and your staff currently handle HIPAA-protected health information (PHI).

Develop a policy. Next, outline specific procedures for protecting patient data. Guides to developing policies and procedures are available from the American Medical Association, the American Academy of Family Physicians, the American Dental Association and other associations. Give your policies some teeth by establishing sanctions for violations (e.g., verbal/written warnings, unpaid suspensions, termination).



Keep on it. Running a more secure office is not a once-and-done job. Take time to regularly look for breaches.

Employ Some Low-Tech Solutions

Above and beyond the HIPAA-mandated requirements, proactive practices can take these low-tech steps to ensure data security:

Get on the stick. You might have a firm policy prohibiting physicians from taking home paper charts. But are staff and physicians using memory sticks — those handy little drives you plug into a USB port? If a non-employee gets a hold of the gadget, patients' medical records could be easily accessed.

***Better:** Use a memory stick that requires a password or contains some other security feature. The same thing goes for laptops and PDAs.*

Watch passwords. Does your group share user IDs and passwords — or have ones that everyone uses? Are you still using the vendor-supplied user IDs and passwords that came with your software? (Hackers will test to see if they've been reset or not.) Worse yet, are your passwords kept on sticky notes on your monitors?

***Better:** Create unique passwords using a combination of numbers, lowercase and capital letters, and set them to expire every 90 days. And make sure you have written policies for changing passwords when a staff person leaves your office.*

Lock 'em up. Set up password-protected screen savers that kick in after a period of inactivity to protect computer access when you step away from your PC.

***Better:** Activate the PC lockdown function by hitting CTRL-ALT-DELETE and ENTER. In Windows XP, the Windows Security dialog box pops up and the "Lock Computer" button is highlighted, which accepts the "Enter" key for quick deployment. When you again hit ENTER or click on "Lock*

Don't Forget The Basics

It's easy to focus on IT and forget about basic, mundane physical security. But some of the more common — and easily addressed — security cracks in medical offices are in fact comparatively low-tech. Consider these basics:

- Where faxes print out (and who can see them).
- Who has access to paper charts and whether safeguards are in place to protect them when they travel outside of the office.
- Who can get into the records room or see charts currently in use.
- Whether the records room is locked when it's not being used.
- What happens to paper with patient information on it. Is it shredded or simply thrown into the trash?
- Whether locks are replaced and alarm codes changed when staff turns over.
- Whether you have written standards for staff to follow regarding patient privacy and can prove you've provided training on them.

Computer" button, the Windows Unlock Computer dialog box pops up. Only upon entering your password — the same password you use when your screen saver has activated — will you return to the application you had been working in.

Log it. System logs allow you to perform an "electronic audit" of computer activity — who accessed which files and when. Ask every IT vendor about their product's ability to create an audit trail to track PHI. Then let employees know the capability is there.

***Caution:** Be careful — if you have the ability to track PHI but you don't regularly check the audit trails, you could be held legally liable if a patient files a formal complaint. ■*

Vital Signs



Physicians And The AMT



It's the classic trap for the unwary. In the mind of the IRS at least, the Alternative Minimum Tax (AMT) is designed to catch folks who are living a bit too large, tax-wise, under the usual deduction rules. The AMT is expected to affect more than 23

million taxpayers in 2007, according to the Tax Policy Center. Taxpayers caught by the AMT pay 26 percent of the first \$175,000 of AMT income, and 28 percent on amounts above that.

A Change In The Rules

The AMT rules differ from those of the regular tax code in a number of ways. Home mortgage interest and charitable contributions are deductible for both regular and AMT taxes. But other commonly deducted expenses, including property taxes and state income taxes, are not. Neither is interest on home equity debt used for "nonresidential purposes," such as paying off car loans.

The AMT Danger Zone

People who have big deductions overall are most likely to feel the sting (e.g., those who have very

high real estate taxes and mortgage interest payments, and residents of states with high income taxes). If you've sold appreciated stocks, mutual funds or an investment property and have substantial capital gains, the proceeds could kick you into AMT territory, too.

Taking Action

The goal of AMT planning is not necessarily AMT avoidance, but rather a reduction in total tax payments on a multiyear basis. The key is to determine in what year you should make estimated tax payments to get the most from deductions and offset the AMT. AMT warning signs aren't always easy to spot. Your best bet is to maintain regular contact with your accountant. ■

Are You In The Game? *Continued from page 2*

Data capabilities — Additionally, you'll need to understand the capability of your practice management and billing systems to submit the required data to health plans. Many billing systems have quirks that may prevent quality data from being submitted.

ROI — Of course, it is important to require a positive return on investment for participating in P4P programs, with all of their requirements and associated costs. But this analysis should look beyond just bonus dollars and also at the potential issue of participation or exclusion from new networks.

The Bottom Line

The use of incentives to improve healthcare is a seismic shift away from third parties passively paying for healthcare services and toward actively purchasing high-quality, efficient care. As the trend toward expanded profiling and performance reporting continues, savvy physicians will develop strategies for how their practices will respond. ■

For more information contact Steve Lutz at 630-545-4550.

Wolf & Company LLP
Certified Public Accountants

Healthcare Services Group

2100 Clearwater Drive
Oak Brook, IL 60523-1927

www.wolfcpa.com



Wolf Financial Group