THE DC'S COMPLETE GUIDE TO COMPLIANCE

REMOVING HIPAA'S BULLS-EYE ON YOUR PRACTICE



Infinedi
ELECTRONIC DATA INTERCHANGE

chiropractic economics

I am proud to be involved with the release of the "DC's Complete Guide to Compliance." Hopefully, we will be able to help chiropractic providers understand the importance of HIPAA and the associate requirements many providers fail to implement in their offices and vendors they associate with. The content of this guide covers many aspects of compliance, cyber security challenges, PHI (protected health information) breaches, patient communications and EHR security requirements.

In today's world of data breaches and cybercrime, it is more important than ever to emphasize the need for privacy and security compliance. This process can be best discovered by periodic risk analysis, as well as, updating policy, procedures, and training. Recent surveys show that less than 60 percent of practices have a plan that includes training, currently trained privacy officers and staff, breach notification policies, current business associate agreements (BAA), and electronic and mobile device policies.

Infinedi has been working for the last three years to develop and improve your claims revenue management cycle from both a back-end and front-end user experience. Our new and more robust service platform will provide you with new methodologies to review, track, and change the claims stream. When fully released, our new platform will allow you to customize how you, and your office, experience the claims cycle, with options for many intuitive, and configurable reports and queries of your claims information. The enhanced graphical interfaces with a contemporary design will help office staff quickly access comprehensive results and process flow information on every page. Most importantly, you can work safely and securely as all of our services are fully covered by HIPAA and accredited by EHNAC (www.EHNAC.com).

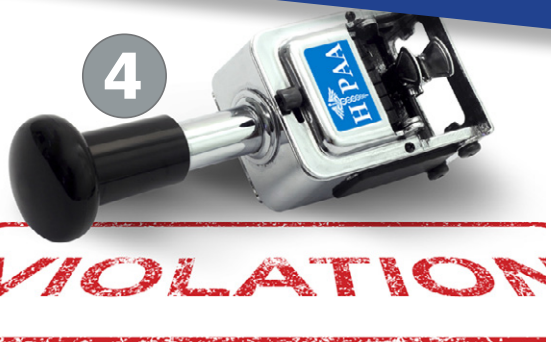
Please take the time to read the following articles, review your polices and update your staff training. Although it may take an investment in time and a little money, it is the best way to avoid a disaster. Stay compliant; protect your practice and patients.

To learn more about Infinedi or Infinedi Analytics, visit Infinedi.net or call 844-321-8312.



Brad Cost
President and CEO
Infinedi

CONTENTS









4 What you don't know about HIPAA data requirements could hurt you.

7 Is your communication with patients putting you at risk?

9 Covering the 4 bases with your electronic health record system.

11 The ever growing presence of social media and its pitfalls.

13 The 5 most common HIPAA mistakes that tend to go overlooked.

15 Small practices climbing the hill of HIPAA.

17 HIPAA violations: The 3 warning signs to watch for.

19 What you need to know as new practitioner.

21 Are you Medicare compliant?

23 Avoiding Disaster.



WHAT YOU DON'T KNOW ABOUT HIPAA DATA REQUIREMENTS COULD HURT YOU

A well-known dental practice management software company which offers products such as Dentrix and Easy Dental, is about to be handed a $250,000 fine by the Federal Trade Commission (FTC).

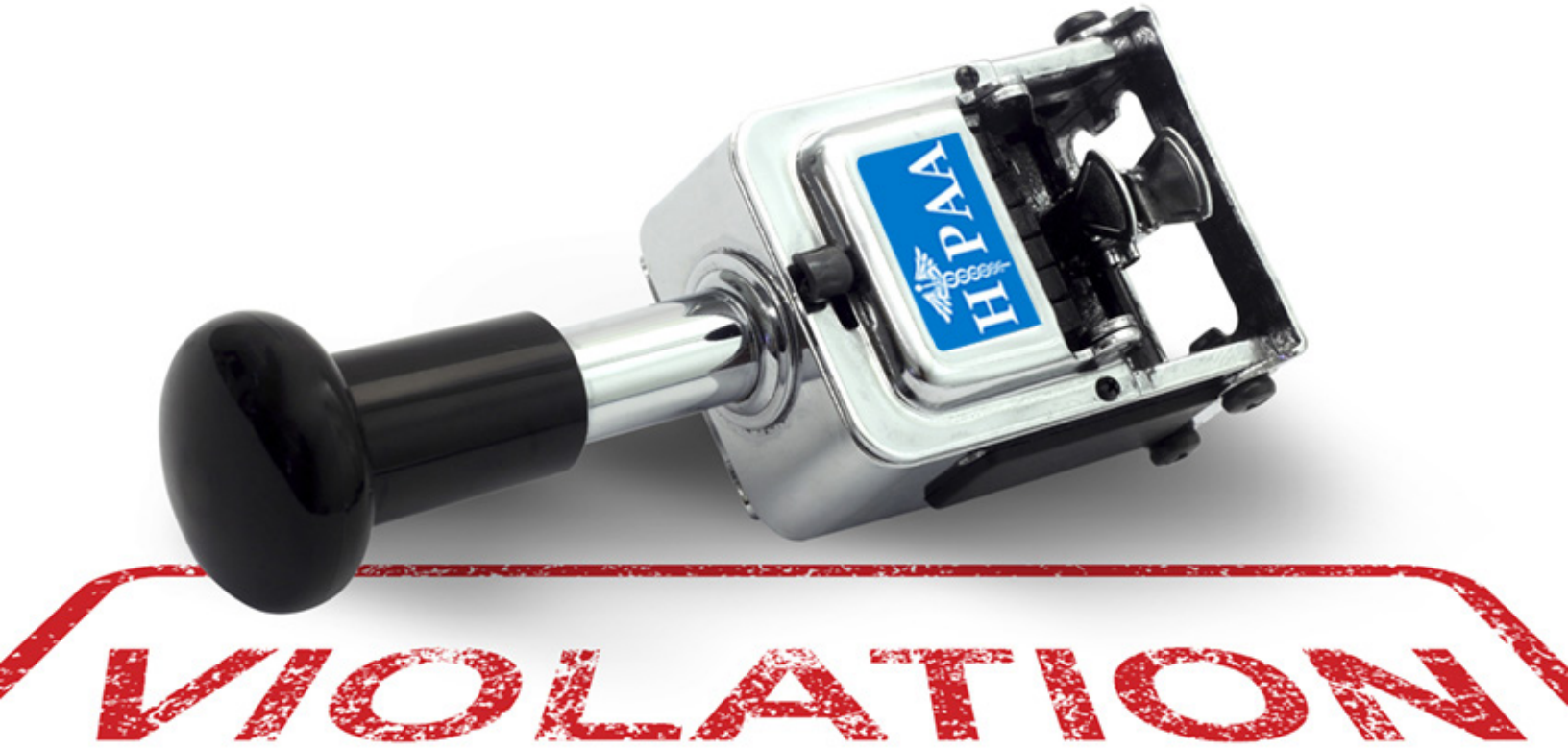
They falsely advertised the level of encryption associated with the transmission and storage of dental patients' protected health information (PHI).[1]

While the FTC charges have little to do with the practice management software company's customers who were duped by the false claims, the collateral damage could be a slew of HIPAA violation fines directed towards these practitioners.

Those unaware of the thousands of HIPAA regulations may be hardpressed to make the connection between this sanction and possible HIPAA violations resulting in fines for those using the software who seemingly innocently transmitted their patient information. However, the potential liability is real.

They knew the standards that its dentists were required to meet under HIPAA security standards, it advertised and promised that it would meet those standards, and then

continued>>



knowingly allegedly them. As a chiropractor, you could just as easily be affected if you are relying on similar claims made by your software company.

Because most practitioners' efforts to stay up to date with HIPAA requirements are lagging or nonexistent, or they have not put the required protections in place within their practices (in this case, the requirement to have business associate contracts with all individuals or entities that store or transmit electronic data; assuring that those contracts do not create an agency relationship between the vendor and physician, and thereby protecting the physician from liability for the business associate's actions), they may have become liable for their vendor's improper encryption under HIPAA.

DEFYING LOGIC

To the logical mind, this may be the opposite of what common sense would dictate, but unfortunately there are no requirements that laws follow the rules of logic.

Assuming that most—if not all—of the practitioners involved in the practice management software company's case failed to read their service agreements and did not have business associate agreements in place to properly disclaim any control over their operations, then the doctors could face a ruling that their software provider is their "agent" for HIPAA liability purposes.

This could result in dire consequences for the providers. In retrospect, it's safe to say that they could have taken steps to mitigate their potential liability, reducing any fines for which they may now be liable.

Since chiropractors use similar software programs and are held to the same HIPAA standards as the aforementioned dentists, practices should heed this as a warning to get their HIPAA procedures up to snuff and be thankful that it didn't happen to them (this time).

The Secretary of Health and Human Services issues a fine of $10,000 to $50,000 per violation in instances where the doctor made a conscious, intentional failure or exhibited reckless indifference to the obligation to comply with a HIPAA requirement

In assessing fines, HIPAA states that the Secretary of Health and Human Services issues a fine of $10,000 to $50,000 per violation in instances where the doctor made a conscious, intentional failure or exhibited reckless indifference to the obligation to comply with a HIPAA requirement.[2]

As recently as five years ago, such fines were few and far between, but HIPAA's enforcement has been greatly amplified, and it's time to start paying attention to the consequences of ignoring compliance. The days of sticking your head in the sand and hoping to dodge the bullet are absolutely over.

STAYING HIPAA COMPLIANT IN MODERN TIMES

As the value of healthcare information rises, it is increasingly being stolen and sold. In an industry report on cybersecurity challenges in healthcare, Raytheon found that healthcare records contain information that is up to 10 times more valuable on the black market than more conventionally stolen financial information.[3]

Because of this increase in value, the healthcare sector is now more than 200 percent more likely to encounter data

continued>>

theft and approximately 340 percent more likely to have a security incident than the average industry. These hackers' target both large and small operations, because regardless of where the information originates, there is money to be made by stealing it.

Increased medical data theft, coupled with several large healthcare information breaches, has pushed the public to demand better government protection. And the Department of Health and Human Services (HHS) delivered.

The HHS Inspector General, speaking for the Office for Civil Rights (OCR), has stated that, "without fully implementing [a permanent] audit program, OCR cannot identify covered entities that are non compliant."4 The OCR director responded by asserting that random audits will begin early in 2016.

To back up the bark with a significantly big bite, OCR's budget was increased by nearly $4 million to fund these audits. As if that wasn't reason enough to jump on the HIPAA compliance bandwagon, all revenue generated from non compliance fines must be used for additional enforcement. HHS explains, "OCR retains and expends these collections to support overall HIPAA enforcement activities."[5]

WHAT CAN YOU DO?

With increased breaches and impending random audits, how can practitioners stay out of hot water?

You do have options on implementing a HIPAA comply ance program in your practice. CEs are available to give you a good starting point and these cover most of the basics.

You can also employ a reputable company offering a do ityourself product that will keep you from having to read the thousands of pages of law, but it will still require some heavy lifting on your part. For the busier doctor and the more sophisticated offices, professionals are available to help you get a HIPAA compliance system in place. ■

Increased medical data theft, coupled with several large healthcare information breaches, has pushed the public to demand better government protection. And the Department of Health and Human Services (HHS) delivered.

– Lindsey Olson, Esq., is an onstaff attorney with HIPAA Compliance Services, which provides comprehensive HIPAA training, compliance materials, and onsite HIPAA program installation services. She is a Certified HIPAA Onsite Consultant.

– Ty Talcott, DC, is the president of HIPAA Compliance Services. He is a Certified HIPAA Privacy and Security expert (CHPSE). Each year he presents dozens of webinars and live presentations across the country to assist doctors in protecting their practices.

REFERENCES

1. Dental Practice Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data. Federal Trade Commission. www.ftc.gov/ newsevents/press-releases/2016/01/dentalpractice softwareprovider settlesftcchargesitmisled. Published Jan. 5, 2016.
2. Legal Information Institute. "Amount of a civil money penalty" – 45 C.F.R.160.404. https://www.law.cornell.edu/cfr/text/45/160.404. Published Feb 2016. Accessed March 2016.
3. Websense. 2015 Industry DrillDown Report. Raytheon. www.websense.com/assets/reports/ report 2015industrydrilldown healthcareen.pdf. Published Sept. 2015.
4. Murrin, Suzanne. OCR should strengthen its oversight of covered entities' compliance with the HIPAA privacy standards. U.S. Department of Health and Human Services. www.oig.hhs.gov/oei/reports/oei091000510.pdf. Published Sept. 2015.
5. HHS FY2016 Budget in Brief. U.S. Department of Health and Human Services. www.hhs.gov/ about/budget/budgetinbrief/ocr/index.html. Published Feb. 2, 2015.



IS YOUR COMMUNICATION WITH PATIENTS PUTTING YOU AT RISK?

Email and text messaging are very convenient ways people communicate, including many of your patients. These forms of communication, however, are not always compliant with HIPAA standards and may put your patients' privacy at risk.

By understanding how HIPAA applies to your electronic communication, you can make your communications more effective while also maintaining compliance and respecting your patients' privacy rights.

MOBILE DEVICE USE

To help healthcare providers understand the HIPAA communication rules for smartphones and other mobile devices, the U.S. Department of Health and Human Services published a website with specific guidelines including a mobile device fact sheet and a "Guide to Privacy and Security of Electronic Health Information". In summary, mobile devices must be used in such a way as to protect patient information, using reasonable safeguards.[1]

In effect, this rules out the use of unsecure networks and unencrypted communication methods like texting. Unsecured text messaging may not be used to communicate patient information, either with patients or colleagues.1 However, using necessary safeguards or adopting secure thirdparty software to facilitate secure texting is an option.2

When considering mobile device use within your practice, these five steps will help you determine how to uphold HIPAA requirements:[2]

1. Determine if mobile devices will be used with patient information. This includes EHR use, using mobile devices as part of your organization's internal system or "used to access, receive, transmit

continued>>

or store patients' health information." You must conduct a risk analysis and consider the risks that apply to your organization if you ultimately decide to use mobile devices in any of these ways.

2. Analyze your use (or planned use) of mobile devices to send health information. Look for threats and potential vulnerabilities.
3. Create your own custom strategy based on the vulnerable areas you identified in step #2. This strategy must include appropriate "privacy and security safeguards" and be regularly evaluated. In your plan, be sure to include your strategies for updating, maintaining and evaluating your strategy regularly.
4. Create, record and begin using your policies and procedures for mobile device use. These should protect patient information and help staff members understand how to appropriately use mobile devices.
5. Begin training staff members about protecting patient information and how to use their mobile devices in accordance with your policies and procedures. Conduct training on an ongoing basis to provide the most up-to-date information.

EMAIL

Email communication with patients is acceptable as a long as healthcare providers make a reasonable effort to protect patient information.[3] Unencrypted messages must take care not to reveal too much personal information. Precautions must be taken to ensure that messages are sent to the correct email address. Patients may ask for an alternative form of communication instead of email, as long as the request is reasonable.

Healthcare providers may safely assume that email is appropriate communication with a particular patient if that individual initiates email contact by sending an email message to the provider.[3] If the patient requests a different form of communication, you should offer something more secure such as mail or phone communication.[3]

Begin training staff members about protecting patient information and how to use their mobile devices in accordance with your policies and procedures. Conduct training on an ongoing basis to provide the most up-to-date information.

KNOW YOUR USE OF INFORMATION

You should do your own due diligence by researching HIPAA guidelines and determining how they apply to your practice's use of electronic communications. Also, be aware that these regulations do change. Other regulations may apply to your practice and you must be prepared to comply with them.

Being prepared and using electronic communication responsibly demonstrates your concern for protecting patient privacy and offering the best care possible. ■

– by Kaitlin Morrison

REFERENCES

1. The U.S. Department of Health and Human Services. "Can you use texting to communicate health information, even if it is to another provider or professional?" https://www.healthit.gov/providers professionals/faqs/canyouusetextingcommunicate-healthinformationevenifitanotherp. Published January 2013. Accessed November 2015.
2. The U.S. Department of Health and Human Services. "Managing Mobile Devices in Your Health Care Organization." https://www.healthit.gov/sites/default/files/factsheetmanagingmobiledevices inyourhealth-careorganization.pdf. Accessed November 2015.
3. The U.S. Department of Health and Human Services. "Does the HIPAA Privacy Rule permit health care providers to use email to discuss health issues and treatment with their patients?"

COVERING THE 4 BASES WITH YOUR ELECTRONIC HEALTH RECORD SYSTEM



EHRs are rapidly changing, and many practices are intimidated by the regulations designed to keep EHR systems compliant with federal security and patient privacy requirements.

The Health Insurance Portability and Accountability Act (HIPAA) does not have to be scary or impossible to understand. By taking the time to evaluate your EHR system for HIPAA compliance, you will be reducing your risk of making costly mistakes.

1. KNOW THE BASIC HIPAA REQUIREMENTS

Covering patient privacy and security, HIPAA standards apply to organizations and agencies that are determined by law to be "covered entities" or "business associates" and are working with patient information, according to the U.S. Department of Health and Human Services.[1] This definition includes healthcare providers, outside companies hired to help with patient information, and other groups. Chiropractic practices are part of these standards.

HIPAA standards go beyond EHR, so reviewing your practice's procedures and paperwork for compliance is a smart bestpractice. For more help, the U.S. Department of Health and Human Services has a website with detailed HIPAA requirements and additional resources for healthcare providers. Because HIPAA standards may change, be sure to review the official requirements regularly.

2. UNDERSTAND THE HIPAA SECURITY RULE

Your EHR must fulfill the requirements of the HIPAA Security Rule by having "administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."[2]

This rule, by outlining specific areas where your EHR must be compliant, provides you with ideas for improving the security of your software system and reducing your risk of information security problems.

To improve your compliance, be sure to address each area individually:[3]

- **Administrative safeguards: Have procedures and policies that prevent employees and other staff from misusing patient**

continued>>

information. Regularly conduct your own risk analysis to identify and eliminate potential security breaches. Review the U.S. Department of Health and Human Services' requirements for a risk analysis.

- PHYSICAL SAFEGUARDS: Protect patient information from outside access and from natural disasters, physical damage to data, and other physical problems by setting appropriate policies and using physical or technological barriers.
- ORGANIZATIONAL STANDARDS: If outside organizations access your patient information (such as an EHR vendor or billing and coding vendor), use contracts and written policies to specify how data is used and protected.
- Maintain written policies and procedures: You must maintain documentation, in writing, of your policies and procedures that are used by your practice to comply with the Security Rule. This documentation must be saved for at least six years after the policies and procedures are created or six years after their last effective date. This documentation should also include "written records of required actions, activities, or assessments."[3] These documents should be updated regularly to account for organizational and other changes.

For more information, you can read about the Security Rule at the U.S. Health and Human Services website.

3. FIND OUT IF YOUR EHR VENDOR IS COMPLIANT

Many EHR vendors are already HIPAA compliant and take these standards very seriously. Asking your vendor about how they maintain compliance, however, is an important part of maintaining your own compliance with the Security Rule. You must also have a written, contractual agreement outlining how your vendor maintains the security of patient information.[3]

Be sure that you and your staff are properly trained in your EHR's features and know how to update your software, use security features, and keep patient data private. Your software may require special settings before it is fully secure. If necessary, ask your vendor for more information about how to control and use security features.

When choosing a new vendor, use the Certified Health IT Product List of EHR products that are certified by the Secretary of Health and Human Services. To earn this certification, vendors must submit their software to testing and verification. These products must meet specific guidelines for security and functionality, including compliance with HIPAA requirements.[3]

Asking your vendor about how they maintain compliance is an important part of maintaining your own compliance with the Security Rule.

4. REVIEW YOUR PRACTICE REGULARLY.

By reviewing your EHR and having a plan in place, you can stay HIPAA compliant. Using available online resources and outside help if you need it, create your own HIPAA risk analysis and find ways to protect your practice and your patients. ■

– by Kaitlin Morrison

REFERENCES

1. U.S. Department of Health and Human Services. "For Covered Entities and Business Associates." http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html. Accessed Novembe 2015.
2. U.S. Department of Health and Human Services. "The Security Rule." http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html. Accessed November 2015.
3. The Office of the National Coordinator for Health Information Technology. "Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity." https://www.healthit.gov/sites/default/files/pdf/privacy/privacyandsecurityguidechapter4.pdf. Published April 2015. Accessed November 2015.

THE EVER GROWING PRESENCE OF



AND ITS PITFALLS

Like other forms of electronic communication, social media websites present strong marketing opportunities and the chance to reach patients directly.

Unfortunately, social media websites also present risks such as violating HIPAA by sharing patient information online.

Knowing the risks of using social media can help you stay in compliance with HIPAA and make the most of social media's benefits.

ANONYMOUS IS NOT ENOUGH

Many practices know that patients' names should be kept private, but HIPAA privacy requirements go beyond protecting patient names. In fact, you should avoid revealing any information that may allow others to guess the patient's identity.[1] Controlling who sees information you post is difficult online and readers who are familiar with the patient may see what you post—keeping the patient anonymous does not necessarily protect their personal identity.

According to the *Boston Globe,* one physician unintentionally posted information revealing a patient's identity on a social media website and was subsequently fired from her position and reprimanded by the state's licensing authority. The patient was anonymous, yet information about his condition allowed community members to guess who he was.[2]

In practice, it is possible to deidentify patient information but impossible to completely prevent others from identifying the individual.[1] In fact, the U.S. Department of Health and Human Services notes that

continued>>

information about an individual's fivedigit zip code, birthdate and gender is probably enough to uniquely identify over half of America's population. 1 In theory, sharing a few demographic facts about your patient on social media may be enough to disclose their identity online and violate HIPAA. If your patient has an unusual medical condition, occupation or other uncommon characteristics, disclosure risks may be even higher.

To be absolutely sure that your social media use is not releasing personally-identifiable information about patients, you should do your own research and create a social media policy to protect your practice.

MAKE A SOCIAL MEDIA PLAN

An article in *Compliance Today,* the journal of the Health Care Compliance Association, suggests weighing the risks of social media, outlining specific uses, and purposes for your practice's social media accounts and assigning specific employees to those accounts while monitoring these websites for compliance.[3]

The article's authors, Jim Sheldon-Dean and Dr. Vidya Phalke, PhD, suggest you take steps to reduce your risks of violating HIPAA, including:[3]

SOCIAL MEDIA POLICIES—Your practice should identify how social media will be used, who is permitted to use your clinic's social media accounts and what types of information may be shared. You should carefully consider what risks exist and how you will respond to them if they happen. For example, consider whether or not personal pages may "friend" patients and how clinical information should be protected.

EMPLOYEE TRAINING—If your office has employees, you should regularly train them on HIPAA compliance and your social media policy.

To be absolutely sure that your social media use is not releasing personally-identifiable information about patients, you should do your own research and create a social media policy to protect your practice.

VERIFY COMPLIANCE—Know how HIPAA protects patient privacy and understand what HIPAA violations look like. Familiarize yourself with how patient identities may be accidently revealed on your social media accounts, then monitor the use of those accounts.

BE CAREFUL WHEN COMMUNICATING WITH INDIVIDUAL PATIENTS

Because the risk of accidently releasing personal information on social media is high, you may want to be careful about contacting individuals. While it may be permissible under HIPAA to privately communicate via social media with a patient, you need to be absolutely sure your patient approves of communicating on social media and understands both the risks and possible outcomes of a data breech.[3]

It would be wise to restrict the types of information you discuss, even in a private message because the text of your conversation may be accessible by others, such as the company that owns the social media website. Explain this possibility and other risks to your patient before beginning to discuss personal information.[3]

HIPAA regulations may change, so be sure to do your own research before using social

continued>>

media to communicate with your patients. The U.S. Department of Health and Human Resources offers a HIPAA for Professionals resource where you can find more specific guidance.

Use social media while protecting your patients

Social media allows you to market your practice, connect with new patients and interact with the chiropractic community so for your practice, these benefits may outweigh the risks of social media. If you are careful and do your own research, you can reduce these risks and benefit from social media's possibilities. ■

– by Kaitlin Morrison

REFERENCES

1. The Boston Globe. "For doctors, social media a tricky case." http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/?page=full. Published April 2011. Accessed December 2015.
2. S. Department of Health and Human Services. "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule." http://www.hhs.gov/hipaa/for professionals/privacy/specialtopics/deidentification/index.html#safeharborguidance. Accessed December 2015.
3. Compliance Today. "Social media and HIPAA compliance: Balancing benefits and risks." http://www.hcca info.org/Portals/0/PDFs/Resources/Compliance_Today/0213/CT_0213_SheldonDeanPhalke.pdf. Published February 2013. Accessed December 2015.

THE 5 MOST COMMON HIPAA MISTAKES THAT TEND TO GO OVERLOOKED

By now, all chiropractic practices have at least a passing familiarity with HIPAA and the regulations and requirements the law entails.

Anyone who handles personal information must protect it, including DCs and their staffs. And even when the utmost care is taken to be HIPAA compliant, there are still areas where many healthcare practices are commonly making mistakes.

continued>>



Equipment is becoming increasingly important. Technology advances make work easier and can often improve patient care and outcomes. However, there are at least two areas where technology could lead to a lack of HIPAA compliance:

1. HARD DRIVES — Last year, a company called Affinity Health Plan returned some photocopiers they had leased, and personal health information was stored on the hard drives of those copiers. Affinity self reported the incident to the Department of Health and Human Services and was fined.

2. MOBILE DEVICES — Mobile devices often improve the workflow in a healthcare practice. Being able to easily and conveniently carry a single device that holds all of the information necessary to provide thorough and proper care to a patient is a boon to many DCs. However, such devices can be stolen, along with the information they contain. Just as leaving a charts unattended puts a facility out of compliance, so does a tablet that is vulnerable to theft. In addition to equipment, chiropractic offices must consider the human factor in being HIPAA compliant. People are just as important as machines when it comes to data security. There are several areas of possible vulnerabilities concerning office staff:

3. UNDERSTANDING HIPAA — When the staff has a clear understanding of the law and its repercussions, they are more willing to implement new policies or follow what may seem like cumbersome guidelines.

4. PAPERWORK — Although many offices are moving toward being paperless, there are still forms that must be completed or provided to patients, such as the Notice of Privacy Practices (NPP). Making sure that each file is complete is as important as making sure it is secure.

Mobile devices often improve the workflow in a healthcare practice. Being able to easily and conveniently carry a single device that holds all of the information necessary to provide thorough and proper care to a patient is a boon to many DCs. However, such devices can be stolen, along with the information they contain.

5. TRAINING — Many Electronic Health Records (EHR) systems are designed to help users stay HIPAA compliant. However, if staff members are not using or are incorrectly using the EHR, then the design will not matter. Making sure that everyone knows how to use the system and that it is being fully implemented will go a long way toward keeping your practice compliant.

HIPAA is a complex law and remaining compliant can seem daunting. However, there are tools and services that can help. Hiring an outside firm to analyze your systems may be worth the time, cost and effort. Often, EHR systems manufacturers and retailers will offer some HIPAA training. A review every two to three years will ensure your practice remains compliant. ■

– By Dava Stewart



SMALL PRACTICES CLIMBING THE HILL OF HIPAA.

A recent survey on HIPAA compliance conducted by NueMD, Porter Research, and the Daniel Brown Law Group uncovered several issues with compliance in medical practices.

Across the board, numbers relating to compliance or confidence in compliance were too low for comfort, especially within smaller operations. If your practice is struggling to keep up, there are a few easy first steps you can take to button up your compliance program.

HIPAA IS MORE IMPORTANT THAN EVER

You might have noticed a recent uptick in coverage on data breaches within healthcare. While a lot of news emphasizes hospitals and larger organizations, small covered entities are just as liable. And unfortunately, small practices usually don't have a ton of cash to pay a fine (which can range from $100 to $50,000 per violation, with an annual cap of $1.5 million).

To drive its point home, the Office for Civil Rights is about to embark on their second round of HIPAA audits. At this year's HIMSS Privacy and Security Forum, Linda Sanches, who heads the audit program, said, "We'll be looking for periodic risk analysis and evidence of compliance, as well as documentation of policies and procedures being in place."

With regard to these policies and procedures, you need to have a plan. Your plan should address all facets of your compliance program, including information flow, training procedures, HIPAA officers, breach notifications, and business associate agreements with outside vendors that access your patients' protected health information (PHI).

One troubling stat from the survey is that only 58 percent of respondents at practices said they have plan. Below are a few key components of a solid compliance plan:

continued>>

HIPAA TRAINING

Train everybody at your practice with no exceptions. The survey called attention to several cases in which staff and providers weren't on the same page as management and owners.

The solution is to periodically train your employees and make sure new staff members receive training during the onboarding process. And don't forget to have proof—auditors will be looking for it.

SECURITY AND PRIVACY OFFICERS

These officers are employees who make sure your practice stays in line with HIPAA standards. To get a better feel for their responsibilities, review these two sample job descriptions for Security Officers and Privacy Officers.

BREACH NOTIFICATION POLICIES

In the case of a security breach, your practice could be required to take specific action to resolve the issue. A breach could be triggered by occurrences such as the theft of a mobile device containing PHI or unauthorized disclosure of PHI.

"If there are less than 500 individuals involved, the organization must provide written notice to each of those individuals," said healthcare lawyer, Dan Brown. "If more than 500 individuals are affected, the organization has an obligation to notify the press about the breach, as well as the Department of Health and Human Services."

The survey also indicated that only 45 percent of respondents from practices said they have a formal policy for PHI breach notifications. Auditors won't be very happy with the other 55 percent.

BUSINESS ASSOCIATE AGREEMENTS

Covered entities are responsible for creating contracts with their business associates to ensure the proper usage of PHI. This sample business associate agreement from HHS.gov states:

"A 'business associate' is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information."

For small practices, this could mean medical billing companies, software vendors, or other outside consultants.

At the HIMSS Privacy and Security Forum, Linda Sanches urged covered entities to create a complete list of all of their business associates.

In the case of a security breach, your practice could be required to take specific action to resolve the issue. A breach could be triggered by occurrences such as the theft of a mobile device containing PHI or unauthorized disclosure of PHI.

ELECTRONICS AND MOBILE DEVICES

Considering the speed at which technology is moving forward, HIPAA implications get a little fuzzy. In many cases, it's not as easy as saying, "this device is compliant" or not. One thing practices can do easily is catalog all electronic devices that could contain PHI, keep track of where they are and what they contain, and keep the list up to date.

Determining whether electronic devices and communication are compliant will require an indepth review of how PHI is stored and transferred. Periodic risk analyses will help you find weak points in your flow of PHI and address problems before a breach occurs.

With a risk analysis, the idea is to

continued>>

identify all pathways that PHI can take, whether electronically, on paper, or via outside business associates, and make sure you don't have any gaps. Proof of risk analyses tell auditors you're taking compliance seriously. Unfortunately, only 33 percent of respondents from practices reported that they've conducted one.

NEXT STEPS

The above tips are a good starting point, but achieving compliance is a big commitment and will require time. To accompany this information, check out this helpful webinar series on HIPAA compliance that offers further insight.

Beyond freely available information on the web, practitioners should contract with healthcare lawyers or HIPAA experts to ensure program compliance. For those with a tight budget, many consultants are open to a "team approach" that will help make the most of internal resources. ■

– by Dava Stewart

HIPAA VIOLATIONS: THE 3 WARNING SIGNS TO WATCH FOR

The Health Insurance Portability and Accountability Act (HIPAA) has been in place for long enough that virtually every clinician and practitioner in business is aware of the law and the consequences of not following it to the letter. That knowledge, however, doesn't mean that DCs across the country know exactly how to follow the rules laid out in HIPAA. Knowing the warning signs of incompliance can help keep the chiropractic office running smoothly, even in the event of an investigation.

HOW AND WHY WOULD A PRACTICE BE INVESTIGATED?

The Office of Civil Rights (OCR), which is part of the Department of Health and Human Services (HHS), is responsible for enforcing the privacy standards set forth in HIPAA. There are many reasons an investigation could be carried out, and, according to the HHS website, there are three ways the OCR enforces HIPAA privacy regulations: by investigating complaints filed with it, conducting compliance reviews to determine if covered entities are in compliance, and performing education and outreach to foster compliance with the Rules' requirements.

There are a few warning signs that may indicate a practice is out of compliance with HIPAA. Keeping a check on the workflow of the practice, as well as with whom information is shared, are important steps when considering patients' privacy.

continued>>

WARNING SIGNS

WHAT ARE SOME "SYMPTOMS" OF INCOMPLIANCE?

There are a few warning signs that may indicate a practice is out of compliance with HIPAA. Keeping a check on the workflow of the practice, as well as with whom information is shared, are important steps when considering patients' privacy. Here are some signs a practice is unintentionally violating patients' rights:

1. **PAPER FILES ARE ACCESSIBLE.** Charts hanging on doors or lying on tables are like blaring red warning signs when it comes to HIPAA violations. If anyone besides a healthcare provider or the patient could pick up a file and flip through it, the patient's privacy is not being protected. With the rise of electronic health records (EHR) systems, paper files are becoming less of a concern in most practices; however, there are still quite a few offices that maintain paper files. Making sure those files are protected must be a priority in those practices.

2. **STAFF MEMBERS CASUALLY DISCUSS PATIENTS.** It may seem hard to believe, but it happens more often than most DCs imagine: Staff members describe patients, or use names, and talk about treatment plans, insurance coverage, conditions, and of other topics that are HIPAA violations — within hearing range of other patients or people in the waiting room. After all, staff members are at work, and they are talking about work, so it doesn't seem like a violation.

Regular training and discussion of HIPAA and all that goes along with remaining compliant is the best way to prevent violation through casual conversation. The more often staff members hear, read, or talk about HIPAA, the more likely they are to have the regulations in mind.

Charts hanging on doors or lying on tables are like blaring red warning signs when it comes to HIPAA violations.

3. **COMPUTER SCREENS LEFT UNATTENDED AND OPEN.** In offices using EHR systems, an open computer screen is the equivalent of leaving a paper chart on a table. In fact, an open screen is worse in some ways because navigating to other patients' files is a fairly simple thing to do. However, even without that kind of purposeful snooping, leaving private information on a screen that other people could see is a violation of HIPAA regulations.

Again, training is the best way to address the potential problem. Once staff members develop the habit of closing everything when they walk away from the computer, patient information is more secure and the possibility of a violation is lower. ■

– By Dava Stewart



WHAT YOU NEED TO KNOW AS A NEW PRACTITIONER

As a new chiropractor, you're not exempt from HIPAA violations. Know how to prepare to avoid future problems.

A common misconception among chiropractors is that if you're a new practitioner and your practice is relatively small, you aren't at risk for violating HIPAA compliance laws.

Regulatory complaints and the penalties associated with them are on the rise and smaller practices have special exposures that can cause even greater risks.

There are many reasons for the increase in regulatory complaints and the enforcement that follows including the Patient Protection and Affordable Care Act requirements, increased enforcement of Medicare laws, and HIPAA compliance and regulatory agencies targeting chiropractors. One of the main reasons, however, is the growing sophistication of healthcare consumers.

Medical doctors (MDs) have generally been faster than DCs in fully implementing HIPAA compliance programs in their offices. This may be due to the fact that hospitals were early targets of regulators and so they developed their programs early. As a result, many MDs were exposed to the rules in a meaningful way long before other types of healthcare practitioners.

Unfortunately, that is to your disadvantage as nearly all chiropractic patients also see MDs. As medical offices conform to new regulations, their patients participate in and are educated relative to what should be done. This makes it more likely for them to complain if you are not following suit.

Whether it's due to ignorance or lack of resources, many smaller practices are the

continued>>

most neglectful. This makes them more likely to get patient or peer complaints.

Keep up with the reasons for complaints and try to avoid them.

There was recently a $50,000 fine collected due to a breach of information on a laptop that only involved 441 patients. That is a far cry from the patient volume seen by hospitals and large clinics.

THE FOLLOWING ARE SPECIAL CHALLENGES FOR THE NEW OR SMALL PRACTICE.

1. Being unaware of the following:

   That there are required clinical files and denied claims audits that must be performed internally (by you or your staff) on a yearly basis and the deficiencies you find, plus your corrective actions, must be documented.

   That there are standard forms with required language that must be stored in your HIPAA compliance manual. Whether you feel you will ever use them or not, you are required to know when and how to use them.

   When and how to correctly use and audit advance beneficiary notice (ABN) forms. This is probably the most misunderstood procedure in most practices.

   That you must conduct and document HIPAA training for all team members yearly — even if you are the only team member. There are required topics you must document that you covered during that training.

   That you must have a way to organize your compliance program via an appropriate HIPAA manual. That just because a new electronic healthcare record (EHR) software system says it is HIPAA compliant, it doesn't mean it addresses the other areas of required compliance listed above.

   That it does not take a fulltime employee to be your HIPAA compliance officer. The doctor or existing staff will be able to handle these functions with minimal impact on daily operations.

2. Inexperience: Use other people's experience so you don't go through the pain. Make sure you know the most recent reasons for fines being levied and the ways to protect yourself.
3. Lack of focus: Always focus on results and business growth, but make sure you take care of matters that can close your doors. You must manage risk in all its forms.
4. Lack of resources: New or small practices are often short on cash and staff. While it takes some time to get your program in place, any doctor or CA can do it with inexpensive educational solutions. Once the program is in place, it should only take about one to two hours per quarter of the year to follow up adequately.
5. Lack of education: Keep up with association trainings, seminars, and conventions. Read journals and get advice from other professionals to help educate yourself.

Many smaller practices are the most neglectful. This makes them more likely to get patient or peer complaints... There was recently a $50,000 fine collected due to a breach of information on a laptop that only involved 441 patients. That is a far cry from the patient volume seen by hospitals and large clinics.

WHAT TO DO

Be aware and start doing something. Showing intent to comply and documenting your activity goes a long

continued>>

way, even if you are deficient in many areas.

Sign and date all documentation relative to your internal audits, corrective actions, and other policies and procedures. In general, if it is not signed and dated, auditors or inspectors will consider it to be invalid or not done at all.

Create a HIPAA manual separate from your policy procedure manual. This is critical to "store" information relative to your compliance program and to record your audit activity, etc. This should be a working document. If your manual has been untouched for six months or longer, there is no way you can have an adequately functioning compliance program.

Make sure your materials are current. Budget a small amount of time and money to get educated via seminars, journals, and professional materials.

Get help and attack each of the challenges listed above. ■

– By Ty Talcott, DC,
and Martha McKinney, CPO

ARE YOU MEDICARE COMPLIANT?



Medicare may seem like a labyrinth of governmental hoops, red tape barriers, and walls of impenetrable bureaucracy. But, the fact is, if you see patients covered under Medicare and you want to get paid for your services, you have to be able to navigate that labyrinth efficiently, and without tripping. Your practice needs to be Medicare compliant.

The first step is to understand what being Medicare compliant means for chiropractors. One good place to start is with a booklet, which was published by the Centers for Medicare and Medicaid in October 2013, titled Chiropractic Services. This literature answers frequently asked questions regarding qualifications and payment requirements.

continued>>

To get a more detailed look at Medicare requirements and regulations, you will want to delve into the Medicare Benefit Policy Manual, chapter 15, "Covered Medical and Other Health Services," most recently revised on April 4, 2014.

One important thing to realize is that chiropractors do not have the option of opting-out of Medicare. The CMS specifically addresses this question on page 25, in section 40.4 of Chapter 15 in the manual. DCs can choose to be nonparticipants, but that is not the same thing as opting out, nor does it mean they are not required to bill Medicare. If you treat a patient who is covered by Medicare, you must bill Medicare. In addition, being a nonparticipant does not exempt you from being audited. The CMS details the differences between non-participation and participation in a document titled "Medicare Enrollment for Physicians, Non-Physician Practitioners, and Other Healthcare Service Providers."

Participation or not aside, in all likelihood, you will be billing for Medicare for some services, and there is the possibility you will be audited for compliance. There are several points to keep in mind:

You can only bill Medicare for covered services. The Medicare Benefit Policy Manual is very specific in stating, "Coverage extends only to treatment by means of manual manipulation of the spine to correct a subluxation provided such treatment is legal in the State where performed," according to the Medicare Benefit Policy Manual, page 20, section 30.5.

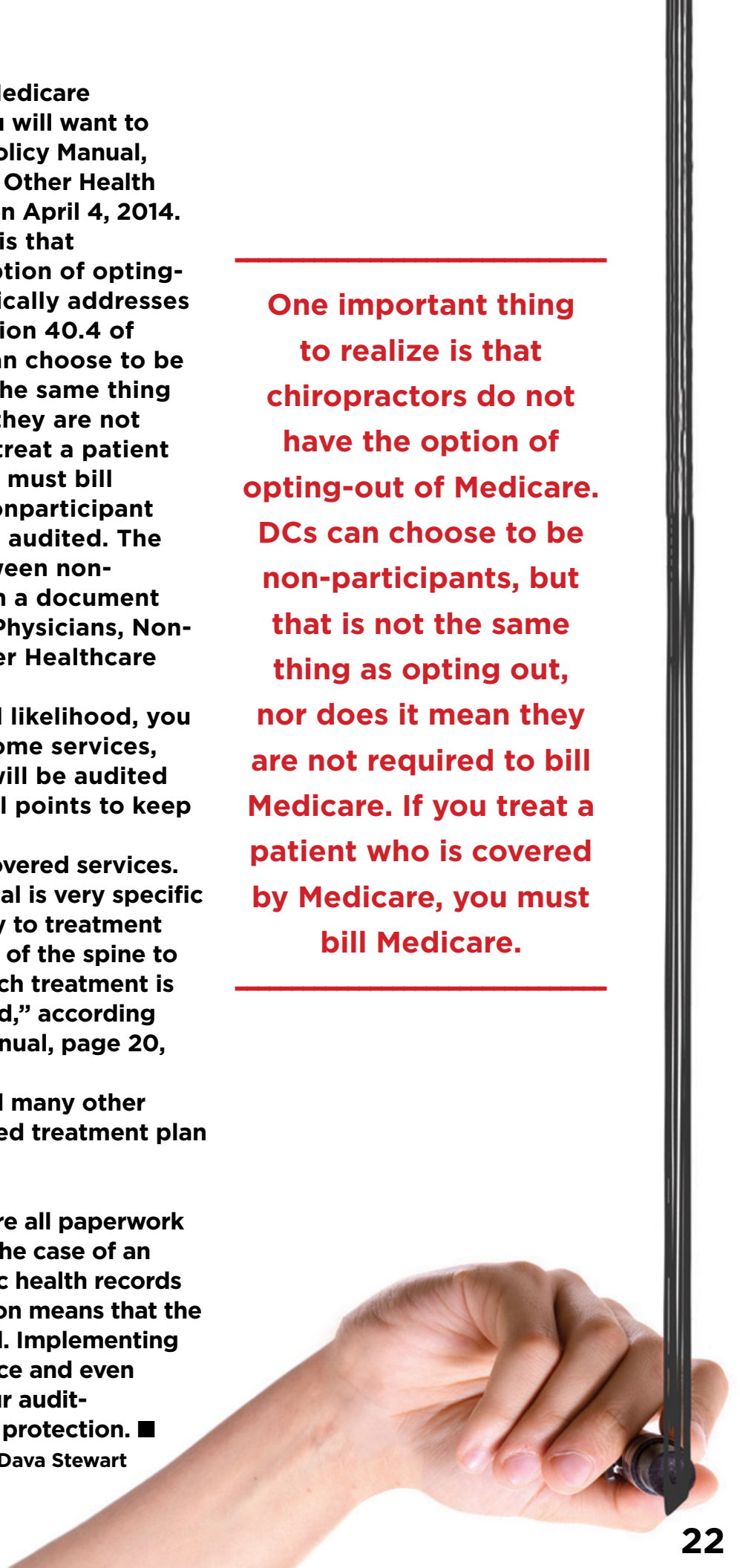
Maintenance therapy, x-rays, and many other services are not covered. A detailed treatment plan must exist.

Visitation notes are crucial.

One of the best ways to make sure all paperwork is in order and will protect you in the case of an audit is to use a certified electronic health records (EHR) software system. Certification means that the system has been vetted and tested. Implementing the system throughout your practice and even hiring a third party to evaluate your audit-preparedness may provide further protection. ■

– by Dava Stewart

One important thing to realize is that chiropractors do not have the option of opting-out of Medicare. DCs can choose to be non-participants, but that is not the same thing as opting out, nor does it mean they are not required to bill Medicare. If you treat a patient who is covered by Medicare, you must bill Medicare.





AVOIDING DISASTER

Learn some of the common violations and deficiencies that have resulted in the levy of fines against DCs.

There's a common fallacy that the only HIPAA offenses that result in fines or punishment are major screw ups. Such as the kind where a patient's information is given to a third party for which there was no written release signed by that patient.

There's currently specific training for auditors so that they can find violations of the new rules for Medicare and HIPAA compliance, and government strike forces can be used for enforcement.

Seemingly minor infractions can oftentimes result in dire consequences, and you need to be aware of — and fix — as many of these issues as possible.

The new $50,000 minimum fines, combined with the potential of losing your license, being required to return payments previously made to you by Medicare or insurance companies, and even facing criminal charges make HIPAA and Medicare regulations a force that can no longer be ignored.

The new $50,000 minimum fines, combined with the potential of losing your license, being required to return payments previously made to you by Medicare or insurance companies, and even facing criminal charges make HIPAA and Medicare regulations a force that can no longer be ignored.

continued>>

The combined efforts of the Office of Inspector General (OIG) and major insurance companies have been strengthened by the addition of the justice department.

They mean business and have recently taken the position that a practice being investigated for Medicare violations should also be investigated for HIPAA compliance and vice versa.

HERE ARE A FEW AREAS OF CONCERN:

- Faxing patient health information (PHI) without following the fax protocol outlined by the OIG. Not using the secured fax line procedures is one of the most frequent complaints cited and the insurance companies are often the ones turning you in. Make sure your practice follows the proper procedures to the letter. Anyone filing insurance is exposed.
- Discussing PHI within earshot of a public area in your practice.
- Having a common therapy area or open reception area where people can overhear conversations. Not taking steps to decrease the carry of voices in your practice can be costly. Give written notification to patients that some of their care may be provided in open areas but that there are private consulting areas available upon request. This is the least you should do.
- Providing only a summary of care and refusing to release actual records.

Faxing patient health information (PHI) without following the fax protocol outlined by the OIG. Not using the secured fax line procedures is one of the most frequent complaints cited and the insurance companies are often the ones turning you in. Make sure your practice follows the proper procedures to the letter. Anyone filing insurance is exposed.

Many doctors don't realize that HIPAA and Medicare auditors will become involved in virtually every aspect of your practice when they decide there is reason to be. You are required to perform annual audits of your charts, to be included in your HIPAA manual. These audits cover topics from diagnosis and treatment plans to trends in claims denial in your practice. They must be documented and signed, and there must be written corrective actions recorded for deficiencies. Without this, it becomes easy for investigators to find subpar practice procedures that can lead to overpayment and patient confidentiality breaches.

- Releasing records to an employer without the patient's permission or a special signed release on file. Just because an employer pays for a patient's insurance doesn't give the employer a right to the patient's health information.

continued>>

- Leaving messages for patients that include PHI, without obtaining prior patient permission. Many practices solve this issue by including a blank space on patient intake forms for patients to indicate phone numbers that are approved for your practice to leave messages. These forms must be signed by the patient to be valid.
- Requiring unreasonable fees for release of records. You cannot deny a patient access to their own records by making copy fees onerous. Charge no more than market rates.
- Withholding records until a balance owed by the patient is paid. If you want to see fireworks explode, let a regulatory agency discover that you were holding a patient's records until a billing dispute was resolved.
- Not having your self-audits completed and documented.

The public is becoming more aware of its rights with the onset of electronic health and medical records.

The reporting of violations is on a strong upswing. When combined with the increase in random audits, the world of compliance becomes more and more dangerous.

Officials of HIPAA and Medicare have indicated that chiropractors and many other specialists have too long ignored the need to become compliant. Therefore, deficiencies in compliance will be considered "willful" in many cases.

This is where the justice department comes in to enforce criminal prosecution relative to audit findings. Don't get caught in the crossfire. Here's how you can take action now:

The public is becoming more aware of its rights with the onset of electronic health and medical records. The reporting of violations is on a strong upswing. When combined with the increase in random audits, the world of compliance becomes more and more dangerous.

- Attend compliance seminars.
- Attend state association license renewals. Many are now requiring regulatory topics be presented.
- Make sure your information is up-to-date. There were new requirements as recent as 2011 and new threats as recent as July 2012.
- Work with professionals who supply training materials for the do-it-yourself-er. It can be done in bite size pieces.
- Have someone come onsite and put your program in place.

Prudent action taken now will be worth far more than the effort you'll need to untangle a compliance problem later. ■

– By Ty Talcott, DC, and Martha McKinney, CPO

chiropractic economics



Web: www.ChiroEco.com



Facebook.com/ChiroEcoMag



Twitter: @ChiroEcoMag



Instagram: @ChiroEcoMag