



Brought to you by the TemPositions Group of Companies - www.tempositions.com

HIPAA Audit Prep: How to Demonstrate Compliance

By Anne DeAcetis
October 31, 2011

Protecting employee privacy is a vital obligation of every employer, especially when it comes to personal health and health care information. But keeping compliant with the laws designed to govern management of this information—HIPAA and HITECH—is a daunting challenge. Companies will soon have to prove themselves up to the task. With HIPAA and HITECH audits on the horizon, it's time to gather the facts, institute smart policies, and get audit-ready.

Marsh & McLennan Agency's Kevin McLaughlin (Director, Professional Liability), assisted by Elissa Palmer (Sales Executive, Employee Benefits), visited TemPositions' HR Roundtable Series on Thursday, October 6, 2011 to share their insights into preparing for audits and navigating the many complex requirements of these laws on a practical, day-to-day basis. They're the first to acknowledge a simple fact: it isn't easy.

"HIPAA seems to be a growing regulation—it keeps manifesting in different ways," McLaughlin explained. "It's something that's very hard to be in compliance with." But, he also noted, there's much that employers can do to protect themselves, even if they fail to meet every standard.

This effort will prove well worth the pain, he stressed. HIPAA audits will be conducted by investigators with "direct monetary incentive" to discover violations and impose fines. HITECH permits "associated firms" to conduct audits—encouraging a new industry of independent investigators-for-hire. And many states, including New York, empower workers to sue in civil courts when they believe information disclosed by an employer has harmed them.

For all these reasons, the costs of noncompliance could be very high. It's time to get proactive, become as compliant as possible, and prepare for the possibility of an audit.

A Brief History of HIPAA and HITECH

HIPAA (the Health Insurance Portability and Accountability Act) was passed in 1996. Intended to bring efficiency to health care delivery systems and enable more Americans to maintain health insurance, it addresses three primary topics: portability, electronic data sharing (Electronic Data Interchange, or EDI) and tax deductions.

HITECH (the Health Information Technology for Economic and Clinical Health Act) is an extension and expansion of HIPAA's rules on EDI. It was passed in 2009 as part of the American Recovery and Reinvestment Act (ARRA), also known as "the Stimulus."

HITECH was created to encourage and further regulate the use of electronic health records (EHR) and digital sharing of Protected Health Information (PHI). But it also increased penalties and liability for HIPAA violations. In 2011, HITECH began providing some incentives to companies that adopted EHR. But in 2015, enforcement will become much stricter.

Both HIPAA and HITECH are governed by the US Department of Health and Human Services (HHS). HHS is one of 18 federal agencies that, under a law called The Common Rule, enforce the same regulations to protect human beings in various circumstances.

The department's web site, www.hhs.gov, can be a very helpful resource, McLaughlin noted. "You can take a look at what's affected by the different regulations," he said. "And there's great information on how this legislation affects you."

HIPAA in Depth

Title I of HIPAA regulates health insurance availability. It addresses portability—how and when workers can maintain their health insurance when they transition from one job to another (whether they leave voluntarily or are terminated). It also limits the restrictions that health insurance companies can place on medical benefits for workers with pre-existing conditions.

Under HIPAA, workers are covered for pre-existing conditions after 12 months (18 months in the case of late enrollment). There are also exceptions when workers can provide proof of continuous coverage.

Some health care plans are exempt from HIPAA requirements, including most vision, dental, and long-term care plans. These benefits are typically add-ons to a general health care plan, and the cost of coverage is tacked on to the total premium. It's important to note that when such coverage is part of an all-inclusive general plan, it is subject to HIPAA rules.

Certain other types of health care-related payments/benefits are also exempt. Payments made by other types of insurance carriers (i.e., auto insurance) are not regulated by HIPAA. And typically, neither are Workers' Compensation benefits—unless the beneficiary is eligible for benefits under Medicare/Medicaid. To ensure these individuals do not receive duplicate payments, their Workers' Compensation benefits must be reported to HHS.

Title II (also commonly known as HIPAA's Administrative Simplification provisions) establishes standards for EDI between employers, health care providers and insurance carriers/brokers. The bill also includes provisions on tax deductions for healthcare, and establishes the government's right to conduct audits and impose penalties.

The EDI Rule

As technology continued to advance in the workplace, McLaughlin explained, electronic data transfers became much more common. HIPAA's EDI Rule was created to control and standardize exactly how the data is shared to help safeguard patient privacy.

Among many other protocols, the EDI Rule establishes codes called the International Classification of Diseases (ICD) that employers, doctors, health care systems and brokers/carriers must use when sharing information about patients/workers. And these codes, McLaughlin explained, have just been substantially revised.

HHS has mandated use of one generation of these codes, ICD-9, since 1979. But HIPAA-regulated entities must transition to ICD-10 in 2013, and the transition will be a challenge. ICD-9 includes approximately 15,000 codes, while ICD-10 will include approximately 155,000.

Of course, employers are only one group regulated by HIPAA. For doctors' offices and health care plans, this change may have a greater impact. But as McLaughlin put it, "HIPAA principles are becoming universalized. I wanted to cover this with you because it offers a glimpse of what may happen for employers."

The Privacy Rule

While EDI is efficient, it's also risky. Networks are vulnerable to hackers, and highly sensitive medical information can be accessed. To mitigate such risks, Title II includes the Privacy Rule, which obligates companies to "reasonably safeguard" patient information and protect it from disclosure—intentional or unintentional.

The Privacy Rule applies to Protected Health Information (PHI), broadly defined as "any medical information that could be used to identify an individual who utilized a healthcare service." PHI spans:

- Employee eligibility for health care plan(s)
- Enrollment and/or disenrollment information
- Health plan premium information for individuals (general plan brochures excluded)
- Health plan premium payments
- First report(s) of injury
- Referrals (authorization and/or certification)
- Any documentation of coordination of health care benefits
- Health care claims and all related information (documentation of doctor visits, physician/staff notes, any attachments included with claims, etc.)
- Health care claim status
- Advice on health care payments and/or remittance

"It's so easy to slip up here," McLaughlin noted, with some sympathy. "Employees are going to ask, 'Why is so-and-so out of the office?' You can only reply, 'They're out. We'll have to work around it and respect their privacy.'"

It's also far harder to safeguard paper files than electronic ones. And many businesses continue to use paper files—including doctors' offices. Faxes are sent over unsecured lines. Folders

containing highly confidential information hang in readily-accessible bins outside exam room doors. But with audits coming, all businesses will have to do better. “Otherwise,” he warned, “they could soon get in a great deal of trouble.”

The Security Rule

The Security Rule was added to HIPAA in 2003, and compliance became mandatory in 2005. It requires employers to proactively guard their Electronic Protected Health Information (EPHI) against “any reasonably anticipated threats or hazards.” EPHI includes electronic records, but also any transmission of paper files over electronic channels—like fax lines.

For now, it’s possible to stay HIPAA-compliant with paper files under the Security Rule, McLaughlin noted. But companies can comply with the Security Rule more easily once they’ve transitioned to computer systems...and they’ll soon be required to do so, under HITECH.

To protect EPHI, the Security Rule requires companies to implement three types of safeguards: Administrative, Physical and Technical.

1) Administrative Safeguards

Administrative Safeguards are general processes that help ensure PHI isn’t disclosed. These privacy rules and procedures must be published in writing and regularly updated. It’s also a good idea to take extra steps to ensure they’re read—and understood. McLaughlin recommended walking employees through these processes in person and/or in small groups.

Limit the number of employees who will have access to PHI, and clearly identify them in your policy. (Curious managers, and even company leadership, should not be granted access if managing EPHI is not central to their positions.) Ensure that all authorized employees have signed relevant, updated employee agreements that mandate compliance with HIPAA.

Address how your company will handle “access authorization, establishment, modification and termination.” Under certain circumstances, you may need to grant temporary access to records to complete specific tasks. Determine how you’ll handle this process and ensure records can’t be accessed inappropriately later. Similarly, make a plan for when employees leave the company.

Companies must demonstrate that they conduct ongoing training on the proper handling of EPHI. McLaughlin recommended using basic sign-in and sign-out sheets, and producing short quizzes for employees to complete. These solutions, while very simple, satisfy this requirement.

Ensure that there’s “management oversight” of these safeguards, McLaughlin stressed. Your written policy should include ongoing processes for supervising and evaluating workers on their compliance. Come up with some easy, common-sense practices, like scheduling quick weekly spot-checks on coding, email practices, filing practices, etc. Take even the smallest violations seriously, and correct them on the spot.

Compliance isn’t only necessary for employees. All third-party vendors must also be HIPAA-compliant. These include insurance carriers and brokers, leasing companies, payroll services,

legal firms, HR consultants, etc. But they may also include IT services and general contractors. Anyone who will work in space where PHI is accessed, McLaughlin warned, must be compliant. The company will be liable for anything they disclose.

Carriers/brokers/etc. should be able to provide certification, so ask for it. Other vendors, like outside IT consultants, must be able to articulate an understanding of HIPAA and commit to compliance.

Administrative safeguards must also include a contingency plan for emergencies. Companies need to demonstrate that they'll know when a breach has taken place (the law holds companies responsible for many things they "knew or should have known") and take appropriate action. When laptops disappear or file cabinets are stolen, McLaughlin noted, you'll need to be ready.

If a security breach involves the records of over 500 people, HIPAA requires companies to immediately inform HHS and issue a formal statement to employees and all affected parties. (For breaches affecting fewer than 500 people, the company can communicate about the incident in their annual report to HHS.)

Typically, meeting this requirement includes issuing a public press release, so consider hiring a PR agency or expert as part of your emergency plan. Disclosures are always unsettling. But you can minimize the damage to your business by handling it in a reassuring manner.

The emergency plan should also address how you'll continue conducting business safely. A hospital, for example, can't afford to stop operating on patients because records are removed or held for ransom by a hacker. Set up redundant systems for EPHI, McLaughlin recommended. Maintain an extra server, or contract with a company that provides encrypted, hosted sites. Back-up systems cost money, but when a breach occurs, they're worth every penny.

Finally, Administrative Safeguards include a published audit procedure. HHS wants to know that if your company is audited, it will be knowledgeable about the process. McLaughlin recommended that attendees visit the HHS web site, where self-audit forms are available.

2) Physical Safeguards

Physical Safeguards help to ensure that EPHI is "physically inaccessible" to unauthorized persons. Simple physical barriers in the workplace offer surprisingly powerful protection.

Keep everything that contains PHI in a restricted area, and physically limit access to people who are authorized to access the information. Your "access controls" should include a waiting area for visitors, sign-in/sign-out sheets, maintenance records (detailing exactly who entered and when the area was accessed for repair), and an escort for every visitor.

Within this secure area, make sure computer screens are pointed away from doorways/walkways and are only visible by the person sitting in front of them. Even an employee who has come in to discuss their own records should not be able to view them onscreen. It's always possible, McLaughlin explained, for an authorized party to accidentally pull up the wrong record.

Ensure your policies include best practices for installing and/or removing hardware and software used to manage PHI. While files can be “deleted,” they never fully disappear from hard drives—and a minimally-talented hacker can retrieve them. So never permit the company to donate PCs or laptops to charity, and always destroy hard drives completely.

3) Technical Safeguards

The Technical Safeguards require companies to protect EPHI within secure “authentication and transmission security systems” so that only authorized personnel can access it. Hackers can get past usernames and passwords easily. But quality encryption systems provide a powerful barrier and should be used across workplace computers, portable systems (laptops) and smart devices.

Companies must ensure that EPHI is not changed or deleted inappropriately. (There’s overlap here with Employee Retirement Income Security Act (ERISA) rules, McLaughlin noted.) So companies must equip their systems to “corroborate the integrity” of their data. When an employee makes changes to EPHI, those changes should include a date stamp, along with the worker’s initials (or other identifying code).

Employers are also required to confirm the identity of any other companies/entities with which they communicate. This means that parties must confirm EDI reaches its intended destination safely. An encrypted email system can automatically alert the sender when a file is successfully sent—while confirming receipt of a paper fax requires a (documented) phone call, every time.

As companies put these Technical Safeguards in place, they’re required to document all their configuration settings. They must conduct, and thoroughly document, an analysis of all risks associated with their system—and their strategies for managing those risks.

The Enforcement Rule

Companies must make all of their HIPAA practices readily available for government review. The Enforcement Rule details the process of HIPAA compliance investigations, and it establishes civil penalties for violations. You won’t get excessive time to prepare in the case of an audit, McLaughlin noted. “If they come in and ask you to tell them what you’re doing,” he explained, “you must answer.”

HITECH in Depth

HITECH was passed to strengthen HIPAA—and also to compel companies to adopt secure information technology (electronic records and encryption) more broadly. Its regulations address the many security concerns that accompany EDI. And, specifically, it imposes penalties for violations that result in breach—including empowering the Office for Civil Rights to enforce the Privacy Rule.

Like HIPAA, HITECH forbids companies from disclosing PHI, intentionally or accidentally. But it further requires that electronic files/data be “unusable, unreadable or undecipherable to unauthorized individuals.” This means emails that contain PHI must be encrypted, whether

they're sent to other parties within the company or to external recipients. If encryption is not available, these emails must at least have password protection.

Technically, HITECH does permit companies to continue faxing records as long as they are viewed only by the intended recipient. But in practice, it will be near-impossible to ensure this—as it's extremely rare for each worker to have their own fax machine. So while faxing has not constituted a HIPAA violation in the past, it will soon constitute a HITECH violation.

Also like HIPAA, HITECH requires companies to report disclosures to HHS. Breaches involving more than 500 individuals must be reported to all affected parties and the media. Breaches involving a smaller number can be included as part of the required annual report to HHS.

HITECH does offer a “safe harbor” from liability, McLaughlin noted, if access to the company's EHR-management system is firmly restricted to authorized individuals. But companies will be liable if they “knew or should have known” about any risk—an extremely broad and ambiguous standard. And without encryption, it's extremely burdensome to guarantee the safety of PHI. A new system, that meets HITECH's standards, will be the more efficient (and defensible) solution.

HITECH specifies that companies must use information technology systems approved by the Certification Commission for Health Information Technology (CCHIT) for the most current year. (In most cases, this is the previous calendar year—a system certified in 2010 would be appropriate for use throughout 2011.)

“These systems are expensive to purchase and implement,” McLaughlin explained, “so do a lot of due diligence.” Your insurance carrier or broker may suggest a vendor, but they're likely to consider their own convenience. Spend time, conduct thorough research, and meet with more than one prospective partner. Make sure they understand your needs—and that they're not new to the industry. “I wouldn't go with a company in its first year of CCHIT certification,” he noted.

This investment will eventually pay off. Encrypted systems for managing EPHI and secure EDI will be far more efficient than any previous solutions, and they're safer. Fax lines are too easy to hack, and paper files are too easy to steal. “Electronic files are easier to control, manage, file, and find,” McLaughlin stressed. “Have you ever misfiled one?”

Common HIPAA Compliance Mistakes

Mistakes are easy to make, but McLaughlin urged attendees to avoid the most common pitfalls:

- Failing to comply with the Security Rule (including updating plan documents and/or associate agreements)
- Failing to properly handle FSAs and wellness programs (this item is unlikely to affect attendees, McLaughlin said, though it's important to understand that PHI includes information about company debit cards used for health-related spending)
- Failing to conduct/document employee training and retraining
- Failing to update notice of Privacy Practices and/or distribute three-year reminders

- Failing to keep an updated, written policy on investigating complaints about privacy (including oral vs. written investigation policies and disciplinary structure)
- Ignoring state privacy laws that interact with HIPAA

State privacy laws enforcing Payment Card Industry (PCI) standards can be particularly challenging, McLaughlin noted. These laws were designed to protect credit card customers from identity theft—but they sometimes include data that employers collect. Perks like transit cards, for example, may soon be regulated by state privacy protection laws as part of PCI.

California SB1386 and AB 1298 are among the strictest statutes involving credit data, though similar laws have been passed in 44 states. And, he noted, many of these laws are “territorial.” California, Illinois and Massachusetts have all passed laws specifying that their residents are protected under their PCI laws, no matter where they’re working when a breach occurs.

Finally, McLaughlin warned, never fail to address concerns raised by your own employees. Individuals report HIPAA violations to the government when they’re angry or feel the company doesn’t take their concerns seriously. Companies will fall short, but they can diffuse many situations before they escalate by demonstrating some sensitivity.

“Have an open-door policy,” McLaughlin stressed. “Thank people for bringing violations to your attention, and assure them you never meant to be non-compliant. Take immediate steps to make sure it doesn’t happen again. Then, follow up with them to let them know you’ve done it.”

The Coming Audits

In the past, HIPAA audits were largely confined to the healthcare industry. Large companies sometimes suffered multimillion-dollar fines—as did CVS, after carelessly disposing of prescription bottles with patient information still affixed. But doctors were treated more gently (during regular “RAC Audits,” they mostly received benevolent advice from independent consulting firms) and employers, for the most part, were investigated least of all.

But now, increased HIPAA audits are coming as part of the Stimulus. Any complaint by an individual—or a security breach that involves more than 500 people—will trigger one. So employers will soon have to fear the same hefty fines as healthcare/medical organizations.

And auditors won’t confine their questions or their searches to any one area of compliance, whether an audit follows a wide breach or a single, specific complaint, McLaughlin warned. Remember, HIPAA auditors will be incentivized to find and punish violations. So expect them to look into all your practices for managing and protecting PHI, your emergency plans, etc.

Fines can be substantial and add up quickly. Miscoding under ICD-10, for example, will result not in a single penalty, but a fine multiplied by the number of instances. Fines for various individual violations will range from \$100 to \$50,000, with an annual maximum of \$1.5 million.

Companies will be able to avoid some fines by correcting their error(s) within 30 days. A company may get a reprieve if they didn’t realize they were violating HIPAA, even after

researching its requirements (this is a nod, perhaps, to the complexity of the law). They may receive leniency if there was some reasonable cause behind the violation, not “willful neglect.” And even in the case of willful neglect, swift changes to become compliant may be rewarded.

Tips for Keeping Compliant

Be Proactive

Attend classes on HIPAA and mine your network for good information. Ask your partners—health insurance carriers, brokers, payroll companies, legal counsel, etc.—to recommend consulting firms and/or best practices for staying compliant.

Appoint a Privacy Officer

Assigning a Privacy Officer is an important first step, Elissa Palmer stressed. It demonstrates that the company understands its obligations—and embraces accountability. The Privacy Officer should become an authority on HIPAA and maintain an open-door policy for fielding and addressing concerns. They should also spearhead policy creation, training and updates.

Conduct an Internal Risk Assessment Audit

Look closely at all the systems and processes you currently use to manage PHI. Identify potential risks, and mitigate them as much as possible. Pay special attention to email use, McLaughlin noted. Recently, one third of all large companies investigated privacy disclosures via their own email systems. More than 25% determined it was “common” or “very common” to find privacy-protected information, including PHI, in emails leaving the company.

Implement General Principles for Use and Disclosure of PHI

HHS offers very clear guidelines on the appropriate use and disclosure of both PHI and Personal Identifiable Information (PII). Visit this information on the HHS web site. Consider how your own company handles this information, and be ready to make changes to achieve compliance.

Publish a HIPAA Policy and Procedure Manual

Draft a manual that specifically guides employees on complying with HIPAA and HITECH—and educate them on the consequences of non-compliance, both internal and external. (Be sure it includes an “Email Acceptable Use” policy). Clearly identify the company’s Privacy Officer, and require employees to report any breaches or possible violations.

Distribute a Memo and the Manual to Staff

Don’t just slip your new manual into employee orientation packets. Announce it with a written memo, as an individual piece of must-read material.

Launch a HIPAA-compliance Training Program

Add a detailed session on HIPAA compliance to orientations for all (relevant) new employees—and plan to repeat this training once a year. Remind workers that if they discover a HIPAA violation, risky practice or breach, they must report it to the Privacy Officer.

Implement All Technical Safeguards and Supporting Practices

As much as possible, stick to practices that are compliant with HIPAA and HITECH (encryption, emergency planning, etc.). Ensure compliance with your “Email Acceptable Use” policy by using filters that flag HIPAA-protected content—and deal firmly with any slip-ups. Remind employees about acceptable practices, and enforce discipline as necessary.

Consider obtaining Privacy Protection Insurance. In the event of a breach, McLaughlin explained, these policies can cover liabilities, costs for your defense and PR/notification needs, corporate income losses, identity theft(s), and other related financial burdens.

Execute Confidentiality Agreements with Relevant Employees

Anyone at the company who works with PHI must sign a confidentiality agreement that acknowledges HIPAA compliance as an obligation. Be sure to include a clause that specifies this confidentiality extends beyond employment (i.e., if the worker leaves, they cannot disclose any PHI they may have been exposed to during their time with the company).

Follow ARRA and, as appropriate, the Red Flag Rule

Compliance with intersecting laws can also help you during an audit. Familiarize yourself with the Stimulus as it relates to employers. (This law is what gives HIPAA auditors their teeth.) And, as appropriate to your business, act in compliance with the Red Flag Rule. It’s an identify-theft prevention law mostly aimed at banks and creditors, but it holds some employers responsible for safeguarding information about a range of transaction accounts.

Stay Vigilant

Through every phase of the employment process, protect privacy—aggressively. Perform background checks on appropriate candidates. And never stop supervising employees that handle PHI, even after they’ve seemingly earned the company’s trust. “The most common workplace thieves are the most trusted workers,” McLaughlin explained.

Stay Educated, Stay Proactive, Stay Audit-Ready

Even if the face of HIPAA and HITECH’s vast and ever-changing requirements, McLaughlin said in closing, there are many steps that companies can take to prove they are aiming for complete compliance. Familiarize yourself with the requirements. Institute the necessary policies. Distribute and maintain clear manuals. Train employees thoroughly, and regularly. And finally, document all of these efforts. Assume the audit is coming.

The hardest part of making any change is getting started, McLaughlin said. The most important thing is to bite the bullet and get started, now. “The changes you make don’t have to be radical at first,” he explained. “But it’s time to start creating the case that what you’re doing is defensible.”

Anne DeAcetis is a freelance writer based in New York. Reach her at anne.deacetis@gmail.com.

The HR Roundtable is a breakfast forum for human resources professionals in New York City sponsored by The TemPositions Group of Companies. TemPositions, one of the largest staffing companies in the New York tri-state area with operations in California, has been helping businesses with their short- and long-term staffing needs since 1962. Visit them online at www.tempositions.com or email them at info@tempositions.com.