Staying Well Within The Law

A newsletter on the current legal issues facing today's health care Industry

Fox Rothschild LLP
ATTORNEYS AT LAW

Third Quarter 2013

What You Need To Know About the HIPAA Mega-Rule

By William H. Maruca

The long-overdue HIPAA/HITECH "Mega-Rule" is finally in effect. The Department of Health and Human Services published the Omnibus Rule in the January 25, 2013 *Federal Register* after missing several predictions of its imminent release. The four-part rule modified the HIPAA Privacy, Security and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act; adopted changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act; finalized the rule for breach notification of unsecured protected health information (PHI); and implemented the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes. The final rule took effect on March 26, 2013, but health care providers and other covered entities (and their business associates) generally were required to modify their policies and meet new requirements by September 23, 2013.

Some of the more relevant features of the omnibus rule include:

Business associates will now be directly liable for compliance with the HIPAA Privacy and Security Rules. Further, more entities will be defined as business associates, including companies that maintain PHI such as storage facilities and cloud computing/data storage vendors (but not those that only transmit the PHI and do not regularly access the content of the PHI, such as telecommunications providers or couriers). Additionally, business associates' subcontractors will be treated as business associates themselves, subject to primary liability exposure. Business Associate Agreements must be updated by September 23, 2013, except where valid agreements were in place on July 25, 2013, in which case the deadline may be extended up to an additional year.

Use of PHI for marketing and fundraising purposes is restricted, and individuals must be given the opportunity to opt out. The sale of protected health information without individual authorization is prohibited.

Individuals have the right to prevent disclosure of records of any treatments they have personally paid for. Some individuals choose to pay out-of-pocket for care that they consider potentially embarrassing or compromising, such as mental health or drug and alcohol treatment, and they will be able to prevent the further release of any information regarding such care.

Unauthorized disclosures of PHI will be presumed to be reportable breaches unless the covered entity can show that there is a low probability that the protected health information has been compromised. A minimum of four factors must be taken into account and documented when determining whether a disclosure is a reportable breach: the nature and extent of the disclosed information; the person to whom the disclosure was made; whether the information was actually acquired or viewed; and the extent to which risk to the information has been mitigated. For example, a single fax containing only a patient's name and address that is mistakenly sent to the wrong physician, when that physician is immediately notified and agrees to destroy or return the fax, may present a low probability that the information has been compromised. By contrast, a lost laptop containing unencrypted patient data including birthdates, Social Security numbers and diagnoses, where the covered entity cannot determine who has found the laptop or whether anyone has seen the data, would represent a much greater risk of compromise. Remember that data encrypted in accordance with the standards of the National Institute of Standards and Technology (NIST) is generally not considered "breached" when inadvertently disclosed, such as when devices containing such data are lost or stolen. Too many covered entities and business associates have failed to implement encryption policies that could have prevented disaster.

Covered entities should act soon to work with knowledgeable counsel to take necessary steps to comply with the omnibus rule, including:

- Identify all business associates, including those newly designated under the new rule, and review and update business associate agreements;
- Review, update and redistribute your Notice of Privacy Practices;
- Review and revise your breach analysis and notification policies and procedures; and
- Review your security policies, particularly with regard to mobile devices and "bring-your-own-device" technology, and implement NIST-compliant encryption wherever possible.

As recent high-profile enforcement actions have indicated, the risks for ignoring your HIPAA/HITECH responsibilities can be catastrophic, and the highest penalties apply in cases of "willful neglect."

A version of this article first appeared in the April 2013 issue of *Western Pennsylvania Healthcare News* and is reprinted here with permission.

In This Issue:

Author

William H. Maruca
412.394.5575
wmaruca@foxrothschild.com

Managing Audit Demands

By Elizabeth J. Hampton

Given the efforts underway to reduce the cost of health care, audits by private payers are on the rise. While that trend likely will continue, providers can and should prepare in advance to meet the audit challenge. There are a variety of best practices to employ before, during and after an audit to alleviate the stress of scrutiny that an audit notice can bring to your medical practice. Understanding why audits are initiated is the first step in successfully navigating through the process.

Why My Practice?

The answer to this question ranges from random selection to targeted investigation. While audits may be random, insurers tend to focus on opportunities to procure overpayment recoveries. For example, practices that maintain billing practices or patterns that vary with those of their peers may be subject to heightened scrutiny. Other audits may be initiated based on a new type of service or treatment offered and billed by the provider. Frequently, audits and investigations are triggered by a patient complaint or a disgruntled employee. Understanding the reason for the audit can be helpful but not always possible. However, if you receive an audit demand and your practice falls into one of these categories, you will have a better idea of the factors precipitating review.

Before the Audit

The best way to prepare for a future audit is to do one before an insurer sends you a demand. Have you looked at your practice lately? Are your patient files properly documented? Are your provider policies up to date? Performing random internal audits may bring light to issues in your practice that you should address before a payer demands to take a look.

Assuming that appropriate precautions are taken to protect private health information (PHI), outside coding experts can be retained to perform a more extensive review of your documentation and billing procedures and offer guidance from a payer audit perspective. Aside from internal documentation reviews, practices should advance efforts to ensure that staff members are properly trained and supervised. Written policies regarding patient files, communication, documentation and privacy issues should be updated, and employees should be responsible for understanding these policies and the role they serve within the practice.

The Audit Notice

So you received an audit notice. Now what? Before discussing the demand with anyone, read it carefully. The contents of the notice may provide information helpful to determine the type of audit requested and the time period in which the practice needs to respond. Take note of who prepared the audit notice. Is the notice directly from a private payer or another company that may work for the payer? If the notice is signed by an investigator, he will often list the initials "S.I.U." near his signature. The "S.I.U." reference means "Special Investigation Unit," a designation maintained by individuals specifically trained in fraud detection.

Once you have reviewed the audit demand, consult with an attorney who has experience assisting clients in this area. Do not talk about the notice with your staff or any other third party until you have had the opportunity to speak with counsel and you are directed accordingly.

During the Audit

Many providers are tempted to speak with the auditor at length before and during the audit. Resist the urge to do so by understanding that the auditor's goal is to find overpayments and anything you tell the auditor can be misconstrued in favor of that result. While there are appropriate ways to communicate to discover information, do not attempt to do this discovery on your own. If an auditor has questions regarding your practice, ask him or her to put questions in writing so that you have an opportunity to carefully evaluate the questions with your counsel.

Look for your attorney to advise you regarding the scope of the audit to ensure that you are providing only what is lawfully requested. Since most audits take place within the practice's office, designate a room in advance for the audit that will not interfere with your work.

After the Audit

Choosing a course of action (or not) following an audit depends upon a variety of factors.

First, has the auditor shared any findings of the audit? Have you been advised that documentation is missing or bills have been improperly coded? If the auditor shares information along this line, listen carefully. Minor documentation issues typically can be resolved while other more significant or pervasive problems may result in substantial liability. It may be difficult to discern whether your practice needs to correct minor issues or whether the audit finding will lead to a more extensive investigation of your practice.

However, if your initial audit concludes and demands to examine additional records and files follow, you may expect that the insurer has directed a continuing investigation of your practice. On the other hand, and in many cases, audits begin and end without incident. Regardless of the audit response, be sure to maintain copies of each and every item requested by and provided to the auditor and consult with your attorney throughout this process.

The development of a best practice approach to survive the audit process will help to reduce audit anxiety, yield favorable audit outcomes for providers and build stronger practices.

Author

Elizabeth J. Hampton
609.895.6752
ehampton@foxrothschild.com

Rising to the Challenges of the Evolving Reimbursement Environment

By William H. Maruca

Health care in the United States is undergoing another episode of dramatic change, but its significance has been amplified by highly polarized politics, online media sources and the 24-7 news cycle. Forward-thinking hospitals and provider networks can position themselves to seize opportunities and minimize heightened risks presented by this turbulent time, but only if they develop effective data gathering and analysis tools.

Despite the firestorm that continues to rage over the Affordable Care Act ("Obamacare" to its opponents), the reimbursement changes it includes are relatively incremental and, in many cases, optional. Contrast them with the radical realignment that was suddenly ushered in by the advent of DRGs in 1983 under the Medicare prospective payment system, which required hospitals to rapidly adapt to fixed fees per admission after decades of cost-based Medicare reimbursement. DRGs led hospitals to focus on cost control and lengths of inpatient stays but also incentivized the growth of outpatient diagnostic and treatment services (and their associated costs), which were not subject to the same limitations.

The changes to today's reimbursement world are driven by trends that move away from fee-for-service payment models and toward pay-for-performance, accountability for outcomes and care coordination and value-based purchasing. These changes are being aggressively pushed by the Center for Medicare and Medicaid Innovation (CMMI), private insurance initiatives, purchaser coalitions, proactive providers and the development of hybrid payor/purchaser entities.

Among the CMMI initiatives are both well-publicized programs such as the Shared Savings Program for Accountable Care Organizations (ACOs) and the Bundled Payment Initiative, as well as a long list of lesser-known pilot programs and payment/delivery models, more than 40 in all, that can be explored at http://innovation.cms.gov/initiatives/index.html. Now that CMMI has survived the Supreme Court's 2012 ACA ruling and the 37 (and counting) symbolic repeal attempts in the House, the agency continues to promote and evaluate a variety of alternative payment mechanisms in an ongoing search for one or more magic bullets that can bring health costs under control.

Accountable care appears to be the most popular of the various models so far. CMMI reports that there are now more than 250 ACOs participating in the shared savings program, including 106 new ACOs added as of January 2013. One in 10 Americans is now being treated by an ACO provider, according to Richard Weil, Ph.D., of the Oliver Wyman Group consulting firm. Half of all ACOs are physician-led organizations that serve fewer than 10,000 beneficiaries, and 20 percent of ACOs include community health centers, rural health clinics and critical access hospitals that serve low-income and rural communities.

The Bundled Payment Initiatives, which in some ways can be described as "ACO-lite," are surprisingly slower to catch on. This initiative combines payments to hospitals, physicians and ancillary providers into a single payment for 48 defined "episodes of care," such as congestive heart failure or joint replacement. Applicants can select the episodes they want to bundle and pick from four variations covering inpatient and/or outpatient care and prospective or retrospective fee structures.

Only one provider is participating in the retrospective acute care inpatient model so far; 55 in the retrospective acute and post-acute care model; 14 in the post-acute care model; and 37 in the prospective acute care model. Since under each of these models applicants can select only those lines of business in which they have confidence that they can deliver care at a cost savings, it suggests that relatively few health systems and networks believe they have developed the technical capability and infrastructure necessary to monitor and control such costs in real time while ensuring quality.

As it stands, the CMMI approach remains voluntary, and only the best-prepared providers choose to participate in their initiatives, so it is premature to guess whether any combination of accountability, pay-for-performance, bundled payments and similar approaches would prove effective if imposed across the board. In the meantime, private payors, particularly on the West Coast, are increasingly implementing similar efforts on a larger scale, and large health care purchasers continue to demand proof of cost-effectiveness beyond the old fee-for-service system. Providers who dip their toes in the unfamiliar waters of alternative reimbursement methods, at limited risk, will be better prepared if they are ultimately tossed into the deep end by sweeping changes.

This article first appeared in the July 2013 issue of *Western Pennsylvania Healthcare News* and is reprinted here with permission.

Author

William H. Maruca
412.394.5575
wmaruca@foxrothschild.com

New Jersey Provider Protections for the ACA Grace Period Provision

By Michael Coco and Elizabeth G. Litten

The passage of the Affordable Care Act (ACA) in 2010 reigned in a new era of federal health care oversight, along with many unanswered questions and rising anxiety among patients, providers and insurers. Among those questions were how the ACA's "grace period" for coverage purchased on an insurance exchange would be interpreted and how that provision would balance the interests of insurers, patients and providers alike. The grace period requires "[a]n issuer of a qualified health plan" to "allow a 3-month grace period for nonpayment of premiums before discontinuing coverage."[1] This allows

[1] 42 USC 18082 (c)(2)(B).

patients who purchase a Qualified Health Plan (QHP) on the exchange who miss making premium payments for three months to continue being covered under their plans. Pursuant to the regulations implementing this provision, an insurer may terminate a member after three months of nonpayment, so long as the insurer provides the requisite notice.[2]

The grace period does not apply to every new health plan, but applies to those plans that are paid for with a premium tax credit. This tax credit is not available to all patients. Rather, applicants for the premium tax credit must fulfill several requirements. For example, such applicants must have a household income of greater than or equal to 100 percent but not more than 400 percent of the federal poverty level.[3]

Originally, the Centers for Medicare and Medicaid Services (CMS) proposed a rule that required insurers to pay claims for coverage during the grace period. That provision, however, was modified in the final rule. In attempting to strike a balance between the rights of the three parties, CMS allowed the insurer to pend payment of claims during the second and third months of delinquency, but required the insurer to continue to pay claims during the first month. Under current New Jersey law, insurers are required to allow a 31-day grace period for nonpayment of a premium.[4] By contrast, the new ACA regulation requires insurers to keep patients enrolled in health plans for three months following nonpayment of a premium, but allows the insurance carrier to hold provide payments for months two and three. This situation poses a significant financial risk to providers.

Currently, New Jersey law requires "prompt payment of claims" on provider bills submitted via electronic means. "Prompt payment" is defined as no later than 30 days.[5] This provision may conflict with the ACA's allowance of the three-month grace period for individuals receiving an advanced premium tax credit. In many circumstances, federal rule preempts state law, where the two conflict directly. However, in instances in which a state law creates a more stringent requirement, the state law may prevail notwithstanding a more lenient federal requirement. Ultimately, the conflict between these two provisions may have to be decided by a court. In any event, the 31-day state law provision would still apply to all QHP Exchange-covered patients not receiving an advanced premium tax credit.

The ACA regulations do require insurers to notify providers in the second and third months of nonpayment, but provider advocacy groups are concerned that such notices will come late or not at all. Thus, under the new health care payment landscape, providers could end up treating a patient for two months before realizing the patient is no longer entitled to insurance payment benefits.

The interplay between the ACA statute and the implementing regulations strikes another blow to providers. Because the ACA allows for the three months' grace period before "discontinuing coverage," the patient is still technically covered by the policy during this time, yet claims for services rendered in the second and third months of the grace period may not be getting paid. This may result, for example, in the provider being bound by the health plan's allowable claim limits and/or balance billing rules because the patient is still technically covered under the insurance policy even though the insurer is not obligated to pay claims. However, the regulations do allow for coverage termination to be retroactive to the first month.[6] For example, if a patient fails to pay the premium for March and fails to pay the next two subsequent premiums, coverage will be terminated retroactively back to March 31.[7] Providers can then bill patients directly for April and May.

What solutions are there for providers that fear being left uncompensated for two months of payments? One option is not to accept patients on an individual Exchange-purchased QHP (an option to be chosen carefully, and only if the provider is not contracted with the QHP to render services to such patients, the services are nonemergent, and no other state or federal law obligates the provider to render the services), or to provide care on a cash basis only, but these options are not a reality for many providers.

There are, however, some safeguards that providers can put into place to mitigate the grace-period provision. One action for providers is to reach out to the Exchange Plan and set up an electronic notification system that would immediately send the provider a notice once a patient defaults on an insurance premium for the first time. To add teeth to this provision, providers could include an indemnification provision in their participating provider contract during the next negotiation term whereby the Plan would have to indemnify the provider for its costs and expenses if the insurer fails to notify the provider within a set time period following the first missed premium payment.

Another safeguard providers can implement is to check a patient's insurance status before major procedures. Although it may be burdensome to check current insurance coverage for every visit, providers may want to set a dollar amount that triggers an insurance check. If the patient's estimated cost for that visit or that specific procedure exceeds a specified dollar amount, then the provider could check with the insurance company regarding coverage to find out whether a nonpremium payment notice has or will be sent. Such a system would need to accommodate a large number of inquiries from various providers and report insurance status with the confidence to ensure providers do not render care for

---

[2] 45 CFR 156.270(d); 77 Fed. Reg. 18310.

[3] 45 CFR 155.305(f).

[4] New Jersey Division of Banking and Insurance, available at: http://www.state.nj.us/dobi/division_insurance/ihcseh/ihcguide/keyfeatures.html#guarantee

[5] N.J.A.C. § 11:22-1.5.

[6] 72 Fed. Reg. 18310, 18427 (March 27, 2012).

[7] Although the ACA has been interpreted to allow retroactive termination, the plain language of the statute allows for a three month grace period "before discontinuing coverage," which could result in a legal challenge in the future.

free and ensure patients are not inappropriately denied medical care based on an insurer's error.

New Jersey hospital providers have the option of making financial arrangements prior to rendering a service or performing a procedure in a nonemergency situation. Such arrangements are only available where the patient does not furnish proof of health insurance and is not eligible for Medicaid, charity care or other state assistance programs.[8] In these uncommon cases, the hospital may require proof of financial ability prior to performing a nonemergency procedure or treatment. Medical screening exams under EMTALA and related state laws would still apply. It is unclear whether a hospital that verifies a patient's premium payment delinquency with the health plan can enter such a payment arrangement, given the patient's status as, technically, covered under the plan during the grace period.

However, such providers could consider arranging a type of "security deposit" system, after checking to see if their contract with the QHP and applicable state law allows. After receiving notice of the patient's failure to pay the first premium, providers could ask for a security deposit for nonemergency provider services. Once the provider receives payment from the health plan, the patient's security deposit would be returned. Physician providers should, however, take caution not to abruptly discontinue their relationship with a patient in violation of their state's licensing requirements. For example, the New Jersey Board of Medical Examiners (BME) regulations require providers to give patients 30 days' advanced notice before discontinuing the patient-physician relationship, and physicians cannot discontinue the relationship during the course of treatment.

While health care providers, unfortunately, appear to have few tools to protect themselves against the ACA grace period provision, by combining some of the suggestions made in this article, providers may be able to reduce some risk of patient default. In the end, some providers may either have to hold out for more "clarification" on how to manage during the grace period, accept insolvent patients as a part of doing business or move to an all-cash model.

Authors

Michael Coco
609.844.3025
mcoco@foxrothschild.com

Elizabeth G. Litten
609.895.3320
elitten@foxrothschild.com

[8] N.J.S.A. 26:2H-18.63.

Avoidable HIPAA Nightmares

By William H. Maruca

You may be familiar with the adage, "There is no such thing as bad publicity as long as they get your name right." One place you don't want your organization's name to appear is on HHS's "Wall of Shame." That's the informal name of the list published by the U.S. Department of Health and Human Services (HHS) that posts large breaches of unsecured HIPAA privacy breach incidents affecting 500 or more individuals. Smaller breaches must be reported to HHS annually and are not subject to public disclosure.

As of July 17, 2013, 627 breaches of unsecured protected health information (PHI) were reported on the Wall of Shame. However, these publicly posted breaches represent less than one percent of all reported breaches. During the period of September 2009 through May 31, 2012, there were more than 57,000 reports of breaches involving fewer than 500 individuals.

What can you do to avoid this kind of ugly publicity and liability exposure? First, focus on the areas of greatest risk. Based on a 2012 report by HHS's Office of Civil Rights (OCR), theft and loss represent 65 percent of large breaches. Laptops and other portable storage devices account for 38 percent of large breaches, paper records are 24 percent and desktop computers account for 15 percent. Only 14 percent are associated with improper access to email, network servers or electronic medical records. Accordingly, a lot of data is getting into the wrong hands via physical objects – smartphones, tablets, thumbdrives, laptops and old-fashioned paper records.

There is an effective solution to most of these breaches (other than the paper kind): encryption. If you're not routinely encrypting all of your PHI, or if you don't know whether it is being encrypted, make this your first priority.

A breach is defined as an impermissible use or disclosure that compromises the security or privacy of the PHI. An unauthorized disclosure is presumed to be a breach unless it can be demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment that considers the nature and extent of the PHI involved; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; and the extent of mitigation efforts.

This is where encryption comes in. Only breaches involving "unsecured" PHI must be reported. If data is encrypted in a manner consistent with the standards the National Institute of Standards and Technology (NIST), such data will be considered to be "rendered unusable, unreadable, or indecipherable to unauthorized individuals persons" and therefore no longer "unsecured."

Staying Well Within The Law

Many of the widely reported breaches and enforcement actions have involved large health systems and insurance companies, but don't let that trend lure you into complacency. In 2012, a two-physician practice in Phoenix agreed to pay HHS a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the PHI of its patients. This occurred after an investigation into an improperly secured internet-based appointment calendar revealed that the practice had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules and had limited safeguards in place to protect patients' electronic data. Earlier this year, a small hospice agency, The Hospice of North Idaho, agreed to pay a $50,000 fine, representing the first settlement involving a breach affecting fewer than 500 individuals.

Another priority should be to limit the use or disclosure of PHI to the "minimum necessary" to accomplish the intended purpose. Cedars-Sinai Medical Center in Los Angeles recently reported that 14 patient records were accessed by unauthorized persons, including employees of independent physician practices. (Reportedly, the records were those of reality TV personality Kim Kardashian). In 2012, a court upheld the conviction and prison sentence of a UCLA employee who had peeked at celebrity records even though the information was not further leaked, sold or used improperly. UCLA also agreed to pay a civil fine of $865,000. Providers and their IT vendors should develop safeguards to restrict access to records to those with a legitimate need to see them.

These suggestions are merely some of the low-hanging fruit that can significantly reduce your HIPAA exposure. To ensure you are in full compliance by the deadline of September 23, 2013, consult knowledgeable counsel.

This article first appeared in the August 2013 issue of *Western Pennsylvania Healthcare News* and is reprinted here with permission.

Author

William H. Maruca
412.394.5575
wmaruca@foxrothschild.com

Fox Rothschild LLP
ATTORNEYS AT LAW

About the Health Law Practice

Fox Rothschild's Health Law Group comprises more than 40 attorneys who counsel clients locally, regionally and nationally. Our multioffice, multidisciplinary approach allows us to offer practical, cost-effective solutions to issues faced by longstanding stakeholders, as well as a variety of industry newcomers.

For more information about any of the articles in Staying Well Within the Law, please contact any member of the Fox Rothschild Health Law Practice. Visit us on the web at www.foxrothschild.com.

Practice Co-Chair
David S. Sokolow
215.299.2712 or 609.895.3308
dsokolow@foxrothschild.com

Practice Co-Chair
Todd A. Rodriguez
610.458.4978
trodriguez@foxrothschild.com

Newsletter Editor
William H. Maruca
412.394.5575
wmaruca@foxrothschild.com