SEMINOLE COUNTY MEDICAL SOCIETY

September 17, 2013

HOT LEGAL TOPICS

BY

THE HEALTH LAW FIRM

Michael L. Smith, R.R.T., J.D.
Christopher E. Brown, J.D.
Lance O. Leider, J.D.

---

1. HIPAA OMNIBUS FINAL RULE EFFECTIVE SEPTEMBER 23, 2013.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules were amended by an Omnibus Final Rule published by the U.S. Department of Health and Human Services (HHS) in January 2013. The Omnibus Final Rule marks the most significant changes to the HIPAA privacy and security Rules since they were first implemented. These changes greatly enhance a patient's privacy rights and protections, and also strengthen the ability to enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider or one of their business associates.

The most significant changes involve business associates who are now directly subject to the mandates of the HIPAA privacy and security rules, and HIPAA enforcement. In addition, covered entities will need to evaluate changes to the breach notification rule, individual rights, additional requirements for Notices of Privacy Practices (NPPs) and the guidelines around the use of protected health information (PHI) for marketing and fundraising initiatives.

The HIPAA Omnibus Final Rule will go into effect on September 23, 2013. By this date, hospitals, physicians and all covered entities must comply with the HIPAA Omnibus Final Rule. The amendments to the rule are available on the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) website.

Covered entities should be performing HIPAA risk assessments to identify their security risks and implement protections before a data breach occurs. HIPAA has always required covered entities to perform HIPAA risk assessments. Very often, the first question the OCR asks when investigating a possible HIPAA violation is what risk assessment the health care provider performed.

The HIPAA security rule does not require a specific risk assessment process. The HIPAA security rule does specify objectives that the risk assessment should accomplish. The objectives of an adequate HIPAA risk analysis are:

1. Identify the scope of the analysis - the analysis should include all the risks and vulnerabilities to the confidentiality, availability and integrity of all electronic health information regardless of its location.
2. Gather data - the covered entity must identify every location where electronic data is stored.
3. Identify and document potential threats and vulnerabilities - the covered entity should consider natural threats, human threats and environmental threats.
4. Assess current security measures - the covered entity must examine and assess the effectiveness of its current measures.
5. Determine the likelihood of threat occurrence - the covered entity should evaluate each potential threat and prioritize its plan to address each threat.
6. Determine the potential impact of threat occurrence - the covered entity should assess the possible outcomes of each identified threat such as unauthorized disclosure of confidential information.
7. Determine the level of risk - the covered entity should categorize each risk and plan its procedures to mitigate any damage cause by each risk.
8. Identify security measures and finalize documentation - the covered entity should throughly document all the steps it used in its risk assessment process.

2. UPDATED STANDARDS FOR PHYSICIAN MEDICAL RECORD REQUIREMENTS RELATED TO COMPOUNDED MEDICATIONS.

The Florida Board of Medicine and the Florida Board of Osteopathic Medicine published new requirements for medical record documentation related to compounded medications administered to patients in an office setting. These standards became effective September 9, 2013. The standards are contained in Florida Administrative Code Rules adopted by each board.

We believe the updated requirements are a result of the recent recalls of tainted compounded

medications that have spread across the country and infected thousands of patients. These new standards will make it easier for health care professionals to trace drug reactions and spot tainted batches of medications quickly. The new changes apply to the exact documentation required anytime a compounded medication is administered to a patient.

For the Florida Board of Medicine this is an update to Rule 64B8-9.003, Florida Administrative Code. For the Florida Board of Osteopathic Medicine this is an update to 64B15-15.004, Florida Administrative Code.

3. WHISTLEBLOWERS ARE SOUNDING THE ALARMS.

We have seen an increase in whistleblower/qui tam cases filed by physicians, nurses or hospital staff employees who have some knowledge of false billing or inappropriate coding taking place. Halifax Health and Shands Healthcare are two recent examples.

> The U.S. Department of Justice (DOJ) alleges Halifax Health compensated six oncologists and three neurosurgeons based on patient referrals to the hospital. A Halifax employee filed the whistleblower lawsuit in 2009, and the DOJ joined the case in 2011. The government is seeking between $725 million and $1.14 billion, alleging Halifax Health submitted false claims to Medicare. This case is scheduled for trial in March 2014, in federal court in Orlando.
>
> In August 2013, Shands Healthcare agreed to pay $26 million to settle a lawsuit that stemmed from a whistleblower/qui tam claim. Six of Shands' Florida hospitals were accused of billing government health programs, such as Medicare and Medicaid, for inpatient claims that should have been coded as outpatient services for five (5) years.

Just this year, we've noticed the government become more aggressive in its anti-fraud and recovery efforts. Now that the government is collecting more money, you can expect their efforts to get worse. Also, since whistleblowers stand to receive up to thirty-five percent (35%) of a recovery made by the government, plus attorney's fees and costs, you can expect more whistleblower lawsuits to be filed. Therefore, it is now more important than ever to verify accurate billing and coding.

4. 2014 IPPS FINAL RULE EFFECTIVE OCTOBER 1, 2013.

The Centers for Medicare and Medicaid Services (CMS) released the 2014 Inpatient Prospective Payment System Final Rule (the 2014 IPPS Final Rule). The compliance date is October 1, 2013. It affects how hospitals will bill for observation stays, long outpatient stays and short inpatient stays.

The 2014 IPPS Final Rule clarifies that the physician order must clearly document the physician's intent for inpatient status and must be present in the medical record in order for a

claim to be paid. The 2014 IPPS Final Rule also creates a requirement that physicians admitting patients must complete a certification document for every inpatient admission. CMS' position is that inpatient admission only qualifies for payment when the physician expects a patient to stay two nights and admits that patient on that expectation. Inpatient admission also qualifies for payment when the patient is undergoing a procedure on the inpatient-only list.

After October 1, 2013, CMS will instruct its medical review contractors to focus auditing efforts on inpatient hospital admissions. To avoid audits and delays in payments, hospital physicians should become familiar with how the 2014 IPPS Final Rule will affect their practice procedures.

5. ICD-10 IS COMING: GET READY FOR THE TRANSITION.

Whether you are ready or not, on October 1, 2014, ICD-9 codes will be replaced with ICD-10 codes. This switch applies to all HIPAA compliant health care providers.

The transition from ICD-9 to ICD-10 will impact health care professionals, providers, billers, health plans, and anyone who analyzes health care claims data. As providers move to ICD-10, there will likely be an increase in fraud and misrepresentation stemming from coding confusion and compliance issues. If a health care provider incorrectly codes a diagnosis, the subsequent treatment can be subject to review or an audit. After October 1, 2014, all diagnoses will need to be coded and documented correctly in order for the provider to receive reimbursements.

To learn the latest ICD-10 news and access more resources, visit the CMS website at www.CMS.gov/ICD10. You can also contact Seminole County Medical Society to learn more on training and compliance events.

6. DSM-5 RELEASED: THE BIG CHANGES.

The American Psychiatric Association (APA) published the fifth version of its Diagnostic and Statistical Manual of Mental Disorders (DSM-5) in May 2013. DSM-5 is a widely used handbook for psychiatrists, psychologists and health care professionals to access and diagnose mental disorders. This manual determines what counts as a mental disorder, therefore what insurers will cover. DSM-5 accounts for the abundance of new research and knowledge about mental disorders. It also includes new diagnoses for mental illnesses such as communication disorders, new depressive disorders and certain impulse related disorders.

DSM-5 diagnoses are often key factors in the assessment of Americans with Disabilities (ADA) claims. It is important for employers to become familiar with the manual as to be able to determine if a mental illness diagnosis qualifies as a disability.