MAY 2010

HOSPICE ENDNOTES
for the North Carolina Hospice Community from Poyner Spruill LLP

Social Media: A Blessing or a Curse for Providers?

By Kim Licata

Twitter, Facebook, LinkedIn, YouTube...use of social media is growing by leaps and bounds. You can't go a day without hearing about social media, whether it's on the television or in a magazine or you are actively using social media. Health-related social media is no different, and for many providers, the potential value of getting their information online is enormous. Before bravely exploring the social media frontier, what do you need to know? After all, it's a jungle out there!

Employment Issues
Social media challenges both employers and employees. Even if an employer prohibits social media, either in part or whole, at work, employees still frequently post comments, stories, and images that pertain to work or their employer in their off-hours. An inappropriate post can create problems (legal or otherwise) for both employers and affected employees. Inappropriate posts (or pictures) may be publicly searchable, leading to embarrassing incidents. Given the risks, as well as the potential benefit of positive stories shared about a company, employers should develop policies on social media use, appoint appropriate "watchdogs," and monitor compliance with the policy.

Privacy
Health care providers know all about privacy and security in light of HIPAA and HITECH. With social media, new threats arise, including claims for invasion of privacy based on posted stories and images. Common sense cannot be left at the door with social media! Think before you post. What may be amusing to a small number of "friends" may not be acceptable to the general public. Educate (and guide) social media users as part of your social media policy. A useful suggestion is to ask employees, "Would you want your posted information to appear on the front page of the *New York Times?*" If not, then don't post it, chances are the information is inappropriate (at least to someone).

Patients and Family Members
Recommendations from patients and their families are critical to the success of a provider. Happy patients mean happy family members. In the context of social media, positive posts and images may make all the difference in selection of a health care provider. Social media can highlight the compassion and positive interventions of hospice in a family's life (or the absence of these things). Hospice providers may consider using a "fan" page, a blog, or other social media group to gather positive stories. Statistics show that a third of Internet users are over age 45, and the fastest growing group of social media users is age 54 or older.

Regulatory Issues
All health care providers are heavily regulated in how they conduct their business, advertise for their services, and provide care. Federal and state agencies, such as the Federal Trade Commission and state attorneys general, analyze statements made in marketing and communications about provider services to protect the public. Other agencies—like the Centers for Medicare & Medicaid Services and the Office of Inspector General—review payment arrangements for services under fraud and abuse laws and regulations. Payment terms, incentives, and advertisements for services can appear in social media. Such information must be reviewed prior to posting for regulatory compliance.

You need to discuss social media so that you can set clear policies, expectations, and boundaries with your staff and patients. To further this discussion, work with legal counsel (and other appropriate consultants) to maximize the benefits of social media while minimizing any potential liabilities. Don't be scared of social media. Look for opportunities to enhance your business with positive social media use.

Kim Licata has advised health care providers and facilities on regulatory and compliance issues for over 13 years. She may be reached at klicata@poynerspruill.com or 919.783.2949.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

OIG Includes Hospices in Its 2010 Work Plan

By Mike Hale

In late October 2009, the Office of Inspector General (OIG) released its Work Plan for the 2010 fiscal year. Not surprisingly, hospice continues to be an area of focus for the OIG in 2010. The OIG publishes its Work Plan annually and sets forth various projects that the six departments within the OIG will address through audits, evaluations or other compliance activities during the fiscal year. The Work Plan is one method through which the OIG achieves its operational mission "to protect program integrity and the well-being of program beneficiaries by detecting and preventing waste, fraud, and abuse; identifying opportunities to improve economy, efficiency, and effectiveness; and holding accountable those who do not meet program requirements or who violate Federal laws." *FY 2010 Work Plan, pg. i.*

The specific hospice-related compliance activities that are included in this year's Work Plan are as follows.

Physician Billing for Medicare Hospice Beneficiaries
The OIG will review the extent of Medicare Part B physician billing for services provided to Medicare hospice beneficiaries. This study is a follow-up to other recent OIG hospice studies and will determine the "frequency of and total expenditures for physician services under Part A and Part B for hospice beneficiaries," as well as identify whether physicians double-billed Part A and Part B for physician services provided to hospice patients. This is considered to be "work in progress," meaning that the results of the study will likely be published in a report to be issued this year.

Trends in Medicare Hospice Utilization
The OIG will evaluate Medicare Part A hospice claims to identify certain trends in utilization. This study may include an evaluation of the number, types and lengths of stay of diagnoses associated with hospice admissions, as well as geographic variations in hospice utilization and differences between for-profit and not-for-profit hospice providers. This study is considered a "new start," meaning that a report will likely be issued in 2011.

Duplicate Drug Claims for Hospice Beneficiaries
In this study, the OIG will evaluate whether payments made under Part D, Medicare's prescription drug program, are correct and not duplicated for hospice beneficiaries under Medicare Part A. Part D drug plans should not pay for drugs that are covered under Part A or Part B. The OIG will also determine the extent of Part D duplication, if any, and identify measures to prevent such duplicate payments. The utilization study is also considered a work in progress.

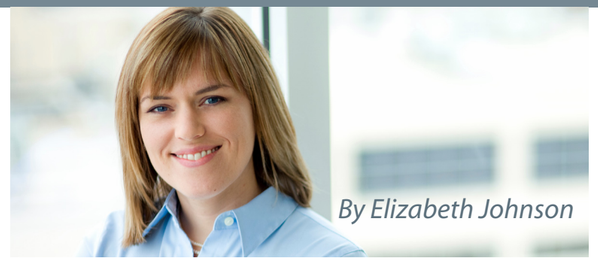
As noted in the Medicare Payment and Advisory Commission's (MedPAC) 2010 *Report to the Congress* (2010 Report) published in March 2010, Medicare spending for hospice services has "nearly quadrupled between 2000 and 2008, reflecting more beneficiaries enrolled in hospice and longer lengths of stay." In addition, approximately 40% of Medicare decedents used hospice in 2008, compared to 23% in 2000. The substantial growth in hospice Medicare expenditures, claims and the number of hospice providers over the past several years has undoubtedly increased the likelihood of duplicate Medicare payments as well as other billing errors, resulting in improper Medicare payments. As a result, the OIG will most likely continue to include hospices in its work plans in the future. In fact, MedPAC recommended in the 2010 Report (as it also recommended in its 2009 *Report to the Congress*) that the secretary of the Department of Health and Human Services should direct the OIG to investigate:

continued on Page 3

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM
301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Audits and Breaches and Fines, Oh My! — Part I

It's time to make sure your HIPAA privacy and security compliance program has a heart



By Elizabeth Johnson

Have you ever had that nagging feeling that you needed to take care of something, but you just didn't have time so you let it go, probably for too long? I usually feel that way about two things: exercise and yard work. Some HIPAA-covered entities feel that way about compliance with the HIPAA Privacy and Security Rules. They are cumbersome, dense, and difficult to fully implement. And even if you have implemented policies and procedures to address each requirement, your compliance program can't be a tin man. To effectively reduce risk of compliance problems and security incidents, you need to make sure the program actually functions, has been meaningfully implemented, and is refreshed periodically to address any compliance gaps created by changes in the law and your own operations. Breathing life into your compliance program takes real work, but doing so will have tangible rewards as the program becomes a living part of your organization's daily functions.

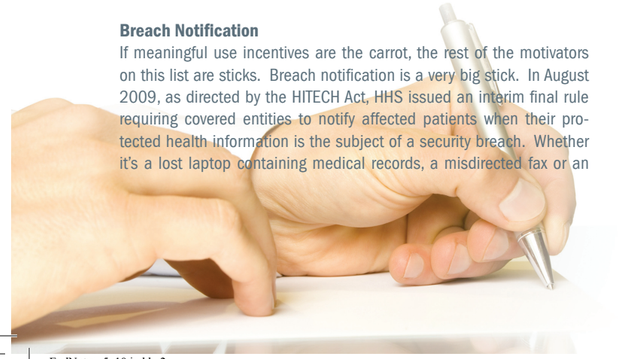
If you don't feel confident about your organization's HIPAA privacy and security compliance, now is a good time to undertake a refresher. Here are a few reasons why.

"Meaningful Use" Incentives

Let's start by discussing the carrot in this bunch. As part of the 2009 economic stimulus package, CMS was directed to provide incentive payments to eligible professionals and hospitals that make "meaningful use" of electronic health record technology and participate in Medicare and Medicaid. As part of their proposed rule to implement this requirement, CMS identified a series of "health outcome policy priorities" to be met, including "ensur[ing] adequate privacy and security protections for personal health information." As a Stage 1 measure, eligible professionals and hospitals must "[c]onduct or review a security risk analysis…and implement security updates as necessary." If you comply with the HIPAA Security Rule, you will have met this Stage 1 requirement.

Breach Notification

If meaningful use incentives are the carrot, the rest of the motivators on this list are sticks. Breach notification is a very big stick. In August 2009, as directed by the HITECH Act, HHS issued an interim final rule requiring covered entities to notify affected patients when their protected health information is the subject of a security breach. Whether it's a lost laptop containing medical records, a misdirected fax or an intrusion by a hacker (or an unauthorized employee), these incidents may require that your organization send a letter to each person whose protected health information was affected, noting what happened, when it happened, and what you are doing to address it. You also have to notify HHS, and possibly the media. Existing notification laws at the state level have shown that sending these letters often prompts a government investigation of the organization's privacy and security compliance, and sometimes spawns lawsuits by affected individuals. Ensuring compliance prior to one of these events can mitigate their impact, in part by minimizing the risk of a government enforcement action and as a defense to a potential lawsuit.



Government Enforcement

For several years now the Federal Trade Commission and state regulators have been taking enforcement actions against organizations that report security breaches. The pattern goes as follows:

1. Organization experiences a security incident affecting personal information
2. Organization sends a letter to affected individuals, as required by state law, describing what went wrong
3. Government regulator receives a similar notice (often required under state law) or reads about the incident in the press
4. Notice letter prompts regulator to investigate whether organization's security was adequate in light of the incident
5. Regulator alleges that incident demonstrates inadequate security, and charges organization with an unfair trade practice pursuant to the federal or state unfair and deceptive trade practices statute it enforces

In February 2009, HHS joined the party, taking a joint enforcement action with the FTC against CVS Pharmacy following multiple reports that employees disposed of prescription information in dumpsters. The result was a settlement with both agencies, including a $2.25 million payment by CVS and an agreement to implement a comprehensive, written information security program with oversight from HHS, as well as submitting to audits of compliance with that plan biennially for 20 years. This action predated the HITECH Act and HHS's breach notification rule, which now require covered entities to self-report the type of security incident that led to the action against CVS.

Increased Penalties

The HITECH Act was just full of motivators to compel HIPAA privacy and security compliance. The same statute that brought you breach notification and additional privacy and security obligations also increased the penalty amounts HHS can seek for noncompliance. Whereas penalties were previously capped at $25,000 for multiple violations of the same provision in a single calendar year, they are now capped at $1.5 million.

Mandatory Audits and State Enforcement

In case breach notification and increased penalty amounts were insufficient incentive to comply, the HITECH Act also made periodic HIPAA audits by HHS mandatory and authorized state attorneys general to enforce HIPAA. Wasting no time (and having announced days earlier his intention to seek the Senate seat soon to be vacated by Chris Dodd), Connecticut Attorney General Richard Blumenthal in January became the first state AG to exercise his newfound HIPAA enforcement authority. Blumenthal filed suit against Health Net, which allegedly lost a portable disk drive containing unencrypted protected health information, social security numbers and bank account numbers of approximately 1.5 million past and present enrollees, including 446,000 Connecticut residents. The suit alleges that Health Net failed to notify affected individuals for approximately six months following discovery of the incident. Mr. Blumenthal already is engaged in a second HIPAA-related action, investigating an alleged breach of medical records at Griffin Hospital in Derby, Connecticut, where a radiologist allegedly accessed patient information and used it to promote his services offered at another medical facility.

Threats to Medicaid and Medicare Reimbursement

In case you were thinking that the worst-case scenario in a breach situation is allegations of HIPAA violations and a potential fine, let's consider the case of Wentworth-Douglass Hospital in Dover, New Hampshire. That facility has been the subject of an investigation by the New Hampshire attorney general following an alleged breach of patient medical records. What's different about this investigation is that CMS joined the investigation, sending surveyors from the New Hampshire Department of Health and Human Services to examine not only privacy and security issues, but also patients' rights and quality assurance in order to determine whether the facility meets the "conditions of participation" for reimbursement by Medicaid and Medicare.

With all these compelling reasons to revisit your HIPAA privacy and security compliance, you may be wondering where to start. In next month's issue of [Shorts/Endnotes], we'll provide a road map to reevaluating HIPAA compliance. In the meantime, our attorneys frequently assist covered entities of all shapes and sizes in implementing HIPAA privacy and security compliance programs. If you have any questions about this article or need assistance with HIPAA or the new HITECH requirements, please contact us today.

Elizabeth Johnson's practice focuses on privacy, information security and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

OIG Includes Hospices...

continued from Page 1

- The prevalence of financial relationships between hospices and long-term care facilities
- Differences in patterns of nursing home referrals to hospice
- The appropriateness of enrollment practices for hospice with unusual utilization practices, such as a high frequency of very long stays
- The appropriateness of hospice marketing and admission practices

You should pay close attention to your billing practices and ensure that duplicate claims for hospice services, as well as claims containing other types of billing errors, are not being submitted. This will involve educating your vendors and other business associates of the services and supplies that are included in the Medicare hospice benefit and not separately billed. In addition, evaluating your length of stay, admission and marketing practices now may help prevent problems in the future as the OIG continues its focus on hospice.

Mike Hale advises clients on a variety of regulatory, contractual and operational issues in hospice, home care and long term care settings. Mike may be reached at 919.783.2968 or mhale@poynerspruill.com.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW