The Refinement of Adverse and Never Events—Time for a Plan

With the release of the National Coverage Determination (NCD) on January 15, 2009 by the Centers for Medicare and Medicaid Services (CMS), the Medicare program has taken a new approach to forcing acute care providers to reckon with some of the most vexing medical management and quality issues in clinical care. This time, however, the focus is not just on hospitals but all providers who have been involved in the patient’s care, whether or not they were implicated in the cause of the unexpected outcome. More importantly, the new rules are effective immediately without much prior notice.

Background

In August 2007 and August 2008, CMS promulgated rules relating to non-payment for the treatment of adverse conditions that patients contract in hospitals. The first eight conditions and the following three respectively, were a result of months of deliberations put into motion by Congress through the passage of the Deficit Reduction Act of 2005 (DRA). Congress instructed the Department of Health and Human Services to determine a minimum of two adverse or acquired conditions in hospitals that (1) were high-volume claims or represented a major cost to the Medicare program, (2) result in a higher payment when present as a secondary diagnosis, and (3) were reasonably preventable based upon evidence-based guidelines.

This initiative followed closely the requirement to establish a primary diagnosis for all Medicare patients, or what is called “present on admission” (POA). As a result, to attempt to delineate whether a secondary infection or diagnosis exists at the time of admission, hospitals check patients for the existence of infections, bed sores and other complications, to document the patient’s medical condition before treatment or surgery in the hospital. Unlike in the past, the “adverse conditions,” those arising during the care of the patient for his or her primary diagnosis that are included in the CMS rules effective October 2008, were not to be paid by the Medicare program. In publishing its findings and announcing the original eight hospital-acquired conditions (HACs) and following three HACs, CMS set forth the number of cases that had been experienced by Medicare patients and the billions of dollars that the program hoped to save. CMS also expressed its interest in protecting Medicare beneficiaries from complications during their respective hospital stays.

The Release of the NCDs

The NCDs announced as final rules just days before President Obama took office focus on what all agree should never happen (a.k.a. “never events”):

- surgery on the wrong patient
- surgery on the wrong body part
- the wrong surgery performed on a patient.
While cost savings to the program were certainly a motivation, more importantly, the NCDs tied the payment system to quality of care in a way that surprised many observers and commentators. CMS dismissed any criticism of its initiative to protect the lives of Medicare patients in this way. By issuing these new rules as NCDs rather than regulations, CMS was able to shorten the comment periods and rulemaking processes. NCDs tend to be administrative in nature, and while comments are requested and received, the timeline is shorter and NCDs are implemented immediately. The American Hospital Association and the American Medical Association commented adversely on the NCDs. Their respective comments questioned the details of how the new rules would work and protested the affect on providers other than the hospitals where the “never events” occurred.

In fact, the NCDs issued on January 15, 2009 apply to all providers that might attempt to bill the Medicare program for the patient’s care, whether or not that particular provider had participated in the decisions made during the surgery. Such providers include, for example, anesthesiologists, radiologists, and other service providers who may not have been implicated in the events leading up to the tragic mistake. While CMS, in announcing the NCDs, indicated that precise billing rules will be issued at a later date, it is possible that those present at the original surgery, or even at a second surgery to reverse the error made initially, were in jeopardy of not receiving payment.

Medicaid Impact

While the NCDs were issued in connection with the Medicare program, CMS also has been working with various state Medicaid directors on amendments to state plans that would incorporate the new rules for adverse events under the DRA and the recently issued NCDs. CMS at first expressed concern over dual eligible patients. It alerted the Medicaid directors that if payment requests were rejected under the Medicare program, the requests might be submitted to the state Medicaid program for payment. CMS took this further by also suggesting to the various states that they limit payments for patients under the particular state’s Medicaid program. In either event, CMS was attempting to restrict federal payments for these adverse conditions and never events.

Using Payment as a Quality Care Initiative

CMS’ recent actions, assuming the new administration does not attempt to reverse the NCDs, gives a clear signal for other payors to use the Medicare NCDs and adverse conditions as a benchmark. This may create a national quality-of-care initiative that, if not responded to by providers, could prove disastrous for financial projections of patient revenue, undermine the credit ratings of hospitals and establish a national standard of care that traditionally has been left to the local or state courts.

Time to Take Action

In response to this challenge to the financial well-being of hospitals and other health care entities, providers should take these immediate preparatory actions:

- boards of directors; risk management professionals; senior management; medical, public relations and financial staff; and legal counsel all must consider implications beyond simply the loss of payment from Medicare and other payors
- be aware that payors will be pushing to adopt adverse or never event standards into contracts, and should be sure to review and negotiate
- determine who decides when a preventable error has occurred. How quickly? What is the impact on claims deadlines?
- be sure POA conditions are properly documented
- consider that not billing patients may be an excellent defense strategy
- consider new forms of electronic surveillance for infections, such as Cardinal’s MedMined, which was recently given HFMA Peer Review status.

The challenge of these new payment restrictions could cause severe financial strains on providers already weakened by the economy and increased uncompensated care costs. Providers should comply with the new rules and reduce the impact of continued levels of adverse events.

Author:

Henry C. Fader
215.981.4640
faderh@pepperlaw.com
Network Advertising Initiative Adopts New Internet Advertising Protocol

The Network Advertising Initiative (NAI) recently released a new version of its self-regulatory code of conduct. The 2008 NAI Principles reflect the work of a year-long initiative to update the NAI Principles last issued in 2001. NAI is a self-regulatory organization for companies in the online advertising marketplace and includes as members networks such as Google and Yahoo! Inc. According to the NAI website:

“The NAI (Network Advertising Initiative) is a cooperative of online marketing and analytics companies committed to building consumer awareness and establishing responsible business and data management practices and standards. As increasingly sophisticated online advertising technologies evolve, consumer concerns about their impact on online privacy mount. The NAI is prepared to meet these concerns with both effective industry self-regulation and sensible protections for online consumers.”

For nearly 10 years, NAI and its members have been involved in developing standards for third-party advertising networks and in providing consumers with explanations about data collection, usage and choice. In 2001, NAI developed the first set of NAI Principles to guide business practices with respect to online advertising services. The 2008 NAI Principles, effective January 1, 2009, evolved out of a recognition that much has changed in online advertising in the past decade.

As described by NAI, many banner ads displayed on Web pages are not selected and delivered by the Web site visited by a consumer, but by network advertising companies that manage and provide advertising for numerous unrelated Web sites. The NAI refers to these companies as “third-party ad networks.” These networks use a variety of techniques such as cookies, Web beacons and other means to track consumers’ online usage and patterns. The networks then customize the advertising content shown to that user when visiting other Web sites.

Notice and Choice

The 2008 NAI Principles require member companies to provide “clear and conspicuous” notice on their Web sites describing data collection, transfer and use practices. The notice is to include:

- the types of advertising activities conducted by the company
- a description of the type of data being collected and how it is used (including whether the data is transferred to a third party)
- disclosure about how long the collected data is stored
- the types of personally identifiable information (PII) and non-personally identifiable information (non-PII) being collected
- notification if PII and non-PII is being merged and how such merged data will be used
- the procedure for either opting-out or opting-in with respect to the type(s) of data.

NAI members must require a Web site that they contract with for advertising purposes to post notice as well (elements of which are included in the 2008 NAI Principles). In particular, this notice must include a “conspicuous link” to the opt-out or opt-in mechanism on the NAI member’s Web page. NAI members must make reasonable efforts to enforce their agreements with subcontracted Web sites.
For purposes of the 2008 NAI Principles, PII is defined to include:

- name
- address
- telephone number
- e-mail address
- financial account numbers
- government-issued identifier, and
- any other data used or intended to be used to identify, contact or precisely locate a person.

The Principles also include another category of information—“sensitive consumer information.” While this definition is to be further developed in an implementation guideline, the Principles include the following types of information in the definition:

- Social Security numbers or other government-issued identifiers
- insurance plan numbers
- financial account numbers
- information that describes the precise real-time geographic location of an individual derived through location-based services such as through GPS-enabled devices
- precise information about past, present or potentially future health or medical conditions or treatments, including genetic, genomic and family medical history.

In the NAI Response to Public Comments on the draft principles (available on the NAI Web site), NAI included a footnote emphasizing the use of the term “precise” in the definition. The Principles do not require an opt-in standard for all health-related advertising or use of data from health-related Web sites. As NAI works to develop the implementation guideline, what information falls within the definition will be clarified based on industry standards and applicable law.

NAI members are required to provide choice to consumers regarding use of their information that is collected through advertising activities. The level of choice depends on the type of data and the way in which it is to be used. In brief, the various choice options (as detailed in the Principles and the Roadmap developed by NAI) are:

- use of non-PII requires a consumer opt-out mechanism, which must be available on the NAI member’s Web site and on the NAI consumer Web site
- use of PII to be merged with non-PII on a going-forward basis (called prospective merger) requires a consumer opt-out mechanism accompanied by robust notice (defined in the Principles to include additional information regarding merger and use of the merger data) of such choice. The opt-out mechanism must be available where the robust notice is provided.
- use of PII to be merged with previously collected non-PII (retrospective merger) requires a consumer opt-in mechanism at the time such PII is collected online or, if collected offline, first used online
- use of sensitive consumer information requires a consumer’s opt-in consent.

Additional Requirements

The Principles include a number of limitations on members’ use and gathering of consumer information collected through advertising. The information collected is only to be used for “marketing purposes” as defined in the Principles. NAI members are not to collect PII from companies unless they have a contract with that company, and members must comply with their own posted privacy policies. The Principles require NAI members to contractually require third parties to comply with applicable provisions in the Principles when the NAI member (1) provides the PII, or (2) provides non-aggregated non-PII to be merged with PII held by the third party.

NAI members are required to provide consumers with reasonable access to PII, and to other information associated with their PII, that is retained by the member for advertising purposes. Furthermore, members are to make reasonable efforts to ensure that they are collecting data from reliable sources. The Principles include brief provisions regarding data retention and data security, and impose a reasonable standard together with requiring compliance with applicable laws. In those instances where the Principles apply a higher standard, members are to follow the Principles so long as such activity is not contrary to applicable law.

Although the Principles are self-regulatory, membership in NAI requires compliance with the Principles. NAI will conduct compliance reviews of member applicants, at least once annually and in response to certain consumer complaints.
The 2008 NAI Principles demonstrate an industry's efforts to self-regulate in an area receiving continued attention from federal and state legislators and regulators. The 2008 NAI Principles, the NAI Roadmap and additional information is available on the NAI Web site at www.networkadvertising.org.

CVS HIPAA Settlement May Forecast Additional Enforcement

In a development of interest to every health care provider handling patient information in hard-copy form, on February 18, 2009 the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) announced that CVS, the largest retail pharmacy chain in the country, will pay the government $2.25 million, and take corrective action, to settle allegations that CVS violated the Health Insurance Portability and Accountability Act (HIPAA) privacy rule and the FTC Act. In particular, CVS was accused of violating the privacy of its millions of prescription customers when it disposed of the customers’ information, such as identifying information found on pill bottle labels.

According to HHS and the FTC, employees at some CVS pharmacies left labels and other items containing patient information in open trash bins outside stores, as recently as 2006. The company also did not have adequate, or adequately enforced, policies and procedures for disposing of such information, nor did the company sufficiently train employees to properly handle such material. The Associated Press reported that items not properly discarded included pill bottles, medication instruction sheets, computer order forms, payroll information, job applications and credit card and insurance information. Those documents contained personal information including Social Security numbers and credit card and insurance information, and in some cases driver’s license numbers and account numbers.

The HIPAA Privacy Rule requires most health care providers (including pharmacies), health plans, and health care clearinghouses to safeguard the privacy of patient health information—including during its disposal. HIPAA also includes general requirements that covered entities adopt adequate policies and procedures, and provide adequate training to employees, to protect the patient information under their care. In this case, the patient information found in open trash bins at multiple sites demonstrated that CVS had inadequate procedures or inadequate employee training, or both.

The settlement resulted from a joint investigation by HHS and the FTC and may mark a shift in the enforcement of the federal HIPAA statute. While health care entities have faced enforcement over their improper disposal of patient information in the past, such enforcement has largely been under state law and regulation. Now, HHS has shown willingness to use the HIPAA statute to enforce federal privacy standards relevant to the disposal of patient information. In addition, the FTC alleged that the breaches of the HIPAA rules constituted a deceptive business practice under the FTC Act because CVS had claimed to customers that “CVS … wants you to know that nothing is more central to our operations than maintaining the privacy of your health information.” This settlement demonstrates that the improper disposal of patient health information may create liability under both HIPAA and the FTC Act.

This settlement demonstrates that the improper disposal of patient health information may create liability under both HIPAA and the FTC Act.
On February 22, 2009 HHS posted new guidance on its Web site regarding the disposal of patient information. The guidance should be reviewed by covered entities that routinely dispose of patient information in any form. As part of that guidance HHS states:

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information ("PHI") ... Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, covered entities must ensure that their workforce members received training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member ... Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal.

The guidance goes on to state that because the HIPAA rules do not require a particular disposal method, covered entities must review their own policies and procedures to make sure they are taking reasonable steps to dispose of PHI. In the new guidance, HHS identifies the following disposal methods as being generally acceptable:

- for PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed
- maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI
- for PHI on electronic media, clearing (using software of hardware products to overwrite media with non-sensitive data), purging (degauzing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media, and
- whatever the disposal method, a covered entity must ensure that appropriate workforce members receive training on and follow the disposal policies and procedures of the covered entity.

Because the CVS settlement shows that HHS and the FTC are willing to bring joint investigations regarding the improper disposal of PHI, covered businesses that handle patient information now need to be concerned with costly potential violations of both HIPAA and the FTC Act. Accordingly, the time is ripe for health care providers to take stock of their policies and procedures, as well as their training and compliance programs relative to the disposal of patient information.

Author:
Kevin J. Dill
215.981.4289
dillk@pepperlaw.com