Health Care Enforcement Defense Advisory

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

MARCH 23, 2011

Two HHS Announcements Boost State Health Care Enforcement Authorities

BY ELLYN L. STERNFIELD AND STEPHANIE D. WILLIS

Health care providers will soon be subject to even more scrutiny from State Attorneys General and State Medicaid Fraud Control Units (MFCUs), as demonstrated by two recent announcements made by the Department of Health and Human Services (HHS). First, the HHS Office of Civil Rights (OCR) announced the dates of its Health Insurance Portability and Accountability Act (HIPAA) enforcement training[1] for State Attorneys General and their staff, which is intended to bolster enforcement under the HIPAA Privacy and Security Rules.[2] Second, the HHS Office of Inspector General (OIG) released a proposed rule[3] that, if promulgated, would allow MFCUs to mine Medicaid claims data to identify aberrant billing schemes for investigation and potential prosecution. These new resources will provide additional support for state enforcement of laws related to health care data privacy and security and health care fraud and abuse. Moreover, these announcements signal the need for health care providers to stay abreast of, and comply with, laws and regulations governing the state and federal health care programs.

HIPAA Enforcement Training

Last week's announcement of HIPAA enforcement training for State Attorneys General and their staff likely signifies OCR's desire to encourage the states to enforce the HIPAA Privacy and Security Rules. The Health Information Technology for Economic and Clinical Health (HITECH) Act,[4] which was enacted as part of the American Recovery and Reinvestment Act of 2009, contains several provisions that strengthen civil and criminal enforcement of the HIPAA Privacy and Security Rules.[5] In addition to granting State Attorneys General the authority to seek injunctions and file civil suits for damages related to violations at the state level, the HITECH Act also extended application of the HIPAA Privacy and Security Rules to business associates of covered entities and created a tiered monetary penalty scheme to address particular violations (hereinafter, "the HITECH Act's Enforcement Provisions").

To date, the federal government has initiated the majority of enforcement activity related to the HIPAA Privacy and Security Rules. Most recently, in February 2011, OCR imposed a $4.3 million civil monetary penalty on Cignet Health of Maryland[6] and entered into a $1 million Resolution Agreement with The General Hospital Corporation and Massachusetts General Physicians Organization, Inc.[7] These actions are the first-ever civil monetary penalty and settlement, respectively, stemming from the HITECH Act's Enforcement Provisions.

Consequently, based on the information to be shared through OCR's HIPAA enforcement training, more State Attorneys General likely will use the HITECH Act Enforcement Provisions to file suits for

damages on behalf of state residents and to enjoin further violations of the HIPAA Privacy and Security Rules within their states. In fact, the Connecticut Attorney General successfully relied on the HITECH Act's Enforcement Provisions to prosecute and ultimately settle such a case with Health Net, which paid a $375,000 penalty, in July 2010.[8] Given that state privacy laws are often more stringent than the HIPAA Privacy and Security Rules, OCR's HIPAA enforcement training may create more opportunities for states to pursue parallel state and federal proceedings and to increase recoveries related to state privacy laws and the HIPAA Privacy and Security Rules.

Inevitably, the increasing use of health information technology will create more risks for health care providers. In turn, health care providers who are covered entities should prepare for these risks by periodically reviewing their privacy and security policies and procedures as applied to themselves and to their business associates, and then modifying them accordingly to reduce exposure to investigations and penalties at both the state and federal level.

Federal Funding for MFCU Data Mining Activities

MFCUs may also soon enjoy increased federal support for investigations of health care providers because the OIG has proposed regulatory changes that would effectively allow MFCUs to use federal matching funds to conduct data mining activities.[9] The proposed rule appears to take its cue from a Medicaid waiver request approved by HHS in July 2010 for a similar demonstration project in Florida.[10] The Florida demonstration project focuses on using utilization and billing patterns in Medicaid claims data to determine where the MFCU should focus its fraud investigation and prosecution efforts. The proposed rule also complements the announcement by HHS and the U.S. Department of Justice of their joint efforts to obtain proactive data mining tools to better detect fraud.[11]

According to the proposed rule, data mining is "the practice of electronically sorting Medicaid claims through statistical models and intelligent technologies" to identify fraud. Data mining activities may include, for example, screening of Medicaid claims or routinely verifying whether recipients actually received services billed by Medicaid providers. Additionally, the proposed rule would require MFCUs to annually report data mining costs as well as cases and monetary recoveries generated from Medicaid data mining activities to HHS.

The preamble to the proposed rule explains the history underlying the current rule. Of note, it acknowledges that MFCUs presently are limited to relying on referrals from state Medicaid agency data mining activities to ascertain patterns of aberrant utilization and billing practices that may rise to the level of fraud. According to evaluations conducted by the OIG, the number of referrals from state Medicaid agencies to MFCUs varies with the level of cooperation between the two entities.[12] The OIG believes that allowing the MFCUs to claim federal funding for Medicaid data mining activities will supplement, support, and ultimately improve fraud detection efforts and collaboration at the state level. Consequently, the OIG anticipates that the new rule will result in an increase in the number of enforcement actions taken by, and recoveries for, state and federal health care programs.

As the government amasses more fraud detection tools, health care providers should establish and consistently employ their own medical record review and billing verification procedures to ensure the integrity of the data and claims that they submit to state and federal health care programs.

The public may provide comments on the proposed rule no later than 5:00 p.m. on May 16, 2011.

* * *

Click here to view Mintz Levin's Health Law attorneys.

Click here to view Mintz Levin's Health Care Enforcement Defense attorneys.

Click here to view Mintz Levin's Fraud and Abuse attorneys.

Endnotes

1 HIPAA Enforcement Training for State Attorneys General, available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html.

2 See, 45 C.F.R. Part 160 and 164, Subparts A, C, and E.

3 76 Fed. Reg. 14637 (Mar. 17, 2011).

4 Pub. L. No. 111-5 (Feb. 17, 2009).

5 See our related Employment, Labor & Benefits and Health Law Advisory from July 13, 2010 at http://www.mintz.com/publications/2252/.

6 Press Release, U.S. Department of Health and Human Services, *HHS imposes a $4.3 million civil money penalty for violations of the HIPAA Privacy Rule*, (Feb. 22, 2011), available at http://www.hhs.gov/news/press/2011pres/02/20110222a.html.

7 Press Release, U.S. Department of Health and Human Services, *Massachusetts General Hospital settles potential HIPAA violations*, (Feb. 24, 2011), available at http://www.hhs.gov/news/press/2011pres/02/20110224b.html.

8 Press Release, Connecticut Attorney General's Office, *Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info* (Jul. 6, 2010), available at http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

9 42 C.F.R. § 1007.19(e)(2) (2010).

10 Press Release, U.S Department of Health and Human Services, *HHS Announces New Tool to Help Fight Health Care Fraud in Florida*, (July 15, 2010), available at http://www.hhs.gov/news/press/2010pres/07/20100715a.html.

11 See our related Health Law Advisory from December 17, 2010 at http://www.mintz.com/publications/2439/. Also consult our related Health Law Alert from February 25, 2011 for information about other new program integrity regulations intended to support state and federal efforts to prevent fraud, available at http://www.mintz.com/publications/2552/.

12 OEI-07-04-00180, Factors Impacting Referral of Suspected Medicaid Fraud Cases: State Medicaid Agency and Medicaid Fraud Control Unit Experiences.

0995-0311-NAT-HCED