The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 4 April 2011

Making Sense Of Recent HIPAA Enforcement Activity

Jo-Ellyn Sakowitz Klein and Kristen L. Henderson

AKIN GUMP STRAUSS HAUER & FELD LLP

In the first few months of 2011, the U.S. Department of Health and Human Services Office for Civil Rights issued its first-ever civil monetary penalty, against Cignet Health, for alleged privacy violations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), exacted a $1 million resolution amount from Massachusetts General Hospital for alleged HIPAA privacy violations, issued a budget request seeking substantial funding for HIPAA compliance and enforcement activities, and announced a new program to train state attorneys general to enforce HIPAA.

Many HIPAA-covered health care providers, health plans and health care clearinghouses are struggling to put these developments into perspective. The sheer size of the Cignet penalty – over $4.3 million – and the fact that the Office for Civil Rights (OCR) exercised its authority to assess civil monetary penalties (CMPs) for the first time led stakeholders to wonder if this development marked a sea change in enforcement attitudes. But concerns were tempered somewhat by the facts of the case, as the provider's abject noncompliance and refusal to cooperate with authorities made it seem like an outlier. The Massachusetts General Hospital (MGH) million-dollar resolution set the HIPAA community more on edge, as the breach – an employee accidentally left files containing medical records on a subway train while commuting – seemed like the type of incident that could occur despite an entity's sincere compliance efforts.

The OCR budget request and announcement of the new state attorney general training program added to an already tense environment. OCR is requesting about $46.7 million for fiscal year 2012, compared to its $44.3 million request for fiscal year 2011 and the $41.1 million enacted amount for fiscal year 2010. OCR is also reaching out to state attorneys general, offering substantial support in their efforts to enforce HIPAA using new authority granted under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. OCR announced a series of intense two-day state attorney general training workshops, starting in April 2011, that will include instruction on issues ranging from HIPAA, HITECH and state legal requirements to investigative techniques for identifying and prosecuting potential violations to resources available to state attorneys general pursuing alleged HIPAA violations. Notably, HITECH allows courts to award damages (capped at $25,000 per calendar year for violations of the same requirement), as well as costs and attorney's fees, in such actions.

This article considers recent enforcement activity against the backdrop of the broader HIPAA enforcement timeline. When placed in context in this manner, the Cignet and MGH settlements seem to be more a continuation of a trend that has been slowly building over time than a shocking new development calling for drastic measures. Given the current environment, prudent covered entities should reinvigorate their HIPAA compliance efforts. This article continues to extract several lessons for covered entities from the enforcement timeline.

Putting Recent HIPAA Enforcement Actions Into Perspective

In the early days of HIPAA, outreach and education were the buzzwords of choice, as covered entities became acquainted with the new requirements. The promulgation of the interim final HIPAA privacy rule in December of 2000 marked the beginning of a period that would extend until compliance with the HIPAA security rule was mandated in 2005, during which covered entities focused on learning the regime and building compliance programs. Revisions to the regulations and the issuance of guidance documents made headlines. There were no seven-figure settlements, no resolution agreements with corrective action plans (CAPs) and no CMPs.

Providence: A Beginning

Then, in July 2008, the U.S. Department of Health and Human Services (HHS) announced the first HIPAA resolution agreement, in which Providence Health System and a pair of related entities (Providence) agreed to a detailed CAP and a $100,000 resolution amount for alleged privacy and security violations. The incident giving rise to the resolution agreement involved the loss of backup tapes, optical disks and laptops laden with unencrypted protected health information (PHI) on 386,000 individuals, which were removed from the entity's premises and left unattended in a car. Affected individuals were notified as required under state laws, and HHS received over 30 complaints. The CAP required Providence to revise its HIPAA policies and procedures, train workforce members accordingly, conduct monitoring and submit compliance reports to HHS for three years. This litany will become rather common. In its press release announcing the resolution agreement, HHS emphasized that Providence's cooperation with regulators allowed HHS to resolve the case without imposing a CMP. These words will take on an almost eerie significance, post-Cignet.

Rite Aid and CVS: Underscoring the Significance of Major Regulatory and Legislative Developments

Fast forward to February 2009, and the passage of the HITECH Act brings major changes to the HIPAA regime. Beyond enhancements to privacy requirements and the extension of HIPAA to business associates, HITECH dramatically increased penal-

***Jo-Ellyn Sakowitz Klein** is Senior Counsel in the health industry practice group and leads the privacy and data protection group at Akin Gump. **Kristen Henderson** is an Associate in the health industry practice group at Akin Gump.*

Please email the author at jsklein@akingump.com with questions about this article.

ties (raising maximums from $25,000 to $1.5 million), created an elaborate tiered penalty structure, added a new mandatory federal breach notification requirement and created new enforcement tools – including HIPAA enforcement authority for state attorneys general.

Almost in the same breath, on February 18, 2009, HHS announced that OCR had concluded a joint investigation with the Federal Trade Commission (FTC) into alleged HIPAA privacy violations by CVS pharmacies, and that the chain had agreed to pay a $2.25 million resolution amount and to take corrective action. The investigation began following media reports that CVS was disposing of pill bottles and other items containing PHI in open dumpsters. OCR's three-year CAP called for new policies and procedures relating to disposal of PHI (including workforce training and sanctions for noncompliance), internal monitoring and third-party audits. CVS entered into a separate consent decree with the FTC.

With the proposal of HITECH regulations in the summer of 2010 came another announcement – this time describing a settlement with Rite Aid that included a $1 million payment and similar CAP terms, plus an FTC consent decree, at the conclusion of a joint OCR/FTC investigation into similar allegations.

Management Services Organization: The Wheels Churn, Quietly

Then, somewhat quietly, in December of 2010, HHS announced a resolution agreement with a covered entity arising from facts revealed during a Federal False Claims Act investigation. Coordinating with the HHS Office for Inspector General and the U.S. Department of Justice, OCR entered into a resolution agreement and CAP with Management Services Organization (MSO), a covered entity that had allegedly shared PHI with a related entity for marketing purposes without the requisite authorization from affected individuals. HHS found that MSO intentionally did not have safeguards in place to protect information from such unauthorized use or disclosure. MSO agreed to pay $35,000 and implement a two-year CAP calling for policies and procedures, workforce training, monitoring and reporting.

Cignet: Outliers Beware

On February 22, 2011, HHS imposed its first-ever CMP for HIPAA violations: a penalty exceeding $4.3 million against Cignet. OCR found that Cignet failed to provide 41 patients with access to their medical records as required under HIPAA and, quite inexplicably, obstructed OCR's investigation. On receiving complaints from affected individuals, OCR initiated an investigation and notified Cignet in writing of its obligation to provide access to the requested records. Cignet failed to comply for months, even after OCR issued a subpoena. Only after OCR filed a petition to enforce its subpoena in a U.S. district court, and the court ordered Cignet to produce the records, did Cignet act. And in doing so, Cignet ran further afoul of HIPAA, producing records – without securing authorization – for several thousand patients above and beyond the 41 at issue. Before issuing its proposed determination, OCR gave Cignet the opportunity to submit evidence of any mitigating factors or affirmative defenses. Cignet failed to respond. In its final determination, OCR noted that Cignet made no efforts to resolve the complaints and, when calculating the amount of the CMP, considered the patients' inability to obtain continuing treatment and the fact that OCR was forced to issue a subpoena as aggravating factors. Applying the HITECH tiered penalty scheme, OCR assessed a $1.3 million penalty for the individual rights violations, plus a $3 million penalty for its "willful neglect" in failing to cooperate with the investigation.

Massachusetts General: The Wheels Churn, Not So Quietly

On the heels of the Cignet announcement, on February 24, 2011, OCR announced a $1 million settlement with MGH for alleged HIPAA privacy violations. An employee commuting on the subway inadvertently left behind files containing PHI for around 200 infectious disease practice patients, including records containing sensitive HIV/AIDS information. OCR's investigation indicated MGH failed to implement reasonable and appropriate safeguards where PHI is removed from the hospital's premises. MGH agreed to a CAP requiring the hospital to develop policies and procedures (notably, addressing USB and laptop encryption as well as physical removal and transport of PHI) and train workforce members accordingly. A specially designated monitor will oversee implementation of the CAP for a three-year period and report back to HHS.

There is no sign that the timeline will not continue from here. Indeed, the enforcement wheels continue to churn. OCR officials have noted that every complaint received by OCR is reviewed and analyzed, and an investigation is initiated if the facts and circumstances alleged indicate a compliance failure. As a result of the HITECH breach notification requirements, reports of sizeable breaches have been mounting, posted on a website for all to see. OCR has indicated that the agency is following up on those incidents. Presumably, some will be resolved through a long-term resolution agreement and CAP, while others will be addressed through voluntary compliance without sanctions. In the MGH press release, OCR Director Georgina Verdugo noted, "We hope the health care industry will take a close look at this [resolution] agreement and recognize that OCR is serious about HIPAA enforcement."

Some Lessons For Covered Entities

The enforcement trail yields a number of lessons for covered entities. First, do not underestimate the importance of having reasonable and appropriate written privacy and security policies and procedures. Policies and procedures should be reevaluated at regular intervals, as well as when incidents occur. Entities should conduct common sense assessments to identify risks specific to their organizations and should be sure to incorporate low-tech (as well as high-tech) solutions. Entities should learn from incidents endured by others and should review the OCR breach notification website, case examples and statistics – as well as the CAPs – for ideas regarding potential areas of weakness.

Covered entities should take care to comply fully with their own policies and procedures. The CAPs emphasize the importance of training – and retraining – workforce members. Especially in areas deemed HIPAA risks, policies and procedures should be tested through thoughtfully considered internal monitoring and audits. Sanction policies should be clearly documented and applied as circumstances dictate. All compliance efforts should be documented. This documentation will be critical should OCR initiate an investigation. And, of course, it is important to cooperate with OCR during any investigations.

The enforcement trail also suggests that fundamental individual rights, like the right to access, may be held particularly sacred; that OCR may be losing patience for sloppy safeguards that result in lost or stolen data (especially where PHI is taken off-premises); and that the agency may come down especially hard where sensitive information (like HIV/AIDS information) is involved. The Rite Aid and CVS settlements also convey the message that OCR expects data to remain secure throughout its lifecycle, from creation through destruction. And, as both Cignet and MGH learned most recently, it is not necessary to have thousands of individuals affected by an incident for an entity to face significant consequences under HIPAA and HITECH.

In conclusion, enforcement efforts have been building and do not seem likely to subside. Only with hindsight will we know for certain whether the recent confluence of events should be taken as a sign that OCR is shifting to a far more aggressive tact on HIPAA enforcement. Covered entities should learn what they can from the enforcement trail and reinvigorate HIPAA compliance efforts.