Tatiana Melnik / Brian Balow

When HHS Calls, You Should Answer

Tatiana Melnik is an associate with the Dickinson Wright law firm. Ms. Melnik sits on the Michigan Bar Information Technology Law Council and the Automation Alley Healthcare Information Technology Committee. Ms. Melnik holds a JD from the University of Michigan Law School, a BS in Information Systems, and a BBA in International Business, both from the University of North Florida.

Brian Balow is a member of the Dickinson Wright law firm and chairs the firm's IT Law Group. Mr. Balow was the firm's Business Technology and Telecommunications practice department manager from 2003 to 2008. Mr. Balow has nearly 20 years of experience in IT law-related matters, including health care IT.

Agency Imposes Civil Money Penalty for Violations of HIPAA Privacy Rule, Relying on HITECH to Increase Penalty

The Department of Health and Human Services (HHS) apparently has taken its mandate under the Health Information Technology for Economic and Clinical Health (HITECH) Act to heart. On February 22, 2011, HHS announced a $4,351,600 civil money penalty imposed by the Office for Civil Rights (OCR) on Cignet Health of Prince George's County, Maryland, for violating the privacy rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

According to HHS, this is the *first* penalty issued "for a covered entity's violations of the HIPAA privacy rule."[1] In determining the penalty amount, OCR relied on the willful neglect provisions of the HITECH Act to increase the amount.

A Move to HIPAA Enforcement

Actors in the health care space know that OCR has taken a relatively soft approach to enforcing HIPAA's security requirements, at least with respect to issuing fines for security breaches involving protected health information (PHI). OCR instead has required violators to take "corrective actions" and enter into resolution agreements.[2]

Concurrent with the push to digitizing medical records, however, Congress recognized the need for more certain and substantial penalties for unauthorized disclosure of PHI. Therefore, to encourage greater enforcement efforts on the part of OCR, HITECH includes provisions for mandatory fines.[3] HITECH Act Section 13410(d) provides a tiered civil monetary penalty structure, as shown in Figure 1.

Additionally, Congress stripped OCR of its role as the sole authority to enforce HIPAA's privacy and security provisions. Congress also granted enforcement rights to

states' attorneys general to bring action on behalf of their citizens.[4] OCR apparently accepted this change, announcing in March 2011 that it is hosting a series of two-day workshops to train states' attorneys general in their new enforcement role.[5]

Clarifying Willful Neglect

HIPAA defines "willful neglect" as "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."[6] Last July, in its proposed rule to modify HIPAA, the OCR clarified that the "term not only presumes actual or constructive knowledge on the part of the covered entity that a violation is virtually certain to occur but also encompasses a *conscious intent* or *degree of recklessness* with regard to its compliance obligations."[7] These compliance obligations include having the required policies and procedures in place necessary to protect PHI and actively enforcing these policies and procedures.

To bring the point home, OCR provided examples:

1. A covered entity disposed of several hard drives containing electronic PHI in an unsecured dumpster, in violation of §164.530(c) and §164.310(d)(2)(i). HHS's investigation reveals that the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard PHI during the disposal process.
2. A covered entity failed to respond to an individual's request that it restrict its uses and disclosures of PHI about the individual. HHS's investigation reveals that the covered entity does not have any policies and procedures in place for consideration of the restriction requests it receives and refuses to accept any requests for restrictions from individual patients who inquire.

The Cignet Case

OCR's investigation of Cignet was sparked by 41 individual patient complaints when Cignet denied them access to their medical records between September 2008 and October 2009. The HIPAA privacy rule requires that covered entities provide patients copies of their medical records within 30 (and no later than 60) days of such patient's request.[8] Cignet never provided the information to the patients. Moreover, and perhaps more critically, Cignet never produced subpoenaed records related to the investigation to OCR, forcing OCR to go to the U.S. District Court for relief.

On March 30, 2010, OCR obtained a default judgment. OCR noted that while Cignet produced the medical records on April 7, 2010, following entry of the default judg-

Figure 1:

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but the violation is corrected within 30 days of the date on which the person liable for the violation knew, or by exercising reasonable diligence would have known, that he/she violated HIPAA; mandatory penalty	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected; mandatory penalty	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

ment, it "made no efforts to resolve the complaints through informal means."[9]

HHS found that Cignet was willfully negligent because (i) it refused to respond to OCR's demands to produce the requested records, and (ii) it had "failed to cooperate with OCR's investigation on a continuing daily basis" since March 17, 2009. OCR further concluded "that the *failure to cooperate was due to Cignet's willful neglect to comply with the Privacy Rule.*"[10]

Importantly, OCR assessed Cignet a *$1.3 million* penalty for failing to comply with the HIPAA privacy rule and a *$3 million* penalty for failing to cooperate with OCR's investigation. OCR notified Cignet of the proposed penalty on October 20, 2010, and advised it of its 90-day period to request a hearing on the amount.[11] Cignet failed to appeal, and the penalty is now final.[12]

Why Does This Matter for HIT?

OCR's handling of the Cignet matter, together with other recent HIPAA/HITECH actions commenced by attorneys general in Connecticut, Indiana, and Vermont, clearly raise the stakes for noncompliance with the privacy rule and other PHI-related security requirements. Now more than ever it is essential that organizations handling PHI (covered entities and business associates) establish and maintain compliance with all aspects of HIPAA. Furthermore, if HHS/OCR come knocking, a lack of proper cooperation could result in a significantly multiplied fine. This is of course in addition to immeasurable damage to reputation and the long-term reporting obligations required under resolution agreements.

Compliance includes developing, implementing, and enforcing proper policies and procedures for properly monitoring PHI disclosures (both physical and electronic) and for responding in the event of an unauthorized PHI disclosure. Additionally, organizations regularly should review the most recent security guidance from the National Institute of Standards pertaining to appropriate encryption methods for PHI. Finally, should any division of HHS ever contact your organization, it is essential that your privacy officer, which is a required position under HIPAA, respond to the inquiry. Involvement of legal counsel also may be appropriate, depending on the nature of the inquiry and the level of potential risk to the organization.

Endnotes:

1. Press Release, Dept. of Health & Human Services, HHS Imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule (Feb. 22, 2011), *available at* www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html [hereinafter HHS Press Release]. On February 23, 2011, HHS issued another press release; this one announcing a settlement with General Hospital Corporation and Massachusetts General Physicians Organization, Inc. for $1,000,000. *See* Press Release, Dept. of Health & Human Services, Massachusetts General Hospital Settles Potential HIPAA Violations (Feb. 24, 2011), *available at* www.hhs.gov/news/press/2011pres/02/20110224b.html.
2. *See generally* HHS, Case Examples and Resolution Agreements, www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Mar. 7, 2011).
3. HITECH Act, § 13410 (2009).
4. Richard Blumenthal, the former Attorney General of Connecticut, was the first to use this new HITECH Act enforcement right, among his other options, when his office sued Health Net of Connecticut for losing the medical and financial information of nearly 450,000 enrollees and failing to timely notify those affected. Most recently, in January 2011, Attorney General William Sorrell of Vermont announced that his office settled a lawsuit against Health Net and Health Net of the Northeast. The Vermont lawsuit involves similar issues to those of Connecticut. To settle its Vermont lawsuit, Health Net would pay $55,000 to Vermont, submit to a data-security audit, and file reports with Vermont regarding information security programs for the next two years.
5. *See* Joseph Conn, *HHS to Train State Attorneys General on HIPAA*, ModernHealth.com, Mar. 10, 2011, www.modernhealthcare.com/article/20110310/NEWS/303109988#ixzz1GWgAvPrs ?trk=tynt.
6. 45 CFR § 160.410.
7. HHS, Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act (July 12, 2010).
8. *See* 45 CFR 164.524.
9. *Id*.
10. HHS Press Release.
11. *See* Letter from the Dept. of Health & Human

Services, Office for Civil Rights to Cignet Health Center (Feb. 4, 2011), *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltyletter.pdf.

12. *Id*.

Reprinted from Journal of Health Care Compliance, Volume 13, Number 3, May-June 2011, pages 81-84, with permission from CCH and Aspen Publishers, Wolters Kluwer businesses.
For permission to reprint, e-mail permissions@cch.com.