Oregon Healthcare News

orhcnews.com | Articles, Interviews and Statistics for the Healthcare Executive

HIPAA Civil Money Penalties: Is There A Limit?

By Emily R. Studebaker
Owner
Garvey Schubert Barer

By Stephen D. Rose
Owner
Garvey Schubert Barer

The Office for Civil Rights ("OCR") recently posted the HIPAA training materials used to educate the State Attorneys General ("State AGs").[1] The Health Information Technology for Clinical and Economic Health ("HITECH") Act, part of the American Recovery and Reinvestment Act of 2009, empowered State AGs to bring civil actions on behalf of their state residents for violations of the HIPAA Privacy and Security Rules. OCR created HIPAA training materials to familiarize the State AGs with OCR's view of the HIPAA Privacy and Security Rules and how they presumed the State AGs would use their new authority to enforce HIPAA.

The HIPAA training materials consist of a number of video recordings of the presentations made to the State AGs. Of interest for purposes of this article is the OCR presentation on computing Civil Money Penalties ("CMPs") and how to maximize the penalties imposed.

The HITECH Act increased significantly the dollar amount of CMPs that could be imposed for violations of the HIPAA Privacy and Security Rules by OCR. Prior to HITECH the maximum penalty that could be imposed for a HIPAA violation was $100 per violation with a maximum of $25,000 per calendar year. The HITECH Act created four levels of CMPs with the minimum amount per category being set based on degree of culpability. The yearly maximum was increased from $25,000 per year to $1,500,000 per year.[2]

OCR was given authority to impose significantly higher penalties by HITECH. Simultaneously State AGs were given authority to prosecute HIPAA violations where the State AG has reason to believe that the interest of one or more of its state residents has been or is threatened by a HIPAA violation. However, the State AGs were not given the same latitude with respect to imposition of CMPs. Rather, the State AGs were limited to the first tier maximums for CMPs they could seek in court: $100 per violation with a $25,000 yearly maximum. The HIPAA trainers presented the table at the top of page two to explain the difference between the CMPs that OCR could impose versus what the State AGs could impose.[3]

Statutory Damages		
For Violations Occurring on or After 2/18/2009	For Violations Occuring	
	SAG	OCR
Damages/Penalty Amount	Up to $100 per violation	$100 to $50,000 or More per Violation
Calendar Year Cap	$25,000	$1,500,000

The OCR HIPAA training materials first note that CMPs with a $100 per violation and $25,000 yearly maximum might seem measly, but then introduce their concept of "continuing violations." The training materials explain that "continuing violations" allow State AGs to "expand" the $100 per violation maximum and take full advantage of the CMPs that can be imposed.

OCR explains that continuing violations can be found where the HIPAA violator acts in an improper basis on a continuing basis or where the entity subject to HIPAA fails to act when the Privacy or Security Rules require action by that entity. Examples are given.

Under HIPAA, Covered Entities are required to have in place written policies and procedures implementing the HIPAA Privacy and Security Rules. Failure to have written policies and procedures constitutes a HIPAA violation. Under the OCR "continuing violation" theory, failure to have written violations does not constitute just one $100 violation. OCR argues that the $100 penalty can be assessed for each day that it can be shown that written policies and procedures were not in place. Thus, if the State AG determines that no written policies or procedures were in place for 2011, a CMP of $25,000 can be imposed. OCR states that the entity is fined $100 per day for 365 days which equals $36,500, but the total CMP is capped by the $25,000 per year maximum. However, OCR notes that the State AG can go back multiple years, so that if no policies or procedures were in place for the last six years a CMP of $150,000 can be imposed: $25,000 per year for each of the six years.

After explaining the concept of "continuing violations," the HIPAA trainers explain how to "stack" violations to maximize CMPs imposed. As part of the HIPAA training each State AG participant was provided with a listing of the HIPAA Privacy and Security Rules and were encouraged to use those materials "as a guide in terms of how many violations you could possibly find" as part of any investigation. The HIPAA trainers noted that many investigations start with just one issue, but once the investigators start reviewing matters they can find other issues and violations.

The OCR HIPAA trainers highlight two pre-HITECH cases which occurred when the maximum CMPs allowed were $100 per violation with the $25,000 yearly cap where they were able to impose total CMPs of $1,000,000 or more. For each of these cases the OCR investigators determined that the entity being investigated failed to have proper HIPAA policies and procedures in place. Further, OCR determined that multiple employees at multiple locations within the chain of stores being investigated had violated the Privacy Rules by failing to properly dispose of documents containing protected health information ("PHI") and that none of the employees had been disciplined for their failure to comply with the Privacy Rule requirements concerning the proper destruction of documentation containing PHI.

Stacking the various continuing violations allowed OCR to calculate CMPs for the two chains of $1,000,000 or more according to the table at the top of page three.[4]

The OCR trainer noted that, for each chain, they assessed CMPs going back three or more years and concluded by stating:

> *So, each year, there may be a max of $25,000 for each violation, but if you multiply each of those violations and you're looking at multiple years, multiple violations, and multiple covered entities, you can reach a million dollars.*[5]

OCR provided HIPAA training at four separate locations throughout the United States in 2011.[6] Every State Attorney General was invited to send attorneys for training and most states took advantage of this training. OCR's emphasis on stacking violations and use of "continuing violations" to maximize CMPs underscores OCR's tightening of enforcement stan-

Stacking the Various Continuing Violations Allowed OCR to Calculate CMPs for the two Chains of $1,000,000 or More:		
164.530(i)(1)	Privacy Rule: Written Policies and Procedures	$25,000 per year per store
164.502(b)	Privacy Rule: Minimum Necessary Requirements	$25,000 per year per store
164.502	Privacy Rule: Prohibition Against Impermissible Use	$25,000 per year per store
164.530(B)(1)	Privacy Rule: Workforce Education on HIPAA:	$25,000 per year per store
164.530(e)	Privacy Rule: Employee Sanctions Requirement	$25,000 per year per store
164.308(a)(1)(ii)(C)	Security Rule: Employee Sanctions Requirement	$25,000 per year per store

dards for HIPAA. In the current era of significant budget shortfalls for states, there is little doubt that states will actively pursue HIPAA enforcement and the aggressive assessment of CMPs.

Emily R. Studebaker practices exclusively in the area of health law, advising ambulatory surgery centers and physician practices on issues including accreditation, certification and licensure as well as certificate of need and transactional matters. She can be reached at estudebaker@gsblaw.com.

Stephen Rose has more than 25 years of experience representing clients in the healthcare industry. His practice focuses on Medicare / Medicaid reimbursement, defending healthcare providers during and after government audits, developing and implementing corporate compliance plans, addressing certificate of need issues, and assisting hospitals with credentialing and privileging issues. He can be reached at srose@gsblaw.com.

[1]http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html

[2]42 U.S.C. § 1320d-5(a).

[3]http://www.hhshipaasagtraining.com/module6.php at slide 13.

[4]All regulation references are to 45 C.F.R. Part 164.

[5]http://www.hhshipaasagtraining.com/module6.php

[6]http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/registration.html

Reprinted with permission from the Oregon Healthcare News. To learn more about the Oregon Healthcare News visit orhcnews.com.