

# HIPAA Compliance Enforcement No Longer 'Toothless Tiger'

July 27 2011 // by [Jeff Drummond](#) // 337 Views // 0 Comments  
[compliance](#), [HIPAA](#), [medical records](#), [breaches](#)



Employees at UCLA Medical Center snoop into celebrity patients' medical records. UCLA self-reports, but still pays a \$865,500 fine. A Massachusetts General Hospital researcher leaves a box of medical files on the subway, the records are never found and there's no indication of identity theft or other wrongdoing. And Mass General pays a \$1 million fine. Cignet Health ignores patient requests for copies of records, and there's no improper disclosure at all, but Cignet is fined \$4.3 million. A UCLA surgeon looks at medical records of celebrities and his boss, but doesn't disclose them, sell them to the National Enquirer, or do anything else for that matter, but he gets four months in prison.

And this just scratches the surface. According to HHS' Web site for "big" breaches (those involving 500 or more people in a particular jurisdiction), in the 17 months that the "wall of shame" has been up, there have been almost 300 breaches involving the records of at least 11 million individuals.

During the first few years after passage of [HIPAA](#) and the publication of the Privacy Rule, HIPAA prosecutions were virtually unheard of. It was more than five years after the enforcement date of the Privacy Rule before the first covered entity scofflaw paid for a HIPAA breach (and that was a settlement agreement, not even a real fine - the first actual fine under HIPAA came this past spring). However, that lax enforcement environment is over.

What's driving this increase in enforcement activities? Privacy advocates have long contended that HIPAA is a toothless tiger, as evidenced by the lack of enforcement. These activists attract media attention, which attracts the attention of legislators and regulators, who want to take visible actions that make them seem effective, whether they are or not. In addition to requiring publication of the "Wall of Shame," the HITECH Act [also](#) raises the level of fines for breaches, particularly egregious breaches, which raises the stakes in the event of a breach investigation. A single HIPAA violation, if egregious enough, can carry a fine of \$1.5 million.

Perhaps most importantly, HITECH allows the attorney general of each state to prosecute HIPAA violations, and allows individuals an opportunity to share in the fines recovered. Under the original HIPAA regulations, only the federal government, through the HHS Office of Civil Rights, had the ability pursue HIPAA violations. And the HIPAA regulations specifically stated that individuals did not have any private course of action to pursue for a HIPAA violation. HITECH changes that. Now, each state's Attorney General can pursue HIPAA violators. State AGs are usually elected officials, and elected officials usually like to get re-elected. A great way to get re-elected is to take some high-profile, newsworthy action that seems to be championing the downtrodden. What man or woman running for re-election wouldn't want to be on the evening news, standing in front of a press conference, talking about how they're protecting some innocent citizen from some evil provider or insurance company that broke the law and violated an innocent victim's personal privacy? And when that citizen gets to share in any fines that might be levied, they will be much more motivated to pursue a claim.

With new, highly-motivated enforcers pursuing HIPAA violations, and incentivized victims looking for a cash recovery for their embarrassment, the enforcement environment has radically changed. Healthcare providers, health plans and any vendors who service the healthcare industry are potential victims of these new, heightened risks. If you aren't serious about [HIPAA compliance](#) in the face of these enforcement risks, you are running [risks greater than you imagine](#).