# **Enforcement**

## **Sanctions**

The Office of Civil Rights is responsible for enforcing the HIPAA privacy regulations. Hospitals are subject to the following sanctions for violations:

* $100 per patient per violation up to a maximum of $25,000 of "an identical requirement or prohibition during a single calendar year." This penalty cannot be imposed if the violation was due to "reasonable cause and not willful neglect" and was corrected within 30 days of the time a person using "reasonable diligence" would have known about it.
* If "knowingly," not more than $50,000 and/or not more than 1 year in prison
* If "under false pretenses," not more than $100,000 and/or not more than 5 years in prison
* If knowingly sells private information for compensation, not more than $250,000 and/or not more than 10 years

## **Duty to Mitigate**

Hospitals and other covered entities must mitigate any harmful effect of a use or disclosure of protected health information that is known to the hospital. This duty extends to violation of internal policies and procedures, not just violations of the regulations.

## **Private Right of Action**

The HIPAA regulations do not provide for a private right of action against a provider for violation of the privacy regulations. But see the Implementation Tip below.

* **Implementation Tip:** Office of Civil Rights compliance expectations will be "scalable;" meaning larger providers with arguably more resources to put toward compliance will be held to a higher standard than smaller providers, at least initially.
* **Implementation Tip:**  Remember that, while the HIPAA regulations do not provide a private cause of action against a provider for violation of the HIPAA privacy regulations, creative plaintiff attorneys may well find a basis in state law to bring a lawsuit based on a HIPAA violation. The HIPAA regulations may provide the inherent standard to be followed in hospital privacy practices.