New Mandatory Fines for HIPAA violations

On February 18, 2009, the United States Congress passed the Health Information Technology for Clinical and Economic Health (HITECH) Act, which dramatically increased the enforcement of HIPAA's data security provisions.

The new security provisions included

- Mandatory Health Data Breach Notification
- Increased Penalty Limits *(going from $25,000 to $1,500,000)*
- States' Attorneys General Enforcement
- Revision of All Business Associate Agreements
- Mandatory Fines for HIPAA Violations

Here is what the US Department of Health and Human Service (HHS), the agency responsible for overseeing HIPAA enforcement, says about the new mandatory financial penalties and improper PHI disposal [Federal Register, Vol. 75, # 134 (July 14, 2010)]:

> ". . . Under section 1176(c), HHS is **required** to impose a civil money penalty for violations due to **willful neglect**. Accordingly, although the Secretary often will still seek to correct indications of noncompliance through voluntary corrective action, there may be circumstances (**such as circumstances indicating willful neglect**), where the Secretary may seek to proceed directly to formal enforcement..."
>
> ". . . an amount not less than $1000 or more than $50,000 for each violation; for a violation in which it is established that the violation was due to **willful neglect** and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation; and for a violation in which it is established that the violation was due to **willful neglect** and was not timely corrected, an amount not less than $50,000 for each violation; except that a penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year."

HHS also gives the following example of Willful Neglect in the same publication, tying it directly to improper PHI disposal:

> "HHS therefore expects to apply the current definition of **willful neglect** to all newly established contexts in the same manner as previously discussed, Consider the following example . . ."
>
> "1) . . . the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process."

SUMMARY: Fines are mandatory when failure to have training and reasonable procedures on proper disposal is discovered. HHS goes on to say that had they found proper training in the same case, the same incident would not have been deemed a case of willful neglect.

Read the full text at: http://gpo.gov/fdsys/pkg/FR-2010-07-14/html/2010-16718.htm

Note: Text is not bold in the Federal Register. It is provided to draw attention to specific important information.