BusinessManagement DAILY

APRIL 23, 2018

Feds' rules for safeguarding sensitive info

A Trump administration official's frustration over confidentiality breaches has turned into useful advice that can benefit HR professionals who worry about disclosure of sensitive information.

Earler this year, Education Secretary Betsy DeVos was livid when she learned media outlets had received advance copies of the Department of Education's proposed 2018 budget, which revealed plans to delay the effective date of pending regulations.

DeVos wondered what punishment was possible for employees caught leaking such information. Could they be charged with a crime?

The department's inspector general said no, not without strict protocols in place for the sharing of confidential (but not classified) information. Then the report went on to suggest rules to protect confidential information.

It turns out, the suggestions are useful guidelines for any employer that wants to protect sensitive information. *Example:* Private employee health information collected to administer the FMLA, the ADA and the Genetic Information Nondisclosure Act.

Here are some common-sense ideas from the Department of Education report for controlling the flow of sensitive information—and punishing leakers:

Develop protocols to clearly designate documents for internal use only.

Train everyone with access to sensitive information on how to segregate confidential information from nonconfidential information. Explain the consequences of ignoring the rules.

Designate individuals who are specifically allowed access to confidential information.

Work with IT staff to create an effective information rights management system that includes security features to block access to files with sensitive information (such as personal medical information). A good rights management program prevents a document from being opened, forwarded, copied or printed except by those who have permission to do so.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002