

**Rite Aid Agrees to Pay \$1 Million to Settle HIPAA Privacy Case - Company agrees to substantial corrective action to safeguard consumer information**

From an email from the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS)

=====

*Rite Aid Corporation and its 40 affiliated entities have agreed to pay \$1 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services (HHS) announced today. In a coordinated action, Rite Aid also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act.*

*□ Rite Aid, one of the nation's largest drug store chains, has also agreed to take corrective action to improve policies and procedures to safeguard the privacy of its customers when disposing of identifying information on pill bottle labels and other health information. The settlements apply to all of Rite Aid's nearly 4,800 retail pharmacies and follow an extensive joint investigation by the HHS Office for Civil Rights (OCR) and the FTC*

*Among other issues, the reviews by OCR and the FTC indicated that:*

*Rite Aid failed to implement adequate policies and procedures to appropriately safeguard patient information during the disposal process;*

***Rite Aid failed to adequately train employees on how to dispose of such information properly; and***

## It's all about T R A I N I N G

By John Glenn  
July 27, 2010

---

*Rite Aid did not maintain a sanctions policy for members of its workforce who failed to properly dispose of patient information.*

*Under the HHS resolution agreement, Rite Aid agreed to pay a \$1 million resolution amount to HHS and must implement a strong corrective action program that includes:*

*Revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;*

***Training workforce members on these new requirements;***

*Conducting internal monitoring; and*

*Engaging a qualified, independent third-party assessor to conduct compliance reviews and render reports to HHS.*

*Rite Aid has also agreed to external independent assessments of its pharmacy stores' compliance with the FTC consent order. The HHS corrective action plan will be in place for three years; the FTC order will be in place for 20 years.*

=====

The other day, July 23, 2010, I blogged about &quot;Security awareness training&quot;. I have, on numerous other occasions on the blog and on the Web site, written about the importance of training.

Usually, the focus is on personal safety; people are, after all, both an organizations most important resource and its first line of warning that a threat is about to occur or increase in

## It's all about T R A I N I N G

By John Glenn  
July 27, 2010

---

intensity.

This time the focus is on The Bottom Line.

Granted, not every organization needs to be concerned with HIPAA or the FTC, but the admonishment is the same for all - on-going training is needed to help keep an organization safe - safe physically, safe financially.

Because Rite Aid, according to HHS's OCR regulators, "failed to adequately train employees on how to dispose of such information properly" the business finds itself under the HHS microscope for three years and under the FTC's close scrutiny for TWENTY years.

And of course there's the matter of the \$1 million fine that, probably in the overall scheme of things, is a pittance to pay.

It might be argued that the cost of doing what should have been done before, specifically

Revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;

Training workforce members on these new requirements; Conducting internal monitoring; and

Engaging a qualified, independent third-party assessor to conduct compliance reviews and render reports to HHS.

might have cost more than the penalty, but remember that now the organization must do all those things AND pay the \$1 million fine AND suffer some PR fallout; how much of an image hit depends on how aggressively HHS's OCR publicizes its queue and how much Rite

## **It's all about T R A I N I N G**

By John Glenn  
July 27, 2010

---

Aid competitors may want to risk mud-slinging.

When it comes to The Bottom Line, and that is what Enterprise Risk Management is all about, it pays to look at all the risks; the obvious (environment, technological, and human) and the less obvious (training, policies and procedures, compliance).

John Glenn, MBCI  
Enterprise Risk Management Practitioner  
Hollywood - Fort Lauderdale Florida