

Taking a Stand on Sanctions

Save to myBoK

by Vera Rulon

The Journal of AHIMA kicks off our Health Information Privacy and Security Week series with a post from AHIMA president [Vera Rulon](#), MS, RHIT, CCS, FAHIMA. Rulon is director of strategy and communications in the chief medical office of Pfizer, Inc.

So I get this communication that my credit card information was stolen due to a data breach at a known hotel chain. My first reaction was panic. The credit card company had already cancelled my card and issued me another, but that didn't help me. I was still in a panic. Financial information and breaches are potentially far reaching and could have jarring impact on personal lives. But then I thought, the financial industry does have sanctions and recovery plans for data breaches. What about healthcare? Are we prepared?

The headlines are undeniable. After finding out about my credit card information, I Googled "data breaches in the news." I was astounded at what was returned! The [Privacy Rights Clearinghouse](#) has a chronology of data breaches from April 20, 2005 through today. The list is long.

On the medical front, an article in [SC Magazine](#) claims that these medical data breaches are on the rise. With the advent of electronic medical records, information is handled differently, therefore breaches occur differently than with the traditional paper record and in larger numbers. In addition, the article claims that not only are breaches on the rise, but that hospitals and medical centers are slow to report these breaches to patients.

In my opinion, reporting breaches to patients is paramount. My usual mantra is that it is better to be transparent and open. Individuals need to know that their personally identifiable information was breached, as I did in my credit card situation, in order to be more alert and aware of any suspicious activity around our information. However, more than that, we the public need to know that those responsible for the breach are sanctioned. After all, if those responsible, whether intentional or not, aren't held accountable, will we ever change behavior or the flawed processes and systems that cause data breaches?

The American Recovery and Reinvestment Act (ARRA) places much needed focus on the need for electronic medical records/HIT and privacy and security of sensitive patient information in our needed trek towards health care reform. Part of the Act are 55 pages of what has been termed "HIPAA 2." Data breaches are specifically addressed with increased penalties of release of this information without authorization.

With the stimulus package addressing the issues of privacy and security breaches creating greater penalties, AHIMA has anticipated these issues through a Practice Brief: "Sanction Guidelines for Privacy and Security Breaches." This brief, due to be published by the *Journal of AHIMA* in May 2009, resulted from a House of Delegates resolution. It is terrific to see the AHIMA federation model working!

The Practice Brief outlines the importance for standards for breach sanctions, the different categories of employees and volunteers and what their responsibilities are, sanctioning models, and recommendations on how the process should be maintained and monitored. The Practice Brief is also clear on why it is paramount to ensure consistency in practice standards with regards to data breaches. For example, inconsistent responses can erode public trust. Also, if privacy and security stands are not applied consistently, more regulation can occur further confusing the situation. Watch this space for the brief next month.

In my humble opinion, this is long overdue. With all sorts of medical identity data breaches occurring it is hard to keep track, and as HIM professionals we have a duty to the public. The healthcare system needs their trust and although we cannot totally eliminate data breaches we can greatly reduce them through transparent processes that sanction those involved.

Original source:

Rulon, Vera. "Taking a Stand on Sanctions" ([Journal of AHIMA website](#)), April 2009.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.