Common Sense for the Common Good: A Critical Time for Security and Privacy Regulation

by **Linda L. Kloss** , RHIA, FAHIMA

Privacy and security are perpetual concerns for the healthcare industry. However, a real and looming threat is that privacy and security will stall progress of nationwide electronic health information exchange, notes Kirk Nahra, a legal expert interviewed in "Untangling Privacy." Darren Lacey, a chief information security officer, refers to this potential as a tragedy of the anticommons, a term with origins in an influential 1968 article by Garrett Hardin published in the journal *Science* .

The commons tragedy occurs when multiple individuals act in their own self-interest and ultimately destroy the shared resource they all depend upon. Most often this describes the overuse and waste of natural resources. Thirty years later Michael Heller described a tragedy of the anticommons, in which many rational individuals acting separately waste a given resource by *underusing* it.

There is great value in the proper use of health information to support patient care and the common good such as quality improvement, clinical research, and public health.

Framework for Information Exchange

This past December the Office of the National Coordinator for Health Information Technology released the long awaited "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information," a must-read for all HIM professionals. Much work remains to flesh out the specific processes for the electronic exchange of individually identifiable health information, but this framework is an important start.

And it comes none too soon. Debate is once again ramping up in Congress, with well-intentioned advocates suggesting legal remedies that would cripple the delivery of healthcare. Privacy breaches continue to hit the front pages of the news. "Sounding the Alarm" describes what constitutes a breach and factors affecting the notification process. "Be prepared" is the advice of the experts in this article.

Responding to criticisms about his article on the commons, Hardin later commented that he should have titled it the tragedy of the *unregulated* commons. This is indeed a critical time for commonsense approaches to security and privacy regulation—federal and state. We must all engage with rule makers to craft enforceable regulation concerning health information exchange that balances the interests of those seeking the benefits of legitimate use of information and those wanting to lock down virtually all of it. Squandering this opportunity by acting only in self-interest could set us back years.

Future-focused Improvement

The policy wish list of many hospital information management and finance managers probably includes a plea that the Recovery Audit Contractor (RAC) process be suspended by the new administration until it can be reconceived and redesigned. In "RAC Ready" Kathy Johnson, Allison Bloom, Denise Morris, and Rod Madamba share their experiences with RAC auditing and translate these to advice for preparation and response.

Compliance generally can be achieved through effective processes that reflect sound business practices. There is no doubt that most healthcare organizations can improve workflow processes for coding, billing, chargemaster, medical necessity, and other systems that come under RAC scrutiny.

However, improvements should enable a future that supports greater levels of electronic processing and standardization. In this way, RAC preparation won't be an isolated response to an external threat but will provide future-focused improvements that

support improved results for organizations.

Article citation:
Kloss, Linda L. "Common Sense for the Common Good: A Critical Time for Security and Privacy Regulation" *Journal of AHIMA* 80, no.2 (February 2009): 19.