

Re-examining HIPAA Six Years Later

Save to myBoK

by Linda L. Kloss, RHIA, CAE, FAHIMA

It was six years ago this month that the HIPAA privacy rule went into effect. For many in healthcare, compliance has become a routine part of doing business. But for too many, the current regulations remain poorly understood and poorly implemented. All the while, the environment has been changing, rendering obsolete some of the assumptions upon which HIPAA was built.

The privacy and security environment in the US today remains a complex and polarizing mix of policy, operations, and legal and regulatory issues. In this issue of the Journal we take a look at what is working, what is not, and where we go from here.

Environmental Scan

In “What’s Next for the Privacy Rule?” Jill Callahan Dennis recounts the progress and pitfalls for providers and patients. Although implemented in 2003, the regulations were crafted a decade ago, and regulators were not anticipating the new kinds of organizations that now have access to patient information. Dennis describes the current policy environment and the difficult choices ahead as we work to improve stewardship and patients rapidly become more aware of their rights.

M. Peter Adler discusses the many reasons why compliance with HIPAA continues to elude most organizations. In “Integrating Privacy and Security” Adler notes that many organizations fail to coordinate their privacy and security programs, further straining scarce resources. He offers recommendations for refocusing and improving enterprise privacy and security programs.

Identity theft is a particularly damaging crime that seems all the more heinous when perpetrated by employees of a healthcare organization. In “Responding to Identify Theft” Jenny O’Brien recounts how one organization reinvigorated its employees’ personal connection to privacy and security through its response to identity theft at one of its facilities.

HIPAA and Interoperability

“Harmonization Destination” reports on the current phase of the unprecedented Health Information Security and Privacy Collaboration project. Earlier phases brought to light the significant variation in privacy and security laws across the 50 states and the even greater variation in practice and interpretation of federal and state laws. We are very proud of the contributions AHIMA members and staff have made to this project. Our commitment reflects our belief that privacy and security lie at the heart of a nationwide health information network.

We don’t expect national consensus around privacy and security anytime soon. We also don’t expect a quick resolution to the knotty policy issue of person identification. As Lorraine Fernandes and Michele O’Connor explain in “Patient Identification in Three Acts” there have been advances in patient ID technology and some solid learning about the issues and alternatives. A new idea is a voluntary healthcare identifier system. Fernandes and O’Connor outline the system and point to a coming RAND study that suggests a possible solution.

Six years ago we were working hard to ensure that that our healthcare organizations were capable of full compliance with privacy regulations. We were thinking of it as launching a rocket, not building a space station. It’s tough to shape and change a culture—particularly while it is being redesigned. It’s very clear that the need for strong leadership from the HIM community is as urgently needed today as it was in 2002. We are a bit older and a bit wiser, and we remain as resolved as ever to do what is right for patients.

Article citation:

Kloss, Linda L. "Re-examining HIPAA Six Years Later" *Journal of AHIMA* 79, no.4 (April 2008):

23.

Driving the Power of Knowledge

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