Balancing Access, Privacy, and Security: Applying Core Values in an Era of Accelerating Digital Practice

By Alan F. Dowling, PhD, chief executive officer

In our rapidly changing world, it is heartening to recognize the immutability of AHIMA's ethics. This year marks the twenty-fifth anniversary of AHIMA's position statement on health information confidentiality. The statement addressed the ethical practices needed to safeguard the health information entrusted to the care of the medical community and encouraged members to "work diligently toward implementation of these practices."

Balancing Privacy and Access

Privacy and security issues were central discussion points when AHIMA opened its international office in Brussels recently. The University of Ghent Medical Center's staff briefed AHIMA staff on Belgium's strict privacy laws.

Impressively, the medical center can report instantaneously on access to patient electronic records, a feat rarely duplicated in the US. Belgium's privacy legislation applies to all personal information, not just health information. Belgium is not alone among EU nations in enacting comprehensive privacy laws.

A February 26 *New York Times* article titled "When American and European Ideas of Privacy Collide" partly attributes this to the "profound European commitment to privacy, one that threatens the American conception of free expression…" In the article Jane Kirtley, who teaches media ethics and law at the University of Minnesota, writes that Europeans consider privacy a "fundamental human right."

In this sense, there is common ground with AHIMA's position. The challenge for us is to ensure privacy while enabling legitimate information flows for care quality and organizational effectiveness.

Ensuring privacy is dependent upon instituting appropriate privacy policy and operating accordingly. Nevertheless, vulnerabilities will evolve.

Safeguarding Privacy with Health IT

One area of both promise and concern is the increased use of existing technology, such as the Internet, and the adoption of new technologies, such as mobile devices, to transmit confidential health information.

Since the 1969 implementation of the Advanced Research Projects Agency Network, the Internet's forerunner, messages have been subject to attack. Kevin Stein and Matthew Scholl remind us in "E-mail Security" that all e-mail users, especially those responsible for transferring protected health information, need to understand e-mail's vulnerabilities and the methods necessary to keep e-mail messaging as safe as possible.

In "Moving Targets," Claudia Tessier notes that the majority of American adults currently use online sources to seek information. Mobile devices are already widely used by many as they interact with medical centers' and insurers' online portals such as Cleveland Clinic's MyChart. Tessier discusses these devices' adoption for use within care delivery teams and lists topics HIM professionals must address as mobile devices are deployed as a core part of health information communications.

History has proven the value of securing health information communications and the reality that breaches in security will occur. "A Guide to California's Breaches" reports that in 2009, the California Department of Public Health received notification of nearly 2,500 breach incidents. California's experience shows that most breaches are inadvertent disclosures, but that intentional unauthorized access is a constant threat.

In a related article, "A Workflow for Breach Notification," Tom Walsh provides a specific and effective approach for complying with HIPAA breach notifications.

Article citation:
Dowling, Alan F.. "Balancing Access, Privacy, and Security: Applying Core Values in an Era of Accelerating Digital Practice" *Journal of AHIMA* 81, no.4 (April 2010): 21.
