DRAWING THE LINES
WITH HIPAA

Most Americans sign the HIPAA agreement annually at their physician's office as a routine requirement for care. HIPAA laws protect our health care privacy, meaning others, unless we allow it, cannot access information regarding our care. For many people, HIPAA is a sacred trust between themselves and their provider.

The Health Insurance and Portability and Accountability Act was enacted in 1996. In its simplest form, HIPAA has two sections: the privacy rule and the security rule. The first deals with providers protecting patient privacy; the latter concerns the security of protected health information either in storage or transmission, especially electronically.

Critics of HIPAA cite flaws in both areas, though the primary concern is cybersecurity. Mac McMillan, an expert in health information and regulatory compliance, notes the obvious: "Does anyone really believe that the environment that average health care workers function in today is really that simple when it comes to data security?" Health care organizations experiencing security breaches — Anthem, Community Health, and my former organization, Banner Health — can attest to the flaws existing in security programs and information architecture. Already, many systems are working to create more stringent security measures than HIPAA requires to protect themselves from hackers and increasingly sophisticated malware.

HIPAA was conceived more than fifteen years ago and since then, McMillan says, "Standards that address security … have gone through multiple updates and changes. Even new areas such as cloud, mobility, and medical device security have emerged, areas that HIPAA never envisioned." In a recent survey of health care executives attending their cybersecurity conference, CynergisTek asked what the most challenging issues are today. Responses included cybersecurity and privacy, vendor breaches, and medical device security. Many organizations have inadequate strategies for effectively preventing security breaches. Detailing the findings of this report, McMillan again noted HIPAA's security provisions are outdated. "In a year of more breaches, new attacks, increased phishing, and yet another year into HIPAA's security rule — which is not aging well in terms of actually improving security" — an even more pressing need for health care organizations to revisit security is created. He notes that any such upgraded standard "continues to lag across the health care industry at large," primarily because there is too much emphasis on compliance with HIPAA regulations.

He also notes the cybersecurity framework developed by the National Institute of Standards and Technology has identified five critical categories: identification, protection, detection, response, and recovery. Detection, McMillan states, "is where the incident happens. It's the 'boom' event." Everything else is prevention or response and recovery.

In the next five years, McMillan expects that a more rigid federal privacy statute may be enacted that will tighten security. Until that time, health care organizations and consumers will have to remain vigilant about security threats.

For works cited: go to www.phikappaphi.org/forum/fall2019

MAIRE O. SIMINGTON (Arizona State University) is on the faculty of the School of Community Health Sciences at the University of Nevada, Las Vegas. She is a graduate of Hofstra University, the University of Phoenix, and ASU. She is a peer reviewer for the *Journal of American Culture* and the *Journal of Healthcare Management*.