How time flies: The Health Insurance Portability and Accountability Act (HIPAA) turned 20 on Aug. 21, 2016. The 175-page statute whose acronym we now consider to be synonymous with health privacy was then known as the Kennedy-Kassebaum bill and focused more on allowing individuals to maintain insurance when changing jobs, limiting some coverage restrictions on pre-existing conditions, and encouraging and standardizing the use of technology for health information. The law was only secondarily concerned with protecting that information from misuse, exploitation or attack.

A lot has changed in the two decades since its enactment. When HIPAA was signed into law by President Bill Clinton two decades ago, the way we used technology was very different. Most home computer users who were online relied on slow, clunky dial-up modems that they shared with their land lines (a vanishing 20th century artifact) and paid for by the minute. Only 20 million Americans had access to the Internet at all, and they spent an average of only 30 minutes per month surfing the World Wide Web (as it was still known). AOL was the largest website and ISP. There was no YouTube, Facebook, Twitter or Wikipedia, and only a minimal online presence of publications like Time and The New York Times. Google had just been launched. Cellphones weren’t very smart yet and most of them were incapable of sending or receiving text messages. (Nokia, who produced one of the first text-enabled cellphones, reported that its customers sent 0.4 SMS texts per month in 1995). The first webmail site, Hotmail, launched in July 1996. There was no instant-messaging software until ICQ appeared in 1997. USB flash drives didn’t hit the market until 2000.

The majority of health transactions were transmitted on paper via snail mail or fax, or through highly incompatible electronic systems. By comparison, the Department of Health and Human Services (DHHS) reports that 93.8 percent of all health care claims transactions today are conducted electronically in standard form.

Today, most of us carry one or more devices containing a treasure trove of potentially exploitable personal information, from credit card numbers to health records to financial account information. Businesses of all kinds, including health care providers and insurers, routinely transmit data online from desktop computers and, increasingly, from those same ubiquitous portable devices. Cellphones, laptops and flash drives have a tendency to wander, and if accessed, can expose personal data to threats barely imaginable in 1996. (This is why we are constantly nagging you about encryption.) Lost and stolen devices are consistently the most commonly cited source of HIPAA breaches, affecting more than 500 individuals as reported on the DHHS Office of Civil Rights’ “wall of shame,” but such mobile devices containing protected health information (PHI) were uncommon when the law was conceived.

As HIPAA took effect, a number of exaggerated myths circulated about how it would impact physician practices, hospitals and other health entities. How many of you can remember hearing rumors that sign-in sheets in medical offices would be prohibited, semi-private hospital rooms would be outlawed due to the risk that discussions of one patient’s health would be overheard by the other patient, staff would not be permitted to call a patient by name in the waiting room, and family members would be prevented from picking up a patient’s prescriptions? None of these rumors was true, but many entities acted on them anyway. I experienced this overreaction myself when a hospital medical records clerk initially refused to give me copies of my own records from a previous physician, by then retired, unless I could tell her the date on which I had last seen him (over a decade previous), citing “that new HIPAA law.”

The exponential growth of digital health information in motion and at rest has inspired a similar explosion of...

Continued on Page 380
opportunistic crime and created a thriving illicit trade in health data. In 2014, Reuters News Service reported: “Your medical information is worth 10 times more than your credit card number on the black market … Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number.”

Accordingly, we now must deal with many issues that were not a gleam in the eyes of the federal and state governments, health care organizations, insurers, patients and many other stakeholders in 1996. Who would have predicted the rise of “ransomware,” the extortion of payments by locking an organization out of their own data using viruses and malware? Surprisingly, the concept first came up in a meeting of the “white hat” anti-hacking community.

According to Wikipedia, the first secure data kidnapping attack was invented by experts at Columbia University and was presented at an IEEE Privacy and Security conference in 1996. Fast forward 20 years to the first six months of 2016, and ransomware attacks of hospitals made headlines after a hospital in Hollywood, Calif., paid $17,000 in ransom (reportedly in bitcoins, another digital invention never considered in 1996).

DHHS released a “FACT SHEET: Ransomware and HIPAA” in July 2016, reporting a 300 percent increase in ransomware attacks reported in the first six months of 2016 as compared with those reported in all of 2015. It’s hard to imagine that, back in 1996 (or even in 2000 or 2003, when the Privacy Rule and Security Rule, respectively, were first promulgated), HIPAA compliance would require staving off and responding to cybersecurity attacks involving data “kidnapping.”

Some other developments that may have surprised HIPAA’s architects of 20 years ago include the Federal Trade Commission’s intrusion into the regulatory game; the promotion of health information mobile apps by health systems to let patients access their own test results, records and data; controversies over HIPAA’s alleged
negative effect on responding to health crises like Ebola and the Zika virus; and obstacles encountered in obtaining and disclosing information in times of tragedies like the Orlando, Fla., nightclub shooting in June 2016 (particularly since such mass tragedies were barely conceivable in those pre 9/11 days).

It can be expected that many more unanticipated and challenging issues will confront HIPAA in the future as the dizzying advance of technology surges onward, matched only by the boundless ingenuity of hackers and others seeking to profit from illegal activities relating to PHI.

Mr. Maruca is a health care partner with the Pittsburgh office of the national law firm Fox Rothschild LLP. He can be reached at (412) 394-5575 or wmaruca@foxrothschild.com. He is the editor of the firm’s HIPAA, HITECH and HIT blog, https://hipaahealthlaw.foxrothschild.com/, and would like to thank Fox Rothschild partners Michael Kline and Elizabeth Litten for their contributions to this article.