LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, MAY 5, 2017

PERSPECTIVE

Killing HIPAA

By Craig B. Garner

"Sarcasm: the last refuge of modest and chaste-souled people when the privacy of their soul is coarsely and intrusively invaded." — Fyodor Dostoevsky.

Imagine a world in which a basic identification card contained a lifetime of medical information, immediately accessible during a routine physical or life-threatening emergency. The technology behind such seeming science fiction could heal a fragmented health care system, affording providers access to critical information in a timely manner to ensure the highest standard of care with maximum efficiency. Only a few years ago, such inefficiencies inherent at the core of American health care provision resulted in as much as $226 billion in increased spending annually, yet salient health care information remained just out of a provider's technical reach.

The greatest obstacle standing between American health care and the elusive, omnipotent digital medical record turns 21 this summer, the equivalent of a modern-day Methuselah in an industry defined by zeros and ones. Born the same year Google was founded and the price of gasoline was $1.22 per gallon, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) sought to improve portability and continuity of health insurance coverage by, among other things, adopting standards for organizations to develop ways in which electronic health transactions could improve health care while also addressing the security of electronic health information systems. The act's privacy component debuted in 1999, followed by a series of modifications in 2002, as well as the addition of a security rule in 2003 and an enforcement rule addendum in 2006. Changes in health care and technology during the first decade of HIPAA ultimately led to the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, which specifically focused on the privacy and security concerns associated with electronic transmission of health information

Even when it was discovered that 100 million of those 2015 breaches were the result of thirdparty hacking, HIPAA showed little mercy toward covered entities, and the Office of Civil Rights (OCR), the federal government's regulatory agency charged with enforcing patient privacy, took the position that a breach is a breach, regardless

by strengthening the civil and criminal enforcement components within HIPAA.

Together, HIPAA and HITECH revolutionized the way health care providers (also known as covered entities) and the nonclinical entities with which they teamed (also known as business associates) shared and made available for use patient health information (PHI). With such broad definitions of "breach" and the resultant draconian punishments for noncompliance, HITECH sent the act of sharing health care information back in time in many ways, forcing providers to rely upon the U.S. Post Office to deliver highly personal, often time-sensitive, sometimes life or death information, while improvements were made to the infrastructures within which electronic and facsimile transmissions took place. Purportedly simplified in 2013 through even more regulatory modifications, modern day HIPAA regulation affords practically no room for error for those who utilize technology as a way to improve the delivery of health care in the United States. As it turns out, we have come to learn that health care is more about perseverance than perfection.

In 2015, health care providers reported 113,181,615 breaches affecting 500 individuals or more, up 905 percent from the previous year. That health care breaches affect more than one-third of the nation's population is almost as troubling as the realization that these figures cover only the reported breaches over the minimum threshold of 500 or more individuals. Even when it was discovered that 100 million of those 2015 breaches were the result of third-party hacking, HIPAA showed little mercy toward covered entities, and the Office of Civil Rights (OCR), the federal government's regulatory agency charged with enforcing patient privacy, took the position that a breach is a breach, regardless.

While the OCR offers guidance to covered entities on topics ranging from the de-identification of patient health information; HIPAA's application in public health, avoiding the pitfalls of discrimination, privacy's place when it comes to HIV; the National Instant Criminal Background Check System; the lesbian, gay, bisexual and transgender community; mobile health application development; cloud computing and emergency situations, not to mention HIPAA's not-so-distant cousin, the Genetic Information Nondiscrimination Act, it remains unclear who really depends upon HIPAA for health care privacy protection. Today's millennials and members of Generation Z struggle to distinguish the electronic health record from Facebook status updates, while those patients representing Generation X most likely want only a bit of discretion when it comes to their Prozac prescriptions and the occasional sexually transmitted disease. For the few septuagenarians (aka baby boomers) and octogenarians (the silent generation) who actively rely upon technology and the internet but still demand vigorous enforcement of privacy rights in health care, Congress can probably craft an appropriate sunset provision to carry them through the nonagenarian and centenarian years, as needed.

Since 2003, the OCR resolved almost 98 percent of the 150,000 HIPAA complaints it received, generating more than $67 million in revenue from privacy-related penalties. However, the frenzy of enforcement activities over these past two years calls into ques-

tion the necessity of HIPAA, when health care providers struggle to obtain basic health information in times of crisis. The $1.55 million settlement in March 2017 due to the absence of executed HIPAA business associate agreements seems somewhat unnecessary since recent changes in the law impose statutory liability to the same business associate, with or without a written contract. The $1.2 million fine against the health plan provider that sold a copy machine but forgot to delete the stored patient health information is unfortunate. The $4.8 million fine against a New York hospital system due to the transgressions of an errant physician deactivating a personal computer server on a system network seems simply unfair. Yet when the California Court of Appeal dismissed 13 class action lawsuits against Sutter Health following the theft of an unencrypted desktop computer containing information of more than four million patients, thereby negating over $4 billion in damages and possible insolvency, other than the plaintiffs' attorneys perhaps, many more were grateful for the merciful, if questionable, decision of the court.

Laudable yet flawed, HIPAA's future must be balanced with the ways in which it chooses to forestall the coveted almighty digital medical record. Today, protections under HIPAA remain sacrosanct, even in cases where the holder of the privilege makes a public disclosure of his or her own personal data. HIPAA prohibits sharing information about a broken wrist with equal vehemence as it does details of mental illness. The authors of HIPAA in 1996 could never have anticipated modern technological upgrades and the true expansion of the word "portability," even if the strict constructionist is keenly aware that "portability" comes before "accountability" in HIPAA's own name.

Today, the value of HIPAA's portability comes from the accessibility it grants, and accountability should not be construed as a strict liability statute. Our nation has historically struggled to balance civil liberties with domestic safety. Whether or not President Donald Trump's controversial wall separating the United States from Mexico will ever come to fruition does not change the historical perspective on Japanese internment camps during World War II or implementation of the Patriot Act in more recent years.

Potential threats to the nation's health care information system include not simply identity theft and insurance fraud, but also loss of personal privacy, embarrassment and even blackmail. Greater threats include possible disruption of health care services designed to cause chaos within the medical community, not to mention foreign espionage, both of which are concerns that should not be taken lightly by any administration. Still, the absence of a digital, fully functioning infrastructure as part of the nation's health care delivery system also poses a threat to the domestic wellbeing of the United States. Today's war to save health care must make some difficult decisions, just as during any sizeable combat mission throughout our nation's history. Seemingly drastic at first blush, killing HIPAA is certainly a viable option, given what remains at risk.

Craig B. Garner *is principal of Garner Health Law Corp. and an adjunct professor at Pepperdine University School of Law, where he teaches courses on hospital law and the Affordable Care Act.*