HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

JULY 2018

Local expertise, regional teams, and multinational compliance

an interview with
Jonathan Turner

by Luis Ospina, CPCO, CHPC

Privacy is dead. Ask Alexa!

» The concept of privacy compliance for the healthcare industry has significantly evolved since HIPAA was enacted in 1996. It needs to be redefined and placed in real context.

» Technology and innovation are forever transforming the industry, making privacy compliance more challenging than ever.

» A big gap exists between the new technologies and the legal framework in charge of regulating them. The law needs to catch up and provide guidance in real time.

» Compliance decisions made by privacy officers are now based more on technological advances and less on basic principles of human interaction.

» It will require a new set of skills for privacy officers to stay relevant and contribute in a meaningful way to implement and cement sound compliance practices for the industry.

Luis Ospina *(lospina@ketchum.edu) is the Compliance Officer at Marshall B. Ketchum University-Ketchum Health in Anaheim, CA.*

An individual needing assistance is excited about using Alexa for his medication refill needs. No more phone calls to the pharmacist; no more emails to his personal care provider (PCP); and best of all, no more trips to the pharmacy to get the medication he needs. He just sends a command to Alexa, asking "her" to place a refill of his prescription. This technology is impressive, however, nothing out of ordinary, knowing the capability of technology today. The scary part comes with what Alexa could do next. Based on an algorithm Amazon engineers are testing, Alexa will eventually be able to identify patterns in the user's voice to determine, with a high degree of accuracy, the mood of the user. This new algorithm uses emotional intelligence in addition to artificial intelligence (AI) models in the coding, empowering Alexa to make quick decisions on the user's behalf.

Depending on how stressed or anxious she "feels" the voice of the user is, Alexa will connect the dots, and in this particular case, will call the user's PCP to notify him that this patient is having an episode of anxiety, or might contact 911 to address a distressed individual who might be ready to commit suicide. All of this without consent from the individual, and even without the user knowing that this is actually happening—until the paramedics and police arrive at the door. Perhaps when this article is published, this story could be already outdated, because another, more impressive feature in Alexa's arsenal was developed and implemented.

Ospina

The new reality

As farfetched as this might sound, this is not far from reality, and compliance professionals are now being challenged to operate in a completely new ecosystem. This new environment involves compliance decisions that are increasingly related to technical knowledge and software coding expertise, rather than the traditional model of reliance on human behavior and conventional learning.

It is well known that when the Health Insurance Portability and Accountability Act

(HIPAA) was enacted in 1996, the concept of privacy was applied to an industry in which the technology ecosystem was in its infancy; therefore, it was impossible to regulate something that did not exist. This is especially relevant when we talk about mobile devices and remote connectivity. As innovation continued to evolve, and despite early signs of technological disruption, industry regulators and stakeholders remained passive, and few "upgrades" were introduced to existing laws. They might have thought that healthcare was completely isolated from technological advances, and patient information was going to be forever confined inside the walls of the provider's office. Alternatively, perhaps technological advances simply outpaced our ability to keep up with rules and regulations.

More than 20 years after the launch of HIPAA, we are confronting a completely different reality. First, there was the arrival and consolidation of the algorithm as the tool of choice to resolve every challenge and expectation in the industry. Second, because the life cycles of technologies tend to be shorter and shorter as new platforms are invented or existing ones are enhanced, it becomes very difficult to regulate something that is perennially changing. Third, connectivity has allowed users to share data to a level never seen before. At the core of these three developments, the concept of privacy remains paramount and in desperate need of redefinition and protection.

Although the concept of AI is not a new one, only recently has it started to be considered a key component of the industry. Obviously, no legislator in 1996 had in mind machine learning, neural networks, or predictive analytics as guiding elements to enact HIPAA. Today, it is almost unthinkable to have a meaningful conversation about the state of the industry without making reference to at least one of the latter concepts.

Regarding the life cycles of technologies, it was never anticipated that innovation would forever change the patient care ecosystem and the industry as a whole. According to a recent study, there are approximately 318,000 mobile health apps now available in app stores, with roughly 200 new apps added daily.[1]

Finally, interoperability is starting to take hold, as more and more providers, agencies, payers, and patients are able to exchange protected health information (PHI) with fewer obstacles. Connectivity has also opened the door to an unexpected potential trend. Think of the Internet of Things (IoT) for instance, with advances in technology allowing medical devices and equipment to be interoperable and able to share patient information in real time. This means patient data will be ubiquitous across the continuum of care, improving patient outcomes.

The changing face of privacy

Privacy continues to struggle as the concept has not equally evolved to meet the challenges of the new ecosystem. Not much can be done to ensure that sensitive information will be protected at all times (in transit or at rest) or at least used properly for the benefit of the patient.

Because healthcare is a data-driven industry, the proliferation of innovative technologies relies heavily on the collection, use, storage, and sharing of patient personal information, a process that not all stakeholders are well prepared to handle. Today, it is the responsibility of compliance professionals to learn the lingo, familiarize themselves with security terminology, and expand their body of knowledge to cover a myriad of new applications relevant to their responsibilities. Gone are the days when we comfortably sat down in our offices to develop policies and design training protocols. Today's ecosystem is like a moving target, which will require privacy and compliance

officers to acquire a new set of skills to stay relevant.

Privacy is becoming more of a risk management matter for consumers and patients, rather than a mere compliance issue for organizations. Think for a moment about how we navigate the internet. Every web page, app, or platform we access requires us to provide some type of personal information that initially seems innocuous to share. The real risk surfaces when this data is aggregated by third parties to produce more sophisticated information that could be used to our detriment. No one is actually forcing us to give up our most sacred information to obtain the benefits of a particular technology; and certainly, no app developer or technology owner is going to stop introducing new solutions just because the privacy of users' information is at stake.

If we pause for a minute and conduct an unscientific analysis of our personal demographic data, we have to conclude that it would be almost impossible to prevent those bytes of information from being used publicly, or prevent access by vendors, marketers, business analysts, and government agencies after we surf the web. Then, another element is brought into the equation: consent. Because we as consumers are really bad gatekeepers of our own data, we just check the "I agree" box in every app we download, allowing those companies to use our information in ways beyond our imagination or what we can predict. A novel idea comes to play a decisive role—the concept of privacy self-management.[2] Advocated by privacy experts and legal scholars, this doctrine calls for users and consumers to exercise more control in the way they deal with their own sensitive information. Advances in technology will invariably alter the human component of ethics and compliance. We need to be prepared for the day in which ethical decisions are going to be executed not by humans, but by predictive analytic machines programmed with intelligent algorithms, just like Alexa.

Finally, there is another challenge worthy of analysis, and that is e-discovery and its implications for the role of privacy officers and their actions when it comes to legal proceedings. Patient data generated through wearables, mobile devices, and biometric applications can wreak havoc on any Compliance/Legal department, if not handled properly. Unless privacy officers have the legal background, they are not prepared to protect both patients and enterprise interests when it comes to litigation events.

Do consumers need to give up their privacy rights to enjoy the full benefits that technology brings into their lives?

Conclusion

As patients become more engaged and educated, compliance officers will confront puzzling tests: how to balance their right to privacy against the need from providers to use and share patient's data in order to improve outcomes. Do consumers need to give up their privacy rights to enjoy the full benefits that technology brings into their lives? Is the concept of privacy in need of re-evaluation or perhaps elimination altogether? The real challenge is why bother about our privacy if, in fact, it cannot be protected after all. Vexing questions, with no foreseeable answers available.

1. IQVIA Institute for Human Data Science Study: Impact of Digital Health Grows as Innovation, Evidence and Adoption of Mobile Health Apps Accelerate. *Business Wire*; November 7, 2017. Available at http://bit.ly/2GOg7tW
2. Daniel J. Solove: "Introduction: Privacy Self-Management and the Consent Dilemma" *Harvard Law Review*; May 20, 2013. Available at http://bit.ly/2IOt2xR