COSMOS
Navigate the Compliance Universe

Compliance Today - October 2020
Are we there yet? Delivering on the promise of digitizing healthcare information

By Jon Moore, MS, JD, HCISPP

Jon Moore (jon.moore@clearwatercompliance.com) is the Chief Risk Officer and Senior Vice President, Consulting Services, at Clearwater in Nashville, TN.

Several decades ago, the US healthcare industry started a journey in search of improved care and reduced costs by digitizing health information. Since then, there have been course corrections introduced through new legislation[1] and regulation,[2] as well as fuel fill-ups in the form of tens of billions of dollars in incentives for the meaningful use of certified healthcare technology.[3] Nevertheless, today it is not clear if the industry is any closer to arriving at its hoped-for destination. Or is it?

On May 1, 2020, the Department of Health & Human Services (HHS) published two final rules in the *Federal Register* targeted at improving interoperability[4] and patient access to health information.[5] One rule was from HHS' Office of the National Coordinator for Health Information (ONC) and another from its Centers for Medicare & Medicaid Services (CMS).

In its March 9, 2020, news release announcing the final rules, HHS stated that "these final rules mark the most extensive healthcare data sharing policies the federal government has implemented, requiring both public and private entities to share health information between patients and other parties while keeping that information private and secure."[6] The US healthcare industry is already feeling the impact of these rules. Many believe that the long-hoped-for destination of improved care and reduced cost is finally in sight. Others fear that this latest turn will only lead to increased costs and decreased privacy and security of patients' electronic health information.

This article will reflect on the road the healthcare industry has traveled to get to this point. It will examine why the latest government policy turned away from promoting the adoption of healthcare technology and toward promoting interoperability of that technology. The review will examine how that turn is expressed in the requirements of the new rules and concerns raised at the potential impact of the regulations on the privacy and security of electronic health information. Finally, it will take a look ahead at the possible implications for the industry.

The road traveled

Industry participants from the federal government and private sector who believed that digitizing healthcare information is key to improving patient care and reducing the cost of that care set the US healthcare industry on a journey. They envision a world where an individual's health information flows freely between patient, provider, payer, researcher, and regulator. They theorized that improved care would come from providers and patients having the information required to make appropriate diagnoses and treatment decisions. Cost savings, they hypothesized, would come not just from the reduced friction in the flow of information, but also from visibility into the cost of care and the opening up of the healthcare market to increased competition.

This theory likely had its origins in the late 1960s or early 1970s, when healthcare organizations started adopting clinical information systems and what became known as electronic health records (EHR).[7] During the 1980s, standards for electronic health information and standards bodies such as Health Level Seven International began to emerge. These systems and standards, it was thought, held tremendous promise for reducing the cost of maintaining health information and improving its accessibility.

It wasn't until 1996, however, and the passing of the Health Insurance Portability and Accountability Act (HIPAA)[8] that we saw legislation supporting the flow of electronic healthcare information. Wisely, at that time, there was also a recognition that the digitization of health information would create new risks to the privacy and security of that information.[9]

The resulting HIPAA Privacy Rule[10] went into effect in 2003 with its definition of protected health information, followed in 2005 by the HIPAA Security Rule,[11] requiring management of the risk to the confidentiality, integrity, and availability of electronic protected health information. In 2006, the Enforcement Rule[12] was introduced, allowing the HHS Office for Civil Rights to impose civil monetary penalties on organizations for violations of HIPAA and to refer offenders to the Department of Justice for potential criminal violations when appropriate.

History shows that despite the emergence of EHRs, electronic health information standards, and HIPAA, the adoption of health information technology (IT) was slow—at least too slow by federal government standards. As a result, 2009 saw the passage of the American Recovery and Reinvestment Act[13] with the included Health Information Technology for Economic and Clinical Health Act (HITECH).[14] HITECH brought with it both carrots and sticks.

The HITECH Act created the ONC, which created a healthcare IT certification program. CMS then began providing incentive payments to qualified healthcare professionals and hospitals for the meaningful use of the ONC-certified EHRs. By 2018, the payments totaled more than $38 billion.[15]

HITECH Act made other course corrections as well. It created a right for patients and third parties they designate to obtain their health information in an electronic format from providers who adopted a certified EHR. It expanded the application of the HIPAA Privacy and Security rules to business associates. But perhaps most importantly, it started Office for Civil Rights enforcement of the HIPAA Security Rule, which resulted in the HIPAA Breach Notification Rule[16] implementing breach reporting requirements, increasing enforcement, and increasing potential legal liability for HIPAA violations.

2010 saw the passage of the Affordable Care Act.[17] Primarily focused on making health insurance more available and affordable, the Affordable Care Act also included funding for grants focused on providing better care at a reduced cost. One recipient of such an award was SMART Health IT.[18] SMART Health IT is a project run out of the nonprofit institutions Boston Children's Hospital Computational Health Informatics Program and the Harvard Medical School Department of Biomedical Informatics.[19] With their $15 million grant,[20] SMART Health IT developed an open, standards-based technology platform that enables innovators to create apps that seamlessly and securely run across the healthcare system.

Despite the legislation and investment, the hoped-for benefits of improved care and reduced cost proved elusive. In late 2013, the Agency for Healthcare Research and Quality commissioned a study by JASON, an independent panel of experts, to figure out why. The results, published in a paper titled *A Robust Health Data Infrastructure,* found that:[21]

- The current lack of interoperability among data resources for EHRs is a significant impediment to the exchange of health information and the development of a robust health data infrastructure. Interoperability issues can be resolved only by establishing a comprehensive, transparent, and overarching software architecture for health information.
- The goals of improved healthcare and lowered healthcare costs can begin to be realized if health-related data can be explored and exploited in the public interest, for both clinical practice and biomedical research. That will require implementing technical solutions that both protect patient privacy and enable data integration across patients.

HHS created a JASON Task Force in 2014 to respond to the findings of the report.[22] The JASON Task Force criticized the JASON study, claiming it did not capture all the progress made. Still, in the end, the Task Force agreed with JASON's primary finding on the lack of interoperability as the critical problem.