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.

Making the turn toward interoperability

The JASON report represented a crucial turning point in US healthcare policy. Before JASON, the focus was on promoting the adoption of healthcare technology. After JASON, the focus shifted to supporting the interoperability of the technology. This change is visible in legislative and executive action.

Passed in 2016, the 21st Century Cures Act (Cures Act)[23] was primarily targeted at streamlining the drug and medical device approval processes. Also, Title IV of the Cures Act defined the term "interoperability" for health IT[24] and established penalties for deterring interoperability by information blocking, imposing fines of up to $1 million per violation.[25] The intention is to promote the use of electronic health records to improve care, empower patients, and improve access to their electronic health information.

President Trump signed Executive Order 13813 "Promoting Healthcare Choice and Competition Across the United States" on October 12, 2017.[26] The Executive Order is intended to "re-inject competition into healthcare markets" and improve Americans' access to quality of information, thereby allowing them to make better-informed healthcare decisions.

CMS Administrator Seema Verma announced the MyHealthEData initiative on March 6, 2018.[27] This initiative "aims to empower patients by ensuring that they control their healthcare data and can decide how their data is going to be used, all while keeping that information safe and secure."[28] Ultimately, the initiative aims to facilitate every American's ability to find the providers and services that best meet their unique healthcare needs and give that provider secure access to their health information.

As further evidence of the change in policy direction, CMS renamed its EHR Incentive Program, formerly known as Meaningful Use, to the Promoting Interoperability Program.[29] This change, made in April 2018, was not merely a name change but also represented an increased focus on interoperability and improving patient access to health information through the measurement of the adoption of certified health IT.

Accelerating forward with implementation

The new final rules implement portions of the Cures Act, contribute to fulfilling Executive Order 13813, and support President Trump's MyHealthEData initiative. How the rules accomplish this is summarized below.

The ONC final rule, titled the "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program,"[30] implements the interoperability provisions of the Cures Act to facilitate the flow of

information between providers, payers, and patients. It hopes to achieve this by making changes to ONC's health information certification program, regulating information blocking, and implementing standards for application programming interfaces (APIs) to exchange healthcare information. The new certification requirements apply to certified health IT developers. The API requirements apply to these same vendors but also healthcare providers and healthcare information networks.

The CMS final rule, titled the "Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers,"[31] requires payer-to-payer data exchange, use of the ONC API standards when implementing patient access APIs and provider directory APIs, and adopting conditions of participation notice requirements. The CMS final rule applies to Medicare Advantage organizations, Medicaid managed care plans, state Medicaid agencies, state Children's Health Insurance Program (CHIP) Agencies, Managed Care entities, and federally facilitated exchanges.

Potential bumps in the road

When first proposed, the rules were met with controversy, particularly over the implications for the security and privacy of protected health information. The debate or concerns fell into four areas:

1. HIPAA will generally not cover the third-party app providers, and user's private health information will be sold and exploited.
2. Transfers may include information that an enrollee or beneficiary does not want exchanged, such as mental health, substance abuse, women's health, and family history.
3. APIs are generally risky, and the required Fast Healthcare Interoperability Resources standard is new; therefore, it does not make sense to allow unregulated third-party apps access through an API at this time.
4. Provider HIPAA liability for the information provided through an API or for denial or discontinuance of access through the API.

HHS addressed each of these concerns in its Response to Public Comments published in the Federal Register as part of the final rules.[32]

Commenters assume that many, if not most, third-party app vendors will be providing their applications directly to the public, and the HIPAA Security, Privacy, and Breach Notification rules will not apply. Instead of the protections of HIPAA, third-party app developers' use of the information would be covered under the app's terms of use and privacy policy. The concern expressed by commenters is that many app users will not read or understand the user agreement and privacy policy, so they will not knowingly consent to the use or sale of their information by the third-party app provider. The third-party app providers will, in turn, monetize the data, distribute it widely, not protect it, and exploit it to the detriment of the individual to whom the information relates. Together, these two factors will effectively defeat the purposes of HIPAA.

HHS's response to this argument is that individuals are entitled to their health information. The public is now much more familiar with technology and, in particular, applications provided for use on devices such as smartphones. The Federal Trade Commission enforces violations of privacy policies, and there are state privacy laws and regulations as well. Furthermore, healthcare organizations are welcomed and encouraged to offer education and awareness training to the public on the use of third-party applications and the risks to the security and privacy of their health information. However, organizations may not actively prevent an individual's use of a

third-party application except as provided in the regulations.

There were several public comments related to concerns commenters have around the transfer of particularly sensitive information. Examples include information such as mental health, women's health, substance abuse, or family history. Commenters worried that providers may discriminate based on this information. Commenters also expressed concern that family members' information will be shared through the APIs without the individuals' consent as part of family history.

In response to these concerns, HHS stated that payers' privacy and security obligations under the HIPAA rules and 42 C.F.R. § 2 are not changed by this final rule. HHS is continuing to work on standards for parsing and segmenting data for consent and privacy management purposes. The health information the rules require to be shared at this time includes claims and encounter data, as well as the data contained in the United States Core Data for Interoperability, Version 1.[33] Family history is not a specific data class within the United States Core Data for Interoperability. As a result, HHS does not believe this should be an issue.

There were several concerns raised around the security of the APIs. An API is a software intermediary that allows two applications to talk to each other. One might think of an API as a contract between two applications that facilitates requests for information and responses. API implementations can be quite complex, and errors in their implementation and vulnerabilities in protocols used can result in unauthorized disclosures of information in the connected application.

HHS responded to these concerns by stating that it believes that the security protocols at 45 C.F.R. § 170.215 are sufficient to authenticate users and authorize individuals to access their data. Also, the HIPAA Security Rule requirements still apply until an organization uploads the information into the third-party app or other recipient's system. The safeguards under the rule, such as risk analysis, technical evaluations, audit, and encryption, apply to the required APIs.

There were several concerns related to the potential of HIPAA liability for issues with the API. The fears expressed were mostly associated with the use of the data after it is accessed. In its response, HHS was relatively clear on where the boundary line of HIPAA liability resides, and it is at the point where the data enters the third-party application. The security and privacy of electronic protected health information within the organization's environment, passing through the API or over the internet to the third-party app, is still the responsibility of the organization for HIPAA compliance purposes. Furthermore, if an organization determines through HIPAA risk analysis that the exchange of information with a particular app or third-party developer is too risky, it may deny access.

The road ahead

Table 1 lists the original compliance dates for requirements under the new rules. Some of these dates have changed due to COVID-19. Organizations should check with HHS for the most current deadlines.

Compliance date	Requirement	Covered parties
May 1, 2020	ONC Rule: Information blocking all elements of electronic health information (EHI) in Cures Act	Healthcare providers, health IT developers of certified health IT, health information networks

November 2, 2020	ONC Rule: Information blocking (EHI United States Core Data for Interoperability data elements)	Healthcare providers, health IT developers of certified health IT, health information networks
November 2, 2020	ONC Rule: API requirements	Certified API developers with API technology certified to the criteria in 45 C.F.R. § 170.315(g)(7), 170.315(g)(8), or 170.315(g)(9)
November 2, 2020	CMS Rule: Condition of participation notice requirements (real-time patient event notifications)	Acute care hospitals, psychiatric hospitals, and critical access hospitals
January 1, 2021	CMS Rule: Patient access and provider directory APIs	CMS-regulated payers
January 1, 2022	CMS Rule: Patient-requested payer-to-payer data exchange	CMS-regulated payers
May 2, 2022	ONC Rule: All API information sources technology certified to the ONC Rules' new criterion under 45 C.F.R. § 170.315(g)(10)	Certified API developers previously certified to the criterion in 45 C.F.R. § 170.315(g)(8)

Table 1: The original compliance dates for requirements under the new rules

The cost associated with implementing the new rules is not trivial. HHS estimates it will cost organizations billions of dollars to implement and maintain the required APIs and data exchanges. The risks associated with implementing the APIs are high. It is quite likely that developers and IT administrators will make mistakes. It is also inevitable that hackers will go after these APIs. Together, these threats will cost organizations millions more as a result of data breaches.

Are these projected costs so high as to justify not going forward with the new requirements? Those calling the shots in the federal government, and particularly at HHS, do not think so. They are probably right if the new rules deliver us to the hoped-for destination of improved care at a reduced cost. If, however, these new rules don't achieve that goal, then the industry will be left to wonder where to turn next or whether we are searching for a destination that might not exist.

Takeaways

- This May, the U.S. Department of Health & Human Services published two final rules targeted at improving interoperability and patient access to health information.
- When first proposed, the rules met with controversy, particularly over the implications for the security and

privacy of protected health information.

- The security and privacy of electronic protected health information within an organization's environment or passing over the internet to a third-party app is still the responsibility of the organization for HIPAA compliance purposes.
- The risks associated with implementing necessary application programming interfaces are high and should be carefully considered.
- If an organization determines through HIPAA risk analysis that the exchange of information with a particular app is too risky, it may deny access.

1 "Health IT Legislation," Office of the National Coordinator for Health Information Technology, last reviewed May 19, 2020, https://bit.ly/3kBfVn3.
2 "Health IT Regulation Resources," Office of the National Coordinator for Health Information Technology, last reviewed February 10, 2019, https://bit.ly/31NW7nN.
3 "Data and Program Reports," CMS, last modified July 28, 2020, https://go.cms.gov/2POFtyN.
4 Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers, 86 Fed. Reg. 25,510 (May 1, 2020) .
5 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 86 Fed. Reg. 25,642 (May 1, 2020) .
6 HHS, "HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data," news release, March 9, 2020, http://bit.ly/38GvFxK.
7 sandy, "A History of EHR Through the Years," Electronic Health Records, ICANotes, April 16, 2019, https://bit.ly/3h8hWFb.
8 Health Insurance Portability and Accountability Act Pub. L. 104-191, 110 Stat. 1936 (1996).
9 Luke Gale, "HIPAA at 20: Looking back at two decades of patient privacy protections," Healthcare Dive, April 30, 2016, https://bit.ly/2CoPdgc.
10 45 C.F.R. §§ 160, 164(a)(e) .
11 45 C.F.R. §§ 160, 164(a)(c) .
12 45 C.F.R. § 160 (c), (d), (e) .
13 American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).
14 HITECH Act, Pub. L. No. 111-5, § 13,001, 123 Stat. 226 (2009).
15 Evan Sweeney, "Community Health Systems Facing EHR Meaningful Use investigation," Fierce Healthcare, August 8, 2018, https://bit.ly/31Yi17W.
16 45 C.F.R. §§ 164.400–414 .
17 42 U.S.C. § 18001 et seq.
18 "SMART Health IT Projects," Boston Children's Hospital Computational Health Informatics Program, last accessed August 11, 2020, https://bit.ly/3af8ixE.
19 "What Is SMART?" Boston Children's Hospital Computational Health Informatics Program, last accessed August 11, 2020, https://bit.ly/31XcgaL.
20 "SMART Health IT Projects," Boston Children's Hospital Computational Health Informatics Program.
21 JASON, *A Robust Health Data Infrastructure*, Agency for Healthcare Research and Quality report No. 14-0041-EF, April 2014, https://bit.ly/31LjRsu.
22 Covington Digital Health Team, "JASON Task Force Issues Final Report," *Covington Digital Health* (blog), Covington & Burling, October 30, 2014, https://bit.ly/3kxY14u.

23 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).
24 21st Century Cures Act § 4003(a), 130 Stat. 1165.
25 21st Century Cures Act § 4004, 130 Stat. 1178.
26 Executive Order 13813 of October 12, 2017 Promoting Healthcare Choice and Competition Across the United States, 82 Fed. Reg. 48,385 (Oct. 17, 2017) .
27 CMS, "Trump Administration Announces MyHealthEData Initiative to Put Patients at the Center of the US Healthcare System," news release, March 6, 2018, https://go.cms.gov/30M6WHy.
28 Joseph Kim, "CMS announces MyHealthEData Initiative and Medicare Blue Button 2.0," MedicineandTechnology.com, March 7, 2018, https://bit.ly/3afQCSJ.
29 "Introduction," Public Health and Promoting Interoperability Programs (formerly, known as Electronic Health Records Meaningful Use), Centers for Disease Control and Prevention, last reviewed September 9, 2019, https://bit.ly/2PJVGFp.
30 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 86 Fed. Reg. 25,642 .
31 Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers, 86 Fed. Reg. 25,510 .
32 Nondiscrimination in Health and Health Education Programs or Activities, Delegation of Authority, 85 Fed. Reg. 37,160, 37, 164 (June 19, 2020) .
33 "United States Core Data for Interoperability (USCDI)," Office of the National Coordinator for Health Information Technology, last accessed August 11, 2020, https://bit.ly/2DHFO3K.