COSMOS
Navigate the Compliance Universe

Compliance Today - March 2019
Compliance 101: Why Meaningful Use is still meaningful

By Gerry Blass and Krystyna H. Monticello, Esq.

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, NJ.

Krystyna H. Monticello (kmonticello@oscislaw.com) is a healthcare attorney at Attorneys at Oscislawski LLC in Princeton, NJ.

- linkedin.com/in/gerry-blass-917a482
- linkedin.com/in/krystyna-monticello-41759614

Is Meaningful Use still relevant today? Since its inception in 2010, the program has evolved to reflect industry-wide uptake in electronic health record (EHR) adoption, technology advances, and close alignment with alternative payment models such as the Quality Payment Program, including the Merit-based Incentive Payment System (MIPS) established under the Medicare Access and CHIP Reauthorization Act (MACRA).

Although no longer officially called "Meaningful Use," the program is still an essential component of any healthcare organization's pursuit of high-quality, standardized care and the secure dissemination of patient information.

What was the original intent of Meaningful Use?

Meaningful Use was written into the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the 2009 American Reinvestment and Recovery Act, to underscore and promote the need for use of interoperable EHRs. The program, originally known as the Medicare and Medicaid EHR Incentive Program, was based on five pillars of health outcomes policy priorities:

1. Improve quality, safety, and efficiency, and reduce health disparities
2. Engage patients and families in their health
3. Improve care coordination
4. Improve population and public health
5. Ensure adequate privacy and security protection for personal health information[1]

At the time, many smaller healthcare organizations—small facilities, systems, and physician practices—were still using paper records and charts. And although larger healthcare organizations may have been using EHR platforms, those platforms were not standardized. Legacy systems in place almost ten years ago lacked the ability to capture information in a standardized way and could not transmit that information easily. With disparate data, the healthcare industry was not set up to advance the five pillars set forth by the Centers for Medicare & Medicaid Services (CMS).

Standardized, electronic data capture in certified EHR technology (CEHRT) was a means towards advancing and

better managing population health, recognizing trends, and improving the quality of care for patients in a fragmented delivery model. Achieving those objectives was not possible with paper-based records.

Meaningful Use adoption was originally broken into three stages, aimed at progressively advancing adoption of EHRs and the standardization needed to achieve the five pillars. To encourage participation, CMS offered incentive payments to providers who could demonstrate that they were participating in each stage and using CEHRT.[2]

Stage 1: Data capture and sharing

The purpose of the first stage was to create standardization, and increase habitual input and sharing of data electronically. For example, physicians typically were not users of an EHR system. Rather, nurses would enter information into the EHR, after it was dictated, ordered, or handwritten by a physician. One of the goals of Stage 1 was for physicians and other clinicians to enter that data directly into the EHR using a computerized provider order entry (CPOE) system.

Stage 2: Advanced clinical processes

The criteria here encouraged the use of the EHR for continuous quality improvement at the point of care and the exchange of information in the most structured format possible.[3] For example, thresholds increased for several measures (e.g., from one clinical decision support intervention to five), and measures that were optional in Stage 1 become mandatory in Stage 2, such as the provision of summaries of care for patient transitions/referrals and medication reconciliation.

Stage 3: Improved outcomes

Stage 3 aimed to focus on improved outcomes through interoperability and better coordination of care and delivery, and it also required adoption of a more advanced CEHRT that was subject to different certification requirements. However, because of significant concerns from the provider and CEHRT communities in meeting CMS's goals for Stage 3, a "Modified Stage 2" was implemented by CMS for 2015 through 2017 to better position providers to transition to Stage 3. Topped-out and redundant measures were removed, reporting burdens were reduced, and measures and objectives were redesigned by CMS. Although more advanced Stage 3 measures were adopted by CMS, these were subsequently amended again by CMS in April of 2018 as a result of its rebrand of the Meaningful Use program.

How has Meaningful Use evolved?

Nearly seven years after Meaningful Use was put in place, most healthcare organizations and providers are using EHRs. By 2016, more than 95% of hospitals eligible for the Medicare and Medicaid EHR Incentive Program had achieved meaningful use of certified health IT.[4] A successful rollout of the original stages meant that the program needed rethinking from a strategic and progressive standpoint.

In April 2018, CMS announced its intention to overhaul Meaningful Use. CMS recognized that the program needed to change to reflect how providers actually deliver care and the advances made in technology over the past few years. CMS renamed the program Promoting Interoperability (PI)[5] and outlined the objectives of the new program:

- Make it more flexible and less burdensome,

- Emphasize interoperability through measures that require the exchange of health information between providers and patients, and
- Incentivize providers to make it easier for patients to obtain their medical records electronically.[6]

In addition to these changes, meaningful use continues to be one of four components of MIPS under the Promoting Interoperability performance category (formerly Advancing Care Information).[7]

With a new name and new objectives also come new measures and reporting criteria. The original five pillars of health outcomes still hold true, but the measures of the new program focus on two main areas: interoperability and patient access. Additionally, many of the previous measures where providers consistently performed well have been phased out, making reporting less of an administrative burden. Further, the incentive for hospitals to participate has shifted from incentive payments to penalty avoidance.

In August 2018, the final rule for Promoting Interoperability was adopted, along with performance-based measurement criteria. Building upon the MIPS performance-based model, rather than the previous stage-based measures, hospitals demonstrate compliance with Promoting Interoperability through a new and more flexible point-based system, a break from CMS's prior pass/fail approach. CMS does not currently mandate improvement in low-scoring areas, but providers should expect that future regulations will enforce overall improvement.

CMS has indicated that it will continue new rulemaking in the future. As providers improve and incrementally achieve the objectives for Promoting Interoperability, CMS will likely amend requirements to prevent stagnation and further advance program goals.

Privacy and security protection of ePHI

At its inception, meaningful use was intended partly to incentivize providers to document and store electronically protected health information (ePHI) data in an EHR. However, it also needed a provision to protect that electronic data—hence, the fifth pillar to ensure adequate privacy and security protection for personal health information.[8]

HIPAA was already in place at that point, enacted in 1996 and enforced by the U.S. Department of Health and Human Services (HHS).[9] HIPAA, with its Privacy Rule and Security Rule issued in 2002 and 2003, respectively, set a baseline for how providers should protect and secure ePHI. The advent of Meaningful Use in 2009 didn't change the requirements under HIPAA, but the combination of the two emphasized the need for providers to start paying more attention to HIPAA and how to protect patient data as they adopted CEHRT.[10]

To have been eligible to receive any incentives from Meaningful Use, or to avoid penalties in the future, providers must ensure privacy and security controls. In earlier stages, one of the Meaningful Use objectives required the provider to protect ePHI created or maintained by their CEHRT through implementation of appropriate technical capabilities. The provider needed to demonstrate that it had done so by conducting a security risk analysis, also known as a security risk assessment, as required under the HIPAA Security Rule at 45 CFR 164.308(a)(1), and by implementing security upgrades and correcting identified security deficiencies as necessary.

Although the security risk assessment is no longer a stand-alone objective under the program's new moniker of Promoting Interoperability, providers must still perform a security risk assessment to be considered a meaningful user and qualify to demonstrate promoting interoperability. Because privacy and security—also required under HIPAA—are still fundamental for the use of CEHRT, the assessment portion is retained in the program.

Ultimately, Meaningful Use was, and continues to be, a powerful ally of HIPAA, helping to enforce compliance with the Security Rule, and reframing it as a long-term strategy for protection of electronic PHI in ever-advancing technology. As technology, patient care, and data use evolve and become more connected, the more vulnerable they become. Even as it evolves, meaningful use continues to offer positive motivation for providers to develop long-term focus on the privacy and security of data and technology.

What is the role of security and compliance officers?

Because of HIPAA, security and compliance officers are focused on security and risk compliance and controls, and the adoption and maintenance of cybersecurity frameworks, such as those from the National Institute of Standards and Technology (NIST) and the Health Information Trust Alliance (HITRUST). Although Meaningful Use is not the primary driver of security and privacy controls, it certainly does aid in the adoption of these controls.

Now, under Promoting Interoperability, healthcare leaders should focus on the concept of secure connectivity and accessibility. In the effort to connect data across care disciplines, account for the Internet of Things (IoT), protect the connectivity of medical devices, and provide easy access to patient information, the fact remains that security is paramount. This is no easy task, considering how quickly the industry moves and how savvy hackers are when trying to access protected information.

Now more than ever, healthcare organizations should have a chief information security officer (CISO) who can lead a security and compliance team and strategically manage the adoption and maintenance of security frameworks, along with the Promoting Interoperability Program. This team should be responsible for ensuring there are policies and controls that:

- Reflect a comprehensive and robust cybersecurity infrastructure;
- Align business and organizational practices with security frameworks;
- Dictate circumstances and technical controls under which individuals, including outside community physicians, can have access to information; and
- Ensure appropriate security controls are in place regardless of how the data is shared—whether through an application programming interface (API), encrypted email, or portal.

Top considerations

Although meaningful use has changed and shifted, there remains a focus on the health information exchange and patient access measures required to demonstrate promoting interoperability. Because of the privacy and security concerns these present to organizations, providers must allocate proper attention and resources to security and privacy. Consideration should be given to the following when adopting and maintaining security and privacy controls at their organizations:

- **Assess past performance** on measures from prior reporting years. Under the new program structure, providers are positioned to build upon an established foundation and understand improvements that can be made on familiar measures.
- **Prioritize the provider-to-patient exchange,** where information is made available to and shared with the patient. As a key goal of CMS, patient care information must be made accessible by providers. This will have the highest performance impact for providers who want to demonstrate promoting interoperability.

- **Keep in mind that this program is not static.** CMS has listened and responded to provider concerns from the beginning. If challenges are encountered, bring those to the attention of advocacy organizations such as the College of Healthcare Information Management Executives (CHIME) to engage CMS in the evolution of the program.
- **Encourage healthcare leaders to shift their thinking** about privacy and security. Privacy and security are not, and should not be considered, secondary to advances in technology and interoperability. Rather, privacy and security are truly foundational to the five pillars of meaningful use.
- **Allocate the proper resources**—such as human, technical, and monetary—to support privacy and security efforts. This becomes even more important as the industry embraces collaborative patient care. It's no longer just about an individual facility's internal silo of data. There are now national and global considerations, increasing the burden on providers to make information more accessible.

By refocusing its objectives, the Meaningful Use program, now known as Promoting Interoperability, has renewed relevance for today's healthcare environment. The program better reflects the more widely accepted use of EHRs, considers that multiple providers caring for the same patient need shared access to information, and recognizes the importance of diligent security as technology and interoperability evolve.

This article is intended for general informational purposes only. It is not intended as legal advice.

Takeaways

- Meaningful use has evolved to address changes in technology adoption and patient care.
- Providers must understand new guidelines to demonstrate Promoting Interoperability (PI).
- The Health Insurance Portability and Accountability Act (HIPAA) and meaningful use work together to encourage privacy and security controls.
- Security and compliance leaders should have a renewed focus on security of connected data.
- Building a security and privacy infrastructure to support current and future needs is critical.

1 Centers for Disease Control and Prevention (CDC), Meaningful Use Introduction. https://bit.ly/2nVpErl
2 Idem
3 Centers for Medicare & Medicaid Services (CMS), Promoting Interoperability (PI). https://go.cms.gov/1QkewLP
4 Office of the National Coordinator for Health Information Technology, Health IT Dashboard. https://bit.ly/2hF7ydy
5 Ibid, Ref #3
6 Healthcare Informatics, "BREAKING: CMS to Rebrand Meaningful Use Program with New Emphasis on Interoperability, Burden Reduction" April 28, 2018. https://bit.ly/2rcVUZZ
7 HealthIT.gov, Advancing Care Information Reporting. https://bit.ly/2sqVz61
8 Ibid, Ref #1
9 HIPAA Journal, "When Was HIPAA Enacted?" March 9, 2018. https://bit.ly/2VRz1sN
10 Healthcare IT News, "How HIPAA final rule and meaningful use could drive data security" January 21, 2013. https://bit.ly/2AOz3IM