Implementing a strategic approach to interoperability for health plans and healthcare providers

The Interoperability and Patient Access final rule

bakertilly
now, for tomorrow

In today's frequently evolving healthcare regulatory landscape, health plans and healthcare providers are met with a constant need to adjust their operations and strategies for managing the health information and data of their patients.

With the intent to give patients the ability to more easily and securely access their own health information and data at no cost, whether from a government health plan or a healthcare provider, the Centers for Medicare & Medicaid Services (CMS) issued its Interoperability and Patient Access final rule (CMS-9115-F). The rule, finalized in March 2020, also requires the adoption of a standards-based data format to drive health information data exchange across industry stakeholders and further innovation in healthcare. In the first half of 2021, some of the first provisions contained within this rule are now passed the enforcement deadlines published by CMS.

As health plans and healthcare providers look to either become or maintain compliance with the Interoperability and Patient Access final rule, organizations have a unique opportunity to maximize their return on investment (ROI) by developing a robust long-term strategy for the use of the assets required to achieve interoperability compliance. This strategy should include a road map that considers use cases for interoperability assets beyond compliance, the development of a detailed work plan with resources that can execute against the plan and an assessment to identify the right technology solution for an organization.

Interoperability goals

Relationships among patients, healthcare providers and health plans are complex. In addition, over time a patient's treatment history likely lives within disparate provider and health plan systems and data repositories. Because of these and other factors, the intent of the Interoperability and Patient Access final rule is to give patients easier and more secure access to their own health information at no cost. This also allows that information, controlled by the patient, to be shared with those healthcare providers and health plans who the patient decides are essential stakeholders in the management of their healthcare.

In addition, with the implementation of the Interoperability and Patient Access final rule, the focus switches to putting the patient at the center of the healthcare ecosystem, making their care and diagnostic history more readily available to them. The Interoperability and Patient Access final rule also allows patients to use third-party applications of their choosing as a way to consolidate their health information from different health plans and providers.

Goals of the Interoperability and Patient Access final rule (CMS-9115-F)

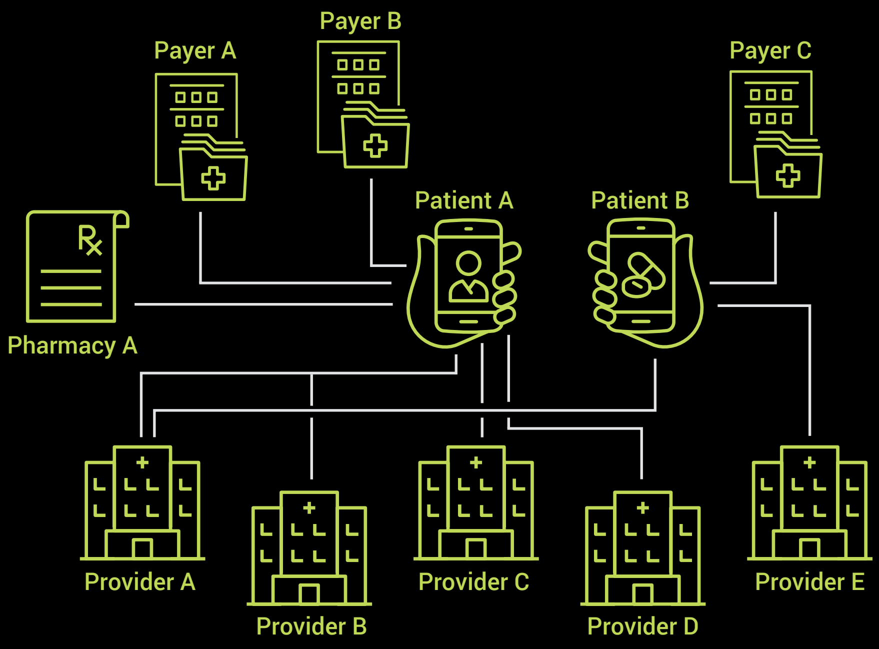
- Give patients the ability to easily and securely access their own health information at no cost
- Implement a standards-based data format that can drive data exchange and innovation in healthcare
- Mandate data sharing between providers, health plans and members to facilitate informed care decisions and improved long-term care outcomes

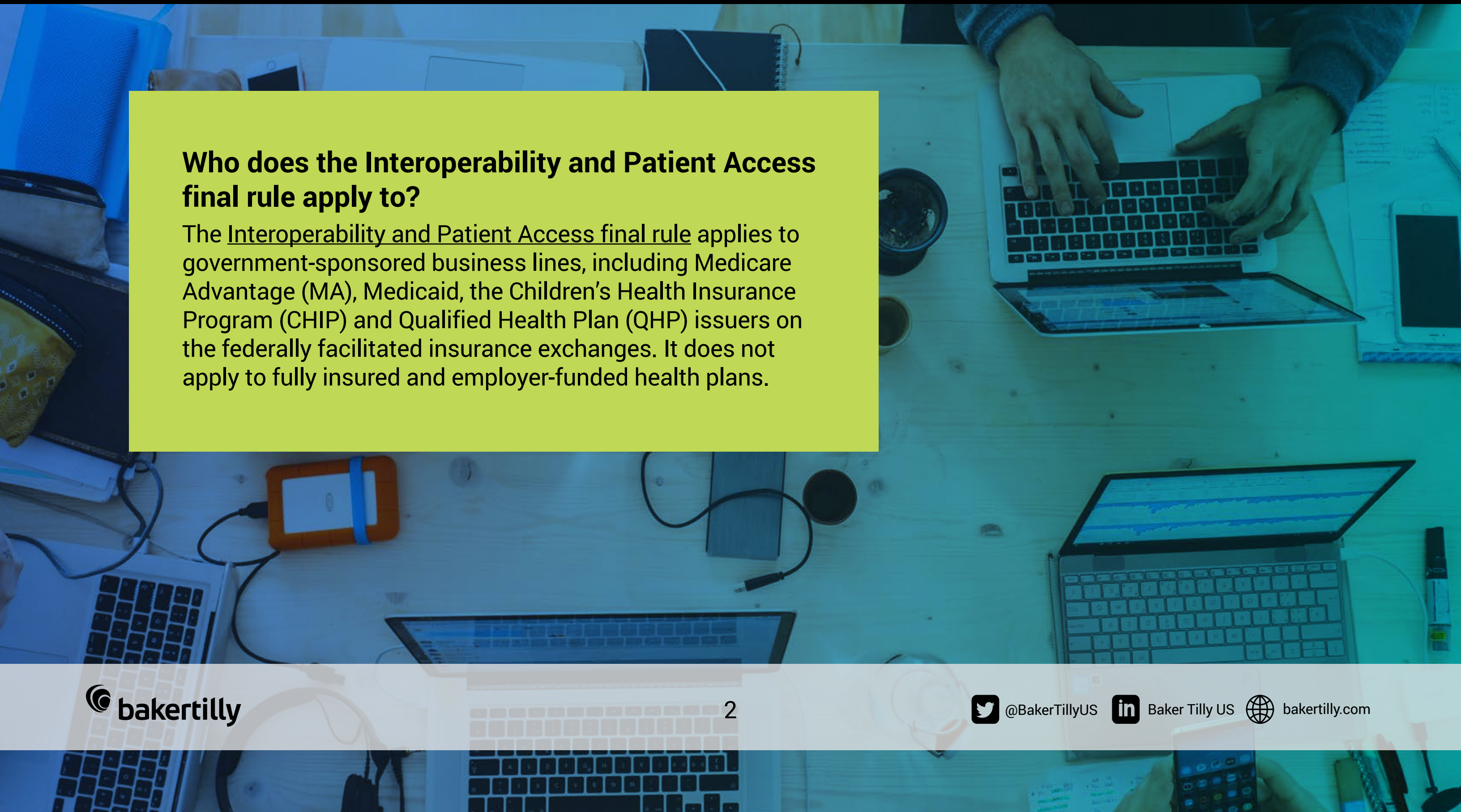
Applicable for:

- Medicare Advantage (MA)
- Medicaid
- Children's Health Insurance Program (CHIP)
- Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs)

Not applicable for:

- Fully insured
- Employer funded





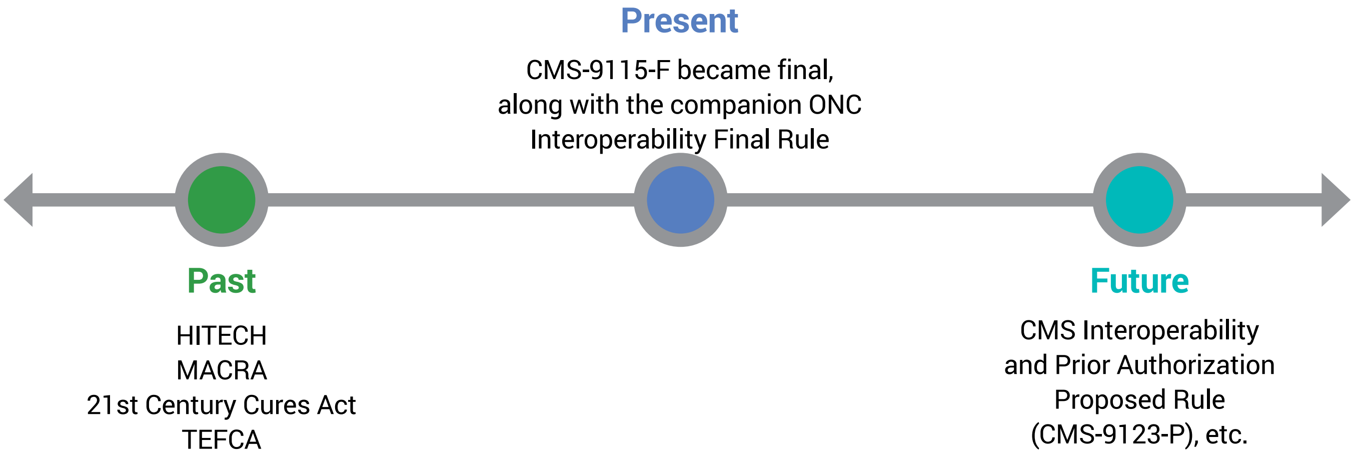
Who does the Interoperability and Patient Access final rule apply to?

The Interoperability and Patient Access final rule applies to government-sponsored business lines, including Medicare Advantage (MA), Medicaid, the Children's Health Insurance Program (CHIP) and Qualified Health Plan (QHP) issuers on the federally facilitated insurance exchanges. It does not apply to fully insured and employer-funded health plans.

A history of interoperability

Interoperability has been the subject of numerous federal laws and regulations since 2004 when the Office of the National Coordinator for Health Information Technology (ONC), within the Department of Health and Human Services (HHS), was first created. In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, promoted the adoption and meaningful use of electronic health records (EHRs). Subsequent initiatives such as the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA), the 21st Century Cures Act of 2016, and the Trusted Exchange Framework and Common Agreement (TEFCA), which was released in 2018, have continued to encourage interoperability between member health plans and healthcare providers.

In today's healthcare landscape, interoperability is being emphasized more than ever before. With the Interoperability and Patient Access final rule finalized in March 2020, along with the companion ONC interoperability final rule, both health plans and healthcare providers face sustained pressure to achieve timely compliance. Furthermore, the industry is showing little sign of slowing down as additional proposed rules were recently introduced, including the Interoperability and Prior Authorization Rule (CMS-9123-P), which builds on the foundation of the Interoperability and Patient Access final rule (CMS-9115-F).



Present

CMS-9115-F became final,
along with the companion ONC
Interoperability Final Rule

Past

HITECH
MACRA
21st Century Cures Act
TEFCA

Future

CMS Interoperability
and Prior Authorization
Proposed Rule
(CMS-9123-P), etc.

The components of the Interoperability and Patient Access final rule

Interoperability and Patient Access final rule comprises seven components:

1. Public reporting of providers that do not have digital contact information included in the National Plan and Provider Enumeration System (NPPES)
2. Public reporting of providers that submit a "no" response to any of the three prevention of information blocking statements for the Merit-based Incentive Payment System (MIPS) under Medicare
3. Requirement that hospitals with EHRs alert providers about their patients' admission, discharge or transfer (ADT) information or when they receive any services within the emergency department, in an effort to improve care coordination
4. Creation of patient access application programming interface (API) to make claims and encounter information available to a member via a third-party application of their choice
5. Creation of provider directory API to make provider directory information publicly available
6. Requirement that health plans facilitate providing a patient's clinical data at their request (payer-to-payer data exchange), allowing a patient to take their health information with them as they move from one health plan to another over time
7. Improving the experience for people dually eligible for Medicare and Medicaid by increasing the frequency of federal-state data exchanges to daily from monthly

Health plan specific policy overview

1. **Patient access API**

   The policy enforcement date: July 1, 2021

   The patient access API requirement focuses on establishing an API that allows health plan members to access their health information via a third-party application of their choice. At a high level, this data includes claims and encounters; provider remittance and enrollee cost sharing; and clinical data, including lab results, if maintained by the health plan.

   Medicare Part C plans must also share formularies and preferred drug lists as well as covered drugs in any tiered formulary structure or utilization management procedures with their members. In addition, patient access APIs must meet specific technical standards for data format (Fast Healthcare Interoperability Resources® (FHIR) Release 4.0.1), and the authorization (SMART IG/OAuth 2.0) and authentication (OpenID Connect) of third-party applications.

   Specific to timing for health plans, this information must be provided to the member no later than one business day after a claim is adjudicated or an encounter received. Plans also will be required to provide available patient history from 2016 onward. To comply with the patient access API requirement, health plans must consider all the data sources they will need to manage to send a comprehensive history to a member.

2. **Provider directory API**

   The policy enforcement date: July 1, 2021

   Health plans also are required to make provider directory information available via a publicly accessible API. This information must include provider names, network status, address, phone numbers and specialties. Medicare Part B plans also must include pharmacy names, type of pharmacy and contact information as well. The information must be available within 30 days of receipt of any new data or changes to a plan's existing directory. Further, this data must comply with applicable FHIR 4.0.1 technical standards.

3. **Payer-to-payer data exchange**

   The policy enforcement date: Jan. 1, 2022

   The third component of the law addresses the exchange of data between health plans. This component requires that, at a current or former member's request, payers send clinical information, including lab results if applicable, that they maintain (primarily United States Core Data for Interoperability (USCDI) data) with a date of service from 2016 onward, to any other health plan identified by the current member or former member.

Healthcare provider policy brief

4. **Information blocking**

   The policy enforcement date: April 5, 2021

   The ONC previously highlighted that information blocking — controlling EHRs in ways that limit their availability and use — is a serious problem and recommended Congress prohibit it and provide penalties and enforcement mechanisms to deter the practice. The final rule's guidance on information blocking applies to all eligible clinicians, hospitals and critical access hospitals participating in the Medicare fee-for-service Promoting Interoperability Program. The guidance also requires healthcare providers to demonstrate they did not knowingly or willfully take action to limit or restrict compatibility or interoperability with their EHR systems, and that they have acted in good faith to use their systems to support the appropriate exchange and use of health information.

   The HHS Office of Inspector General (OIG) proposed a definition of a violation to clarify how it would determine which information-blocking practices would result in civil monetary penalty (CMP) fines as well as the basis for imposing CMPs and calculating the amount of the penalty.

5. **Digital contact information**

   The policy enforcement date: late 2020

   The digital contact information referred to in the final rule relates to the provider's secure digital end point (e.g., direct address), which is similar to a regular email address, but includes additional security measures to ensure messages are only accessible to the intended recipient in order to keep the information confidential and secure. The heart of this policy is encouraging and enabling providers to utilize the secure contact information to facilitate healthcare coordination for patients.

6. **ADT event notifications**

   The policy enforcement date: May 1, 2021

   The ADT notification requirement applies to hospitals, psychiatric hospitals and critical access hospitals. These facilities are required to have a fully operational notification system that is compliant with state and federal regulations to securely exchange that information. At a minimum, providers must include the patient name, the treating practitioner and the sending institution within this system; optional data could include diagnosis details, depending on state laws.

   Additionally, hospitals are required to physically send a notification from the approved system to the providers that the patient has given them as the providers responsible for their care. In instances where a hospital cannot identify a primary care practitioner or provider for a patient, CMS does not expect that an ADT notification would be sent. However, hospitals are required to demonstrate they have made a reasonable effort to ensure notifications are sent and received where applicable. Noncompliant providers risk CMS denial of payment and other sanctions.

State agency policy brief

7. **Federal-state data exchanges**

   The policy enforcement date: April 1, 2022

   The final requirement within the Interoperability and Patient Access final rule pertains to state Medicaid agencies and focuses on improving the experience for people dually eligible for Medicare and Medicaid. In this final requirement, state Medicaid agencies will be required to increase the frequency of federal-state data exchanges (including the state buy-in file and "MMA files") to daily from monthly. This requirement aims to ensure Medicaid beneficiaries receive access to appropriate services when they need them.

Getting started

Technical standards

Healthcare providers and health plans can utilize a number of resources to comply with the Interoperability and Patient Access final rule. The rule requires the use of four main technical standards:

1. **HL7 FHIR 4.0.1®:** This is the latest version of the FHIR resources, which define content and structure of core health information; this can be used to build standard applications and data feeds. The adoption of FHIR enables health plans, healthcare providers and third-party app developers to use the same data standards, thus enabling data interoperability.
2. **USCDI:** This is a standardized set of health data classes and constituent data elements used for nationwide interoperable health information exchange, and is required for use by the Interoperability and Patient Access final rule to further support consistency of data sharing formats.
3. **SMART IG/OAuth 2.0:** This focuses on the authorization components of the API rules and provides reliable, secure authorization for a variety of application architectures using that standard. It also enables third-party apps to request authorization to access a FHIR resource and retrieve that resource back.
4. **OpenID Connect:** This is the authentication layer built on top of the OAuth 2.0 protocol that enables clients to verify end-user identity and obtain basic profile information from claims data in an interoperable manner.

Implementation resources

CMS has resources to help healthcare providers and health plans implement technical standards as well as best practices for providers, health plans and app developers working to tackle these requirements, including Patient Privacy and Security Resources and Best Practices for Payers and App Developers. Da Vinci also developed a number of implementation guides as part of its effort to accelerate the adoption of FHIR resources. Lastly, CARIN Alliance is an HL7 FHIR accelerator program, which has built an implementation guide for Blue Button capabilities issued by CMS. Blue Button is a standards-based API that delivers Medicare Part A, B, and D data for more than 60 million Medicare beneficiaries.

Sample market solutions

An organization will need to consider its options for implementing interoperability technology solutions: develop in-house, leverage a PaaS vendor for part or most of the solution, or collaborate with an existing application vendor. A number of private sector solutions in the healthcare community can be evaluated as part of an organization's overall interoperability strategy. These include Azure API for FHIR and FHIR Works on AWS. Further, the CARIN Alliance also manages My Health Application, which lists health applications that have digitally connected to providers, hospitals and health plans around the U.S. As appropriate, an organization should conduct due diligence on any solution under consideration to find the right fit.

Conclusion

Healthcare organizations should not just use the interoperability rule as an exercise to achieve and maintain compliance with new regulations, but should seize it as an opportunity to maximize their implementation ROI through proactive and strategic planning. By thinking beyond solely achieving compliance, organizations can unlock additional potential and benefits of implementing a more deliberate approach to interoperability, including the expansion to such use cases as:

- Identifying and targeting patient care gaps for quality measures, risk adjustments and STARS improvements
- Driving care management programs to facilitate more proactive care that reduces costs, improves care outcomes and facilitates value-based care (VBC)
- Refreshing consumer communication records and tailoring future outreach
- Reinforcing ongoing efforts focused on provider directory accuracy
- Promoting additional efforts to enable timely information and insight sharing between health plans and providers

Successful compliance with the Interoperability and Patient Access final rule requires more than a technology solution. It will also involve operational readiness, customer engagement and compliance teams working in harmony. In addition, the data required to help a health plan or healthcare provider be in compliance with interoperability requirements is often the same data that will support an organization's strategic value points. As an organization executes its work plan across different stakeholder groups and different technology stacks, whether they are source systems, data assets or new FHIR infrastructure, bringing all those teams together to work on interoperability compliance can also breed success throughout the organization.

What organizations should do now

As health plans and healthcare providers look at resources to implement a successful interoperability strategy, organizations should immediately do a few things:

Build a comprehensive strategy that considers business enablement and operational readiness in addition to technology

Define the downstream use cases for interoperability assets that can be integrated into a long-term strategy road map

Develop a robust work plan that considers the different resources and stakeholder groups that need to participate for success

Align technical data strategy with business strategy to ensure long-term success

Proactively engage consumers in interoperability compliance and education to influence overall member experience

Acquire resources from appropriate sources, and commit the resources to execute an integrated delivery plan to completion

How to get the most out of your interoperability journey

Rally around available resources and innovation communities: CMS best practice guides, leverage existing industry resources such as CARIN Alliance, and HL7 FHIR Da Vinci guides.

Consider your organization's options for implementing your interoperability technology solutions: develop in-house, leverage a PaaS vendor for part or most of solution, or collaborate with existing application vendor partners. As appropriate, conduct due diligence on solutions under consideration to find the right fit.

Take advantage of the opportunity to maximize ROI by investing in a long-term strategy to define additional use cases for interoperability assets built to achieve compliance.

Build and manage a robust work plan that considers all aspects of your implementation, with dedicated resources responsible for its success.

Regularly monitor the healthcare landscape for evolving guidance and policy from ONC and CMS, and prepare for additional interoperability requirements in the future (e.g., CMS-9123-P, etc.).

Connect with us

@BakerTillyUS

Baker Tilly US

bakertilly.com

About Baker Tilly

Baker Tilly US, LLP (Baker Tilly) is a leading advisory, tax and assurance firm, providing clients a genuine coast-to-coast and global advantage with critical mass and top-notch talent in major regions of the U.S. and in many of the world's leading financial centers – New York, London, San Francisco, Los Angeles and Chicago. Baker Tilly is an independent member of Baker Tilly International, a worldwide network of independent accounting and business advisory firms in 148 territories. The combined revenue of independent member firms is $4 billion.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments. Baker Tilly US, LLP, trading as Baker Tilly, is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

© 2021 Baker Tilly US, LLP