Clearwater

Whitepaper

Protecting Patient Health Information: The MIPS Requirement for Security Risk Analysis

Table of Contents

Introduction

In 2015, the U.S. Congress passed a new law, the Medicare Access and CHIP Reauthorization Act (MACRA), which changed how Medicare Part B clinicians manage their fee schedules through a newly created Quality Payment Program (QPP).

Prior to MACRA, Medicare payment increases were established based on what was then the Sustainable Growth Rate (SGR). According to QPP, as providers increased service utilization, the SGR had a direct impact on the physician fee schedule, primarily noting that continuing to use SGR would have resulted in decreased reimbursement fees.

As a result, MACRA established the QPP that not only repealed SGR, but also changed how Medicare rewards providers for service value instead of volume. It shifted Medicare reimbursement increases away from fee-for-service (volume-based) reimbursement to value-based reimbursement and established the Merit Based Incentive Payments System (MIPS) and a bonus payment program for clinicians who take part in Advanced Alternative Payment Models (Advanced APMs).

Essentially, the changes mean that now clinicians are rewarded for better performance, which results in higher payment increases, and worse performance results in lower increases or decreases.

All Medicare Part B clinicians who meet established requirements (discussed in detail below) must participate in the MIPS program. Others who do not may opt-in for eligibility but are not required to report to MIPS.

Understanding MIPS

MIPS is a part of the QPP and the successor program to the Physician Quality Reporting system (PQRs) and meaningful use (MU) of Electronic Health Records, later rebranded as the Promoting Interoperability program.

QPP's goals are to:

- Improve beneficiary outcomes
- Increase adoption of Advanced APMs
- Reduce clinician burden

- Maximize participation
- Improve data sharing and information sharing
- Ensure operational excellence in program implementation
- Deliver IT systems capabilities that meet user needs

Clinicians can choose between two QPP participation tracks: MIPS or Advanced APMs. While these programs are broadly similar, they have distinct differences:

- If you participate in MIPS, you will earn a performance-based payment adjustment.
- If you participate in an Advanced APM, you may earn a Medicare incentive payment for sufficiently participating in an innovative payment model.

What are MIPS requirements?

Participation in MIPS is fairly straightforward.

Inclusion is based on annual Medicare volume thresholds:

- Bill: More than $90,000 for Part B covered professional services, and
- See: More than 200 Part B patients, and
- Provide: More than 200 covered professional services to Part B patients

Participants can report to MIPS as groups or individuals. Clinicians that do not meet these volume thresholds can still submit MIPS data voluntarily, which will be available on the Physician Compare website. Visit https://qpp.cms.gov/participation-lookup to determine your MIPS participation status.

Reporting frameworks

There are three reporting frameworks to choose from:

- Traditional MIPS
  - Performance measured across four areas: quality, improvement activities, promoting interoperability, and cost
  - Risk analysis requirement is within promoting interoperability
  - Each performance area is scored separately and weighted differently to contribute to your overall score.
    - Promoting Interoperability: 25% of your overall score
    - Cost: 30%
    - Quality: 30%
    - Improvement Activities: 15%

- MIPS APM (APP)
  - Performance is measured across three areas: quality, improvement activities, and promoting interoperability
  - Promoting Interoperability: 30% of overall score
  - Quality: 55%
  - Cost: 30%
  - Improvement Activities: 15%
- MIPS Value-Based Pathways (MVP)
  - Aligns performance with different specialties or conditions
  - Incorporates Promoting Interoperability measures and a set of administrative claims-based quality measures focused on population health to reduce reporting burden
  - Promoting Interoperability is "foundational"
  - Cost and quality measures align with specialty

The Promoting Interoperability set of requirements is in all three reporting frameworks, and as such, so is the requirement to conduct a risk analysis.

Promoting interoperability

Promoting Interoperability, or the program formerly known as Meaningful Use, is a critical piece of MIPS participation under all reporting frameworks.

Reporting must cover several measures within four objective areas, plus three yes/no attestation objectives. A security risk analysis is one of the yes/no attestation objectives.

The performance period is a minimum of any continuous 90-day period within the calendar year. Eligible clinicians must submit data collected for all required measures from each objective (unless claiming an applicable exclusion) for the same 90 continuous days (or more) during 2022.

Participants must also submit "yes" to:

- Prevention of Information Blocking
- Protect Patient Health Information (including Security Risk Analysis)
- High Priority Practices SAFER Guides

Failure to report on required attestation results in an automatic 0 score for the Promoting Interoperability performance category. Participants must also use 2015 certified electronic health record (EHR) technology (CEHRT) on the first day of the Promoting Interoperability performance period for the full performance period.

Recent changes

There have been some adjustments made for MIPS for the 2022 performance year, including:

- COVID-19
  - Neutral payment adjustments in 2022 for many participants
  - General flexibilities available to count toward complex patient bonuses and cost performance categories
  - Any physicians participating as individuals are automatically enrolled in Extreme and Uncontrollable Circumstances (EUC) exceptions
- SAFER Guides
  - New objective highlighting patient safety
  - Must attest to conducting a self-assessment about how EHR use can impact patient safety

Requirements for risk analysis

Protecting ePHI remains a constant objective, so the requirement for conducting risk analysis persists unchanged under MIPS. Unfortunately, many healthcare organizations still struggle with conducting a compliant risk analysis.

A quick reminder:

It's important to note how you're currently documenting these variables and aspects within the requirement to conduct a risk analysis. If you're not capturing some of these details in your documentation, determine how you can do so now because all of these pieces play a role in your participation.

HIPAA risk analysis

HIPAA directs covered entities and business associates to: "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."
§164.308(a)(1)(ii)(A):

This means you should ensure you have policies and procedures to address the purpose and scope of risk analysis, workforce member roles and responsibilities, management involvement in risk analysis, how frequently you will review and update the risk analysis, and evidence of conducting the risk analysis.

Your HIPAA risk analysis should include:

- A defined scope that identifies all systems that create, transmit, maintain, or transmit ePHI
- Details of identified threats and vulnerabilities
- Assessment of current security measures
- Impact and likelihood analysis
- Risk ratings
- Periodic reviews and updates

MIPS requirement for risk analysis

MIPS requires participants to: "Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by CEHRT in accordance with requirements in 45 CFR164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process."

This refers to the security management standard of the HIPAA Security Rule where there are four implementation specifications. Risk analysis is the first of these implementation specifications, followed by risk management, sanction policy information, and system activity.

A review of the risk analysis is included in this language, but other specifications are also important. The goal is to address ePHI security created or maintained by your EHR, including implementation of security updates and corrections as part of your risk management process. Completing an accurate and thorough risk analysis is required to receive a Promoting Interoperability score greater than 0. Completing the risk analysis requirement is all or nothing; if the requirement is not fully satisfied, then no credit is given.

Satisfying MIPS risk analysis requirement

MIPS does not add to the scope of a HIPAA risk analysis, but it includes additional administrative tasks and specifics, especially around analysis timing.

To meet your MIPS requirements, note:

- For a risk analysis to count toward a MIPS performance period, it must be unique to the performance period.
- Since MIPS performance is measured annually, your risk analysis should be conducted or updated annually. The analysis can occur outside of the reporting period but must be conducted within the same calendar year as the reporting period.
- The analysis scope must include all ePHI in your organization.
- The analysis must be conducted when the 2015 CEHRT is implemented.
- Risk analysis must be conducted upon installation or upgrade to a new EHR system, and a review must be conducted covering each performance period.
- Any security updates and identified deficiencies should be included in the clinician's risk management process and implemented or corrected as dictated by that process.
- At a minimum, you must be able to show a plan to correct or mitigate deficiencies and that you're taking steps to implement that plan. Your corrective action plan should cover the attributes of a risk analysis required by HIPAA, such as roles, responsibilities, risk ratings, frequency of updates, management involvement, and timing.

Remember that you are accountable for what your internal process dictates, so your risk management process should be realistic and set attainable goals.

SAFER guides

The safety assurance factors for EHR resilience (Safer Guides) focus on patient safety. They were added to the physician fee schedule for 2022. These guides are designed to help healthcare organizations conduct self-assessments to optimize the safe use of EHRs in the following areas:

Foundational

1. **High priority practices (this applies to MIPS Promoting Interoperability)**
2. **Organizational responsibilities**

Infrastructure

3. **Contingency planning**
4. **System conffguration**
5. **System interfaces**

Clinical Process

6. **Patient identiffcation**
7. **Computerized provider order entry with decision support**
8. **Test results reporting and follow-up**
9. **Clinician communication**

Each guide begins with a checklist of recommended practices. These are intended to help clinicians deal with safety concerns related to the continuously changing technology and regulatory landscape. They are not intended for legal and compliance purposes, and implementing a recommended practice does not mean it's HIPAA compliant. The safer guides are for informational purposes only.

Meeting MIPS SAFER guides requirements

To gain a Promoting Interoperability score greater than 0, you must attest to the High Priority Practices SAFER Guide attestation measure: "Conduct an annual self-assessment of the High Priority Practices SAFER Guide during the calendar year in which the performance period occurs. MIPS eligible clinicians are expected to fill out the checklist and practice worksheet at the beginning of the guide."

This is required but unscored. That means it's all or nothing, just like the risk analysis. The High Priority Practices Safer Guide directs participants to identify high-risk, and high-priority recommended safety practices to optimize the safety and use of an EHR.

MIPS directs participants to conduct an annual self-assessment of the High Priority Practices Safer Guide. The self-assessment questionnaire consists of 18 questions to rate as Fully, Partially, or Not Implemented. You can answer each question with the aid of a corresponding group worksheet. You can attest to "yes" or "no." Just be sure to attest; otherwise, your score is 0.

MIPS audits

A MIPS audit can be triggered immediately after attestation (pre-payment) or years after receiving payment (post-payment).

What happens if you're faced with a MIPS audit?

- Engagement Letter
  - Providers selected for an audit will receive an initial request (engagement) letter from the auditor, Figliozzi and Co.
  - Individual participants and participating hospitals receive different engagement letters.
- Information Request List
  - A list will be attached to the engagement letter outlining all required documentation from your EHR system to support your attestation measures and responses.
  - Monitor your email address on file to quickly respond to additional requests.
- Documentation Submission
  - The engagement letter will outline methods and a deadline for documentation submission, which can be submitted electronically via a secure web portal or by mailing the requested information to the auditor.
- Review Process
  - Once the auditor receives the documentation, the review process begins. The auditor will review the submitted documentation at their home office location.

- An on-site review of your provider location could follow.
- The auditor may request additional information during or after this initial review process.

- Post-Audit
  - The auditor will send an audit determination letter to inform the provider whether the provider was successful or failed the audit.
  - In the event of a failed audit, the letter will outline failed measures and describe the appeal process.
  - Failed audits will result in positive payment adjustments not being issued or payments being recouped. Based on the audit, if providers are found not to meet the threshold for a positive payment adjustment, payment amounts will be recouped in the case of post-payment audits, or payment will not be made in the case of prepayment audits.
  - Payment recruitment will be communicated via a separate demand letter and will include all information regarding the repayment process.

MIPS audit documentation

Failure to complete an accurate and thorough risk analysis is a leading cause of failing Promoting Interoperability audits.

Risk analysis documentation

Your Promoting Interoperability score will be reduced to 0 if you can't meet the protect patient health information objective, so be thorough in your documentation process. Consider the following in your records of each risk analysis and response:

- Can you produce a report documenting procedures performed during the analysis and its results?
- Does your report show that is was produced for that provider's system?
- Does your documentation clearly indicate the name of the practice, organization, or provider, and CEHRT system?
- Is it dated during the calendar year and when CEHRT was implemented?
- Can you show both current and prior risk analyses and results?
- How can you demonstrate your risk analysis process policies and procedures are being followed?

- How is documentation from the prior year's risk analysis available to those responsible for the risk analysis process? How can you demonstrate periodic review and updates are occurring?
- Auditors can look at multiple years of risk analysis documentation (up to six years before the date of audit notification) to determine if the risks identified are being addressed in an ongoing risk management process. Generally, they want to see progress if they find evidence of risks not being addressed according to a risk management process. Will your records meet that expectation?

Risk response documentation

Risk response is sometimes overlooked by MIPS participants, but it is an essential part of completing requirements and supporting attestation for an audit. Here is what you should have ready:

- Documentation demonstrating security measures implemented to reduce risks as a result of the current risk analysis or assessment
- Demonstrate efforts used to manage risks from the previous calendar year.
- Describe assignment of roles, functions, and a timeline to address risks as they're uncovered (i.e., corrective action plan)
- Policies and procedures of the risk management process
- Policies and procedures related to the implementation of risk management for the prior six years of the date of audit notification
- Documentation demonstrating the current and ongoing risks reviewed and updated
- Documentation from the previous year demonstrating implementation of the risk management process, how it is available to those responsible for the risk management process, and that evidence the documentation is periodically reviewed and updated

You should think about how you maintain evidence of risk responses, noting you could face an audit six years after the fact. Can your systems generate historical evidence going that far back? Do you have to capture the evidence at each point to reflect what was in place during your performance period?

Finally, keep in mind that, ultimately, auditors have broad discretion on how to interpret and decide on the evidence they gather. To make the process go as smoothly as possible for everyone involved, it is in your best interest to be precise, responsive, and cooperative.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact