HEALTH PROGRAM

Under the leadership of former Senate Majority Leaders Tom Daschle and Bill Frist, M.D., the Bipartisan Policy Center’s Health Program develops bipartisan policy recommendations that will improve health care, lower costs, and enhance coverage and delivery. The program focuses on coverage and access to care, delivery system reform, cost containment, chronic and long-term care, and rural and behavioral health.

ACKNOWLEDGMENTS

BPC would like to thank the Peterson Center on Healthcare for its generous support of BPC’s Digital Health work. BPC acknowledges former staff member Sabah Bhatnagar for her contributions to this work.

DISCLAIMER

The findings and recommendations expressed herein do not necessarily represent the views or opinions of BPC’s founders, its funders, or its board of directors.
Table of Contents

4 EXECUTIVE SUMMARY

7 OVERVIEW

16 POLICY RECOMMENDATIONS
16 Ensuring Appropriate Service Coverage
21 Improving Equity
26 Ensuring Data Security and Privacy

30 CONCLUSION

34 GLOSSARY OF ACRONYMS

35 ENDNOTES
Executive Summary

Digital health advocates believe remote monitoring—the use of digital technologies to collect and relay patient data to health care professionals—has the potential to transform disease management, health outcomes, and patient care, especially for individuals with multiple chronic conditions who lack convenient access to providers. Medicare, most state Medicaid agencies, and many private health insurance plans cover remote monitoring services.

For the purposes of this report, we define remote monitoring as an umbrella term for remote physiologic monitoring (RPM) and remote therapeutic monitoring (RTM). RPM refers to the monitoring of physiologic data—such as weight, blood glucose, or blood pressure—while RTM refers to the monitoring of patients’ self-reported nonphysiologic data, such as pain levels or medication adherence. Currently, the Centers for Medicare & Medicaid Services (CMS) limits RTM reimbursement to cases involving the respiratory system, musculoskeletal system, and cognitive behavioral therapy.

Although the percentage of patients using RPM remains relatively low (594 monthly claims per 100,000 Medicare enrollees in 2021), the use of RPM increased among Medicare beneficiaries more than sixfold from 2018-2021.\(^1\) In part, this increase was due to CMS’ expanded coverage rules during the COVID-19 public health emergency. Thirty-four state Medicaid programs covered RPM services as of March 2023; however, many Medicaid programs restrict RPM use in some way.\(^2\) RTM uptake has also steadily increased since its introduction in 2022, yet billing and documentation requirements can hinder its widespread adoption.\(^3,4\)

The evidence base on remote monitoring, particularly for RPM tools, is growing. Yet some policy experts cite a lack of robust evidence on the optimal use of remote monitoring, including its duration and target patient groups. In the absence of such evidence, these experts question whether we are effectively “rightsizing” the use of these services. Underuse could limit access to beneficial care, while overuse could unnecessarily increase spending in federal health care programs. Additionally, providers cite the need for tools—such as generative artificial intelligence (AI)—to manage streams of data, otherwise the volume of patient-generated information can become overwhelming and unmanageable.

Over the past year, the Bipartisan Policy Center undertook an extensive effort to develop evidence-based, federal policy recommendations for the appropriate use and coverage of remote monitoring services. BPC assessed patients’ access to and use of remote monitoring technologies and their impact on health outcomes and cost. We conducted a series of interviews and hosted a private roundtable with health policy experts, federal officials, technology leaders,
medical providers, payers, consumers, and academics to gain insight into the opportunities and challenges regarding remote monitoring.

This report looks broadly at ways to improve the use of remote monitoring services, ensure equitable access to these services across populations, and enhance data security and privacy standards. Now is the time for payers and providers to refine their approach and maximize appropriate adoption for patients who stand to benefit from remote monitoring.

**POLICY RECOMMENDATIONS**

**A. Ensuring Appropriate Service Coverage**

Today, qualified health care providers have wide latitude regarding the provision and billing of remote monitoring services. But more research is needed on how to optimize the use of remote monitoring, including by disease state and patient group. Clinical guidelines are critical for the provision of these services.

- CMS should work with medical specialty societies to evaluate the evidence and determine appropriate coverage mechanisms to guide the optimal use of remote monitoring, including for which patients and over what duration. This work could include collaborating with Medicare Administrative Contractors (MACs) or issuing National Coverage Determinations (NCDs).

- As more evidence emerges about the appropriate use of remote monitoring devices, the secretary of HHS should use the department’s existing authority to recommend a diverse set of billing codes so providers have more options for the time they spend on the data and the number of minimum days of data required.

- CMS should further clarify current policies regarding appropriate coding and billing of RPM and RTM. It should also require providers not enrolled in risk-based models to attest to medical necessity for patients’ continued use of remote monitoring—at a frequency deemed appropriate by the HHS secretary and based on condition-specific clinical guidelines.

- CMS should work with the American Medical Association (AMA) and relevant medical specialty societies to develop additional RTM billing codes to allow for use cases beyond musculoskeletal, respiratory, and cognitive behavioral therapy—as the evidence supports.

- Congress should request the Medicare Payment Advisory Commission (MedPAC) to report on the impact of remote monitoring on clinical outcomes and cost by disease state, and on any new billing thresholds or code durations, at least every three years.
B. Improving Equity

To ensure high quality and the equitable provision of remote monitoring services—including for those individuals with poor disease control, poor medication adherence, and/or difficulty maintaining regular care—providers and patients need access to comprehensive information on device performance. Additionally, safety-net providers need flexible reimbursement policies.

• Congress should direct the Food and Drug Administration (FDA) to promulgate a rule clarifying that remote monitoring device labels should include performance characteristics to support the safe and effective use of these devices.

• The FDA should develop an easy-to-reference list or notation—similar to the AI device list—for consumers to search online for legally marketed remote monitoring devices.

• CMS should clarify that it allows store-and-forward technologies for billing codes related to remote monitoring and provide guidance on how often patients should transmit data to providers. This will allow flexibility for patients or providers who do not have access to broadband to benefit from and deliver remote monitoring services.

• Congress should clarify and refine anti-kickback safe harbors related to providing devices to patients. This is especially important for safety-net providers who often lack the resources to cover startup costs for a remote monitoring program.

C. Ensuring Data Security and Privacy

Patient privacy and security concerns have increased with the rise of digital technologies and have affected the uptake of remote monitoring by both patients and providers.

• The HHS Office of Civil Rights should identify whether existing privacy policies adequately protect personal health information gathered, stored, and transmitted through remote monitoring. If gaps remain, the office should assess whether it has the authority to close that gap and, if it does not, Congress should do so.

• HHS should study the use of cybersecurity safe harbor laws to determine their effectiveness.

• HHS, through the Office of the National Coordinator for Health Information Technology, should continue to ensure the existence of appropriate data standards so that remote monitoring devices can be interoperable with electronic health record (EHR) systems.
Overview

Digital health is a rapidly evolving landscape that encompasses an array of devices, software, and delivery modes. Over the past year and a half, BPC homed in on remote monitoring devices and evaluated their impact on equitable access to care, as well as on patient outcomes and cost effectiveness. This report synthesizes findings from the available published literature and from in-depth interviews with health policy experts, federal officials, technology leaders, vendors, medical providers, payers, consumers, and academics.

DEFINING REMOTE PHYSIOLOGIC AND REMOTE THERAPEUTIC MONITORING

For the purposes of this report, we define remote monitoring as an umbrella term for remote physiologic monitoring (RPM) and remote therapeutic monitoring (RTM). The main difference between RPM and RTM is the type of data collected. RPM covers only physiologic data—such as heart rate and blood pressure—while RTM monitors nonphysiologic data, such as pain levels and medication adherence. For reimbursement, RPM requires the device to automatically record patient data; RTM allows patients’ self-reported data. Additionally, the American Medical Association’s Resource-Based Relative Value Scale Update Committee designed RTM codes to be used primarily by physical therapists and other providers who cannot bill for emergency and management services, while it designed RPM codes for physicians. For a comprehensive overview of the differences between RPM and RTM, see Appendix A.
CMS introduced the RPM Current Procedural Terminology (CPT) codes in the calendar year 2020 CMS Physician Fee Schedule, which included codes for setting up equipment, monitoring the data, and interacting with patients to review the data. CMS does not restrict RPM codes to specific conditions. These codes assist with the monitoring of a wide variety of conditions, including diabetes, high blood pressure, heart conditions, and sleep apnea.

CMS introduced RTM CPT codes a few years later in the calendar year 2022 CMS Physician Fee Schedule. Although the RTM codes are structured similarly to the RPM codes, they cover a much smaller range of cases and are reimbursed only for “respiratory system status, musculoskeletal system status, therapy adherence, and therapy response” use cases. AMA refined these codes to include cognitive behavioral therapy, although current utilization is low. Unlike RPM, which has a general billing code and does not restrict coverage to specific conditions, the AMA developed the RTM codes with the intention to expand them and account for other body systems as technology develops. For examples of both RPM and RTM devices, see Figure 1.

**Figure 1. Examples of RPM and RTM Devices**

<table>
<thead>
<tr>
<th>RPM device examples</th>
<th>RTM device examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>continuous glucose monitors</td>
<td>virtual physical therapy</td>
</tr>
<tr>
<td>blood pressure monitors</td>
<td>pain management software</td>
</tr>
<tr>
<td>heart monitors</td>
<td>digital knee</td>
</tr>
</tbody>
</table>

**EVIDENCE-BASED USE CASES**

Research is evolving regarding the impact of remote monitoring on patient outcomes and cost. RPM’s evidence base is stronger than its newer counterpart, RTM. The following examples, while not exhaustive, highlight the potential for remote monitoring to improve patient outcomes and realize cost savings.

**Type 1 Diabetes:** Many health care providers believe continuous glucose monitoring should be a part of the standard treatment for Type 1 diabetes. One systematic literature review found that continuous glucose monitoring is associated with improved HbA1c levels, reduced hospitalizations, and reduced instances of diabetic ketoacidosis. Yet studies that evaluated the cost effects yielded mixed results, making it difficult to provide a savings estimate.
Heart Failure: Numerous systematic reviews demonstrate the clinical benefits of RPM for treating heart failure. One Department of Veterans Affairs (VA) study using RPM and telehealth exemplifies the potential for improved patient outcomes and cost savings. In this study, the VA provided 38 participants with in-home devices to monitor vital signs; nurses called patients weekly regarding changes detected by the device and pharmacists adjusted prescriptions accordingly. Researchers estimated the intervention prevented 26 emergency room visits over five months. The outcome demonstrated the potential for significant cost savings, since the VA serves over 300,000 veterans with chronic heart failure and the average cost of a single heart failure hospital admission is $23,077.

Hypertension: Evidence suggests that remote blood pressure monitoring can improve health outcomes and save money. One meta-analysis concluded that patients using RPM to monitor blood pressure at home had significantly reduced in-office readings. Another study of women with hypertensive disorders in pregnancy found that telehealth combined with remote blood pressure monitoring was associated with a reduction in hospital readmissions. One modeling study estimated that home blood pressure monitoring could save nearly $7,800 in health care costs per person over 20 years, with the greatest potential for savings among racial minorities and people living in rural areas.

Wound Care: A study of wound therapy RTM—not currently covered by Medicare—demonstrates the potential for cost savings. The treatment combines portable negative pressure wound therapy—which uses suction to promote wound healing—with an integrated RTM device that transmits data for monitoring by virtual specialists. RTM was associated with overall cost savings of $3,753 per patient. Another study on negative pressure wound therapy found that RTM with regular adherence calls was associated with increased therapy adherence in 73% of patients, leading to greater reductions in wound volume and surface area.

Coverage and Utilization Across Payers

Medicare, most state Medicaid agencies, and many private insurance agencies cover remote monitoring. Medicaid and private insurance offer broader coverage for RPM than for RTM, possibly due to the more recent introduction of the RTM CPT codes.

Medicare

The Medicare program covers both RPM and RTM. Medicare reimburses providers for device supply, device setup, time spent analyzing patient data, and
time spent interacting with patients to adjust treatment. For a list of remote monitoring CPT codes and their reimbursement rates, see Appendix B.

Before the COVID-19 public health emergency and the addition of RTM codes, CMS set a variety of requirements for RPM reimbursement, including but not limited to:

- Patients must have a pre-existing relationship with the provider.
- Providers must be eligible to furnish evaluation and management services.
- Services must monitor acute care or chronic conditions.
- The device must meet the definition of a medical device, as defined by the FDA.
- The device must electronically collect and automatically upload data to a secure location for interpretation by the billing provider.
- The device must collect data for at least 16 out of 30 days.

During the COVID public health emergency, Medicare permitted providers to bill for RPM services furnished to new patients and reduced the 16-day reporting requirement to two days. Once the public health emergency ended, Medicare reinstated the pre-pandemic rules, requiring established patient-provider relationships and 16 days of reporting.

In 2022, CMS introduced RTM payment policies for the monitoring of respiratory system status, musculoskeletal system status, therapy adherence, and therapy response. Although most requirements mirror those of RPM, the following distinctions exist:

- A wider array of providers—including physical therapists, occupational therapists, and physiatrists—can use RTM codes, whereas only physicians, nurse practitioners, and physician assistants eligible to bill for evaluation and management services can use RPM.
- Patients can self-report RTM data, while RPM data requires automatic uploading.
- Providers cannot bill both RPM and RTM for the same patient in a single month.

Medicare spending on remote monitoring is increasing rapidly, likely due to a combination of increased usage, widespread adoption of telehealth during the pandemic, and the establishment of permanent RPM and RTM codes. An

____________________

\[\text{In the 2024 Physician Fee Schedule, CMS clarifies that this 16-day requirement does not apply to treatment codes. See: https://www.federalregister.gov/public-inspection/2023-24184/medicare-and-medicaid-programs-calendar-year-2024-payment-policies-under-the-physician-fee-schedule. Also see Appendix B for more details.} \]

\[\text{Physiatrists are physicians who specialize in physical medicine and rehabilitation. See: https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/physiatrist} \]
analysis of RPM spending for Medicare enrollees showed an increase from $5.5 million in 2019 to $101 million in 2021.\textsuperscript{32} Despite the large increase, this growth still represents only 594 monthly claims per 100,000 enrollees. A separate analysis found that a small group of primary care providers has largely driven the increase in RPM spending. RTM uptake has also steadily increased since its recent introduction, yet billing and documentation requirements can hinder widespread adoption.\textsuperscript{33,34}

Despite increasing usage, remote monitoring tools are likely underutilized in some areas. Experts we spoke with indicated that access to remote monitoring is more a function of where a patient lives and who their provider is, rather than their medical condition and if they would benefit from remote monitoring. A 2022 survey found that only one-quarter of medical practices offered remote monitoring.\textsuperscript{35,36}

Lawmakers have expressed concerns about the misuse of remote monitoring codes in Medicare. In the 2015 Medicare Reauthorization Act, Congress directed the Government Accountability Office to complete a report on the use of telehealth and RPM in the private insurance market.\textsuperscript{37} The report called attention to the absence of originating site codes in billing records, a potential indication of improper billing.\textsuperscript{38} A report on remote monitoring by the HHS Office of Inspector General, scheduled for release in 2024, will provide new information on the evolution of remote monitoring; the characteristics of Medicare patients and providers using these services; and the potential for fraud, waste, and abuse.\textsuperscript{39}

**Medicaid**

Currently, 37 state Medicaid programs reimburse for RPM; requirements for coverage vary significantly by state, however.\textsuperscript{40} Many state Medicaid programs that offer remote monitoring reimbursement have restrictions associated with its use. Common restrictions include limiting reimbursement to only home health agencies, specifying which conditions qualify for monitoring, and setting criteria for acceptable monitoring devices and data collection.\textsuperscript{41} Medicaid coverage of RTM has much less clarity than RPM: West Virginia released a bulletin in 2022 announcing the new RTM codes, but it is unclear whether other states have released similar guidance.\textsuperscript{42}

**Private Payers**

A variety of major private insurers cover RPM, including Humana, Aetna, Cigna, UnitedHealthcare, and some branches of BlueCross BlueShield.\textsuperscript{43} Several follow CMS guidelines when determining which RPM devices and services to cover, while other private plans offer different coverage.\textsuperscript{44} Private insurers are less likely to cover RTM. Cigna, for example, issued a medical coverage policy in May 2023 explaining its decision to cover RPM services but not RTM, citing RTM’s lack of peer-reviewed evidence.\textsuperscript{45} On the other hand, Anthem Blue Cross Blue Shield began covering RTM in 2023.\textsuperscript{46} An August 2023 AMA report
on commercial payer coverage of digital technologies notes that the lack of coverage alignment between payers and the inconsistent levels of transparency on coding guidelines, can limit the uptake of these technologies.\textsuperscript{37}

**FDA Regulation**

CMS payment policies require that remote monitoring devices meet the FDA’s definition of a medical device. Section 201(h) of the Food, Drug, and Cosmetic Act states that devices must either be recognized in the official National Formulary; intended for use in the diagnosis, cure, mitigation, treatment, or prevention of a disease or condition; or “intended to affect the structure or any function of the body.”\textsuperscript{38} The FDA considers software to be a medical device—termed Software as a Medical Device—if it meets this same definition.

To ensure safety and effectiveness, the FDA regulates remote monitoring medical devices and provides guidance to manufacturers on their design, testing, and labeling. Devices have three major pathways to market depending on their risk classification.\textsuperscript{48} High risk devices must go through premarket approval, a review process that requires results from clinical trials. Most moderate risk devices undergo premarket notification (510(k)) review, which often does not require clinical trials and focuses on establishing similarity to an already cleared device.\textsuperscript{50} Manufacturers must register and list low risk devices. Many available remote monitoring tools are classified as moderate risk; however, some could be high or low risk.

The FDA also requires device manufacturers to comply with post-market requirements, such as reporting adverse events, monitoring device performance, and adjusting the device or its labeling to address safety or effectiveness concerns.\textsuperscript{51}

The FDA has also taken steps in recent years to address Software as a Medical Device. In 2019, the agency proposed a regulatory framework for modifications to AI machine learning-based software as a medical device. The FDA introduced the concept of a predetermined change control plan (PCCP), which would allow for certain modifications to occur without the need for a renewed premarket review. The Food and Drug Omnibus Reform Act of 2022 added Section 515C to give the FDA express authority to accept PCCPs. The FDA has now begun to accept PCCPs and to establish standards for devices that rely on adaptive algorithms.\textsuperscript{52,53,54,55} The agency has also taken steps to harmonize its approach with the U.K. and Canadian health authorities.\textsuperscript{56}

However, the FDA provides limited and sometimes differing information on the performance of the devices, and there is no easy way to compare two similar devices. Researchers have raised concerns about the limits of the FDA’s regulatory authority over remote monitoring devices, including the agency’s ability to mitigate risks of fraudulent devices, ensure patient privacy, and address device safety and accuracy issues.\textsuperscript{57}
The FDA launched the Patient Monitoring and Control Program in 2021 to address regulatory science gaps, including:\(^\text{58}\)

- lack of clear guidelines on testing with patient monitoring datasets, which limits the utility of this type of least burdensome testing and often results in the collection of new data or a reanalysis of existing information;
- limited availability of test methods and comprehensive information required to enable medical devices and systems to communicate (i.e., interoperability); and,
- lack of a way to evaluate a product over numerous iterations, including updates to algorithms.

The Biden administration’s October 2023 Executive Order on AI calls on HHS to develop an AI assurance policy to evaluate and monitor AI-enabled health care tools.\(^\text{59}\) FDA oversight of medical devices is likely to be a part of this policy.

**EQUITY IMPLICATIONS**

Remote monitoring services have myriad health equity implications. Remote monitoring can expand access to health services for populations facing barriers to care, including people with mobility issues, residents of rural areas, individuals without access to transportation, and people with lower incomes.\(^\text{60,61,62,63}\) Individual companies and institutions tout the potential for remote monitoring to increase access to care.\(^\text{64,65}\)

However, without proactive measures, remote patient monitoring could perpetuate or even exacerbate pre-existing disparities in access to and quality of care.

Before 2024, safety-net providers faced unique financial barriers to starting and maintaining remote monitoring because they could not bill for these programs.\(^\text{66}\) CMS pays federally qualified health centers (FQHCs) and rural health clinics (RHCs) an all-inclusive rate for each patient visit, and providers cannot bill separately for most individual services.\(^\text{67}\) Healthcare Common Procedure Coding System code G0511 for general care management is one of the few separate billing options, and it covers services typically performed outside of face-to-face visits, such as chronic care management. In the 2024 Physician Fee Schedule, CMS finalized its proposal to include remote monitoring services in Healthcare Common Procedure Coding System code G0511 and allow safety-net providers to bill code G0511 multiple times per month.\(^\text{68}\) As such, safety-net providers can now receive separate reimbursement for RPM and RTM.

Broadband issues can inhibit patients’ use of remote monitoring services. Many Americans grapple with limited broadband, including 46 million individuals living in rural and frontier communities.\(^\text{69}\) A study comparing rural hospitals to their urban and suburban counterparts found that patients using rural remote
monitoring programs reported more concerns regarding privacy, ability to pay, and lack of strong cell service.\textsuperscript{76} Data show that the digital divide affects the use of health IT, despite the fact that the majority of Americans want access to digital health data.\textsuperscript{71,72}

Providers and older adults, non-native speakers, racial minorities, and individuals unfamiliar with digital tools might face unique barriers to adopting and reaping the benefits of remote monitoring services.\textsuperscript{73,74,75} Among these challenges are the algorithmic biases present in some medical devices. The following example illustrates this challenge and highlights the importance of centering equity considerations:

Providers utilizing remote monitoring note that the volume of patient-generated information can become unmanageable. Automation systems—including ones that incorporate AI—could help providers to manage streams of data by sending alerts when values are out of range and conducting additional analyses to inform disease management protocols.

Yet AI algorithms, reliant on vast amounts of data for training, can inadvertently exacerbate biases present in the data. Research has uncovered racial biases in medical devices, including ones used for remote monitoring.\textsuperscript{76} For example, pulse-oximeters consistently yield unreliable results for people of color, and AI tools that used data from these devices to guide treatment decisions during the pandemic may have exacerbated this existing bias.\textsuperscript{77,78,79} Any AI-integrated automation systems would need to include safeguards to protect against these and other risks.

As policymakers prepare for the future of remote monitoring, they will need to be mindful of these inequities to fully realize the benefits of remote monitoring.

\section*{DATA SECURITY AND PRIVACY}

The United States has no single overarching privacy law, and privacy regulations may not fully cover data from home-monitoring technologies.\textsuperscript{80}

Regulatory bodies have enforced the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Breach Notification Rule in actions against remote monitoring and digital health companies.\textsuperscript{81,82} HIPAA is the main health-related privacy statute, and it protects patient information when held by certain covered entities, including health providers, health insurers, and the business associates of those individuals or organizations.\textsuperscript{81,82} Yet HIPAA might not apply to user-generated data or data generated by remote monitoring devices before those data are sent to...
RPM device and software firms are unlikely to be business associates under the definition in 45 CFR 160.103. HIPAA might not appropriately protect information collected by telehealth companies because these companies typically connect patients with providers, rather than provide care themselves.

The Federal Trade Commission (FTC) enforces the prohibition of unfair or deceptive acts or practices and has promulgated the Health Breach Notification Rule, which requires a company to notify the public when it has had a data breach. The FTC recently began enforcing this rule, notably with a $1.5 million settlement with GoodRx. In June 2023, the commission published a Notice of Proposed Rulemaking regarding updates to the Health Breach Notification Rule. The proposed rule would add wellness products—such as sexual health, sleep, and diet apps—to the definition of health care services or supplies. It also requires third-party service providers to vendors of personal health records to provide notification to these vendors following the discovery of a breach.

There are numerous additional cybersecurity requirements and standards for health data. FDA-reviewed devices must adhere to a level of cybersecurity that provides reasonable assurance of security for users. The Consolidated Appropriations Act of 2023 granted the FDA authority to refuse to accept any premarket submission that did not meet its cybersecurity requirements, and in April 2023 the agency sent a letter to health care providers regarding cybersecurity vulnerabilities in a genetic sequencing device. There are also voluntary frameworks, such as the Health Information Trust Alliance common standards and the framework from the National Institute of Standards and Technology, as well as interoperability standards, such as the Fast Healthcare Interoperability Standards.

Yet cybersecurity gaps likely remain. Many legally marketed devices fall within the category of devices for which the FDA is exercising enforcement discretion, and they might not meet the FDA standards for cybersecurity. More than 70% of surveyed telehealth providers report using legacy operating systems, which can pose risks to security because they often cannot be patched or updated. Additionally, patients who are monitored or managed at home likely do not have the same privacy and cybersecurity safeguards as a hospital setting. Patients without cybersecurity safeguards might also spread malware to their providers.
Policy Recommendations

A. Service Coverage

CMS should work with medical specialty societies to evaluate the evidence and determine appropriate coverage mechanisms to guide the optimal use of remote monitoring, including for which patients and over what duration. This work could include collaborating with Medicare Administrative Contractors (MACs) or issuing National Coverage Determinations (NCDs).

Medicare providers have wide discretion to determine whether remote monitoring services are “reasonable and necessary” for their patients. Research shows significant differences in the use of remote monitoring technology for patients with similar diagnoses. Studies also do not show substantial targeting of the technology on people with more serious or poorly controlled diseases.

At the same time, remote monitoring CPT code requirements limit the extent to which providers can tailor their approach to service delivery by patient or condition. For example, some remote monitoring CPT codes require providers to interact with patients for a minimum of 20 minutes to receive reimbursement.

In 2023, the Patient Safety Network of the Agency for Healthcare Research and Quality released a report emphasizing the need for “robust processes and clear guidelines” to help providers identify appropriate patients and optimally use these services. The cost effectiveness of remote monitoring can vary by type of
service, diseases monitored, and the setting in which monitoring is occurring, according to the report.  

In February 2023, Medicare Administrative Contractors held a multijurisdictional Contractor Advisory Committee meeting to review the strength of the clinical evidence for RPM and RTM. Several experts voiced concerns about restricting coverage—such as through Local Coverage Determinations—while research is ongoing. Following this meeting, MACs decided not to develop Local Coverage Determinations for remote monitoring.  

CMS should continue to monitor the evidence and use its existing authorities to craft appropriate coverage mechanisms that guide the optimal use of remote monitoring tools. Based on the evidence, CMS could work with MACs to address local needs or issue NCDs to establish a uniform, nationwide approach. The coverage mechanisms should at minimum specify conditions, target populations, measure(s) to monitor, measurement frequency, and recommended measurement duration. They could also offer guidance on how frequently providers need to review the data. Some health conditions might require daily review of data, whereas others might only need review weekly or monthly.  

CMS should partner with medical specialty societies and other external experts through existing pathways, including the Medicare Evidence Development and Coverage Advisory Committee and the Agency for Healthcare Research and Quality Technology Assessments. CMS also references practice guidelines and compendia—such as those developed by the American Diabetes Association—when it makes national coverage determinations. For example, the agency covers cancer treatments included in practice guidelines. These existing pathways and processes will help to clarify the appropriate use of remote tools, both encouraging their use when there is evidence of benefit and discouraging their use when there is not.  

As more evidence emerges about the appropriate use of remote monitoring devices, the secretary of HHS should use the department's existing authority to recommend a diverse set of billing codes so providers have more options for the time they spend on the data and the number of minimum days of data required.  

To bill Medicare for remote monitoring devices, a provider must monitor a patient for at least 16 days of a 30-day period; to bill Medicare for treatment or data interpretation, a provider must spend at least 20 minutes of time on these services per month. During the COVID-19 public health emergency, Medicare reduced the 16 reporting days to two days; once the public health emergency ended, Medicare reinstated the pre-pandemic rules.  

The 16-day data collection and 20-minute interaction limits might not be appropriate for every clinical situation. For example, providers might only
need a few days of foot temperature data for diabetic patients at risk of developing foot ulcers. And a provider might find that less than 20 minutes of care management and interaction is sufficient for medication titration in certain conditions.

As more evidence becomes available about the best uses of remote monitoring devices, CMS should use its existing authority to create multiple billing thresholds so there are more options for the minimum days of data required and for the time a provider spends on treatment or interpreting data.

A bipartisan bill introduced in 2021 by Reps. Troy Balderson (R-OH) and Katie Porter (D-CA) would extend the lower two-day billing threshold until two years after the public health emergency and would require the HHS secretary to report on appropriate long-term billing thresholds.  

As evidence develops, RTM and RPM might be able to use the same CPT codes, and the nuances of provider time could be captured similarly for both technologies. Most stakeholders agree, however, that for now, the separation of the two is important to maintain.

**CMS should further clarify current policies regarding appropriate coding and billing of RPM and RTM. It should also require providers not enrolled in risk-based models to attest to medical necessity for patients’ continued use of remote monitoring—at a frequency deemed appropriate by the HHS secretary and based on condition-specific clinical guidelines.**

Providers’ use of remote monitoring billing codes varies widely—some use the codes for monitoring patient physiological data, others use remote monitoring data as an impetus to bring patients in for an office or virtual visit, while yet others do both simultaneously.

CMS has taken steps to clarify policies in recent years. In 2021, CMS said that the 20 minutes of intraservice work associated with the treatment codes for remote monitoring includes “a practitioner’s time engaged in interactive communication as well as time engaged in non-face-to-face care management services during a calendar month.” Additionally, the CMS **2023 Physician Fee Schedule** highlighted rules to protect against the double billing of codes for chronic pain management and remote monitoring, and the **2024 Physician Fee Schedule** clarified which specific remote monitoring codes must adhere to the 16-day data collection requirement.

CMS should provide further guidance to providers on how and when to use remote monitoring billing codes via one or more of the following regulatory and communications avenues:

* CMS could provide clarity through the Physician Fee Schedule, which lists the fees CMS pays providers for specific work.
• In the fiscal year 2023 omnibus, Congress directed CMS to share information with states on ways to leverage telehealth and remote monitoring to reach people experiencing homelessness. As part of this communication, CMS could include language about when to use remote monitoring codes and which codes should not be billed together.

• CMS could publish a bulletin or FAQ explaining the codes and when to use them. A bulletin is considered subregulatory guidance and provides the agency’s thinking on an issue.

• CMS could partner with providers’ professional societies and expert groups to provide continuing medical education on remote monitoring and include accurate information about billing. CMS could also provide non-continuing medical education courses online. If data emerge around billing confusion for any particular disease state, CMS could work with the specialty societies representing these providers to provide additional education.

• Last, and likely most easily, CMS could clarify billing requirements through communications channels, such as officials’ speeches or the CMS blog. Additionally, CMS should require providers not enrolled in risk-based models to attest to medical necessity for patients’ continued use of remote monitoring technology—at a frequency deemed appropriate by the HHS secretary and based on condition-specific clinical guidelines.

Today, providers qualified to bill for remote monitoring services have wide latitude to choose which patients receive remote monitoring services and for how long. Yet ongoing monitoring of controlled disease sometimes provides limited utility. For example, one study found that most hypertension medication adjustments occurred within the first four months of starting RPM. Beyond this period, the frequency of medication adjustment aligned with rates observed before RPM use.

In a fee-for-service reimbursement environment, providers can have strong incentive to increase the utilization of RPM, potentially beyond its period of clinical benefit. Third-party remote monitoring vendors could further incentivize uptake by reducing the costs for providers to scale their services, including by supplying monitoring devices and conducting patient onboarding.

To help ensure the appropriate use of remote monitoring, CMS should require providers to attest to the clinical necessity of a patient’s continued use of the services. Until clinical guidelines are established, attestations allow providers a relatively simple way to ensure they are thoughtful about monitoring usage and to curb ongoing remote monitoring applications that provide little to no clinical value. Numerous health programs, including some Medicaid programs, have successfully used provider attestation. They have also used attestation to address other Medicare requirements, such as interoperability. Similar requirements have worked to curb inappropriate antibiotic usage.
CMS should exempt providers participating in risk-based models from an attestation requirement. Value-based models already incentivize providers to adopt higher-value, cost-effective uses in their practices. CMS could also consider additional flexibility for providers participating in risk-based models, such as reconsidering restrictions that limit remote monitoring use to one provider per patient in a 30-day period, even when a patient uses more than one device. This restriction disproportionally affects Medicare beneficiaries with multiple chronic conditions who may need various specialists along with a primary care provider to manage their care.

Regardless of a formal attestation requirement, the authorizing provider should re-evaluate the necessity of the service regularly, at a frequency that aligns with clinical guidelines. This would verify that a patient’s data continues to be important to monitor and provides clinical value.

**CMS should work with the American Medical Association (AMA) and relevant medical specialty societies to develop additional RTM billing codes to allow for use cases beyond musculoskeletal, respiratory, and cognitive behavioral therapy—as the evidence supports.**

Currently, RTM billing codes exist only for three body systems: musculoskeletal, respiratory, and cognitive behavioral therapy. Industry and other stakeholders have requested that CMS develop a generic RTM device code, but it has not created one.

Before any expansion of RTM service codes, it is important to consider the implications on patient health outcomes and costs. Evidence-based tools may exist in the market today that are not related to musculoskeletal, respiratory, or cognitive behavioral therapy. For example, one manufacturer published data demonstrating positive outcomes and cost savings when patients use its wound care system. Yet providers cannot bill for this system because it does not fit in the existing allowable RTM categories.¹²⁸

Experts we talked to said that CMS’ current RTM coverage policies largely relate to which manufacturers were actively involved in submission processes. Limits on RTM codes might artificially constrict the market of available tools and have a chilling effect on innovation.

CMS should work with the AMA to evaluate the evidence base that could support additional RTM billing codes to allow for use beyond those cases currently available.

Sufficient evidence does not yet exist to support a recommendation consolidating remote physiologic and remote therapeutic monitoring into a single set of payment codes. However, it is important to note that in both cases, CMS is paying for the provider’s time reviewing the patient’s data. In the future,
MedPAC could review emerging data to recommend consolidation, or CMS could consider rulemaking on the matter.

**Congress should request the Medicare Payment Advisory Commission (MedPAC) to report on the impact of remote monitoring on clinical outcomes and cost by disease state, and on any new billing thresholds or code durations, at least every three years.**

The best-use cases for remote monitoring—based on disease, device, patient, time frame for monitoring, risk factors, and other parameters—are still unclear.

At a Medicare Administrative Contractor advisory meeting in early 2023, many attendees provided mixed evidence on the clinical effectiveness of remote monitoring. One attendee noted that any changes to coverage or reimbursement during the evidence-gathering phase could harm the uptake of remote monitoring. Another attendee conceded that “the widespread adoption and data generation on specific clinical applications for remote patient monitoring won’t really mature for another couple of years.” In May 2023, the contractors announced they would not be making changes to RPM coverage.

Further evidence will help Medicare determine the clinical utility of remote monitoring, including how often it informs clinical decisions and promotes positive patient outcomes. Congress should request that MedPAC gather and analyze the existing data on remote monitoring and report at least every three years on its findings. The MedPAC report should provide an analysis or meta-analysis of studies by disease state and include information about device type, patient characteristics, and length of monitoring.

### B. Improving Equity

**Congress should direct the FDA to promulgate a rule clarifying that remote monitoring device labels should include performance characteristics to support the safe and effective use of these devices.**

CMS reimbursement policies require that remote monitoring devices meet the definition of a legal device. Yet FDA-approved or -cleared devices do not always share sufficient performance information to allow providers and patients to understand the clinical utility of the data. And limited information on performance characteristics can make it difficult for patients to avoid counterfeit devices.

FDA-regulated devices, including remote monitoring devices, are not always accurate and do not consistently perform the same across demographic groups. For example, FDA-regulated blood pressure cuffs have produced inaccurate at-home readings, despite regulations requiring regular calibration. Research has also shown that pulse oximeters can be less
accurate on people with darker skin. This bias has prompted FDA advisory committee meetings and calls from state attorneys general for clearer labeling and rigorous device testing.

In 2018, the FDA published guidance for industry on reporting age, race, and ethnicity data for medical devices. However, it focused on devices for which there are clinical studies, and many devices do not undergo clinical trials before coming to market. In 2022, the FDA approved only 22 devices through the premarket approval process and more than 3,000 devices through the 510(k) pathway, the majority of which did not undergo clinical trials.

The FDA should support the safe and effective use of remote monitoring devices by promulgating a rule clarifying that device labels should include performance characteristics. Transparency is particularly important with monitoring devices increasingly incorporating automation systems and AI.

Performance characteristics should include, but not be limited to, the analytical performance of the device, the error rate, and the relevant population on which the device has been tested, and how it performs across races, ethnicities, and sexes. Information should also address performance drift by indicating the time frame over which devices “without the need for calibration” are accurate.

The In Vitro Diagnostics Rule—which mandates the disclosure of performance characteristics, opening instructions, and calibration procedures—offers a model for transparent device labeling.

The FDA should develop an easy to reference list or notation—similar to the AI device list—for consumers to search online for legally marketed remote monitoring devices.

The FDA operates a number of databases where the public can search for medical devices, but no single database is dedicated to remote patient monitoring devices. It can be difficult, as a result, to find accurate information about the status and proper utilization of these devices.

There are separate databases for each of the review mechanisms (de novo, 510k, premarket approval), a registration and listing database, and a general devices database. Remote monitoring devices can go through any of these mechanisms, and no centralized database compiles them at this time. An FDA webpage on emergency use authorizations for remote or wearable patient monitoring devices provided information about devices authorized for use during the COVID-19 public health emergency, when the FDA promulgated an enforcement discretion policy. Yet the site does not include any remote devices approved, cleared, or granted marketing authorization outside of the emergency use authorization process.

Relabeling by distributors might further complicate efforts to find information about a remote monitoring device. BPC found one such example of a program that distributed glucometers to help recipients control their blood glucose. The
specific glucometer does not appear in the FDA databases because the company, which is not the original manufacturer, relabeled the product. The agency often keeps this information as a trade secret. However, it is key to evaluating a device’s performance, and the FDA should make it public.

Ultimately, patients and providers have no simple way to find out whether a remote monitoring device is FDA cleared or approved. There is no list of cleared or approved remote monitoring devices and no denotation in the databases to easily find which devices are remote monitoring. As such, manufacturers may face difficulties complying with CMS requirements for FDA review, and patients and providers may not be able to locate accurate information about the status and proper utilization of their devices.

The FDA should create a list of legally marketed remote monitoring devices, as it does for artificial intelligence devices, although that list is not comprehensive. It could also create other ways to search for these products in its numerous databases or across the databases, including by labeling remote monitoring devices. Many legally marketed devices are not FDA reviewed due to enforcement discretion, so this list would be incomplete. Nonetheless, it would be a helpful resource.

CMS should clarify that it allows store-and-forward technologies for billing codes related to remote monitoring and provide guidance on how often patients should transmit data to providers. This would allow flexibility for patients or providers who do not have access to broadband to benefit from and deliver remote monitoring services.

Individuals living in areas without broadband technology face significant barriers in receiving remote monitoring services. Currently, about 42 million Americans lack access to broadband.

Remote monitoring devices transmit data through cellular or broadband. Cellular remote monitoring devices use the same network as cellphones to transmit data, while Bluetooth-enabled remote monitoring devices use wireless communication and require an internet connection. While remote monitoring devices currently do not send large amounts of data, not all devices can connect to a cellphone’s hot spot or send data directly through cellular platforms.

There is confusion about to how often devices and/or patients must transmit data to a provider to qualify for remote monitoring reimbursement. If data are not recorded and transmitted in real time, some experts said providers might not be able to bill for remote monitoring services.

CMS could address this confusion and facilitate access to remote monitoring by clarifying that it reimburses for store-and-forward technology. Store-and-forward, also called asynchronous technologies, allows for the electronic transmission of medical information to a practitioner at a distant site for
use outside of a live patient interaction. CMS should allow store-and-forward technology for remote monitoring billing codes and provide guidance on how often devices and/or patients must transmit data to a provider. For example, requiring data uploads at least weekly could be an appropriate safeguard. To the extent possible, this frequency should be based on disease-specific evidence. As federal agencies work to expand broadband, clarification from CMS regarding store-and-forward for remote monitoring services would facilitate access to care for patients who lack broadband access.\textsuperscript{156}

\textbf{Congress should clarify and refine anti-kickback safe harbors related to providing devices to patients. This is especially important for safety-net providers who often lack the resources to cover startup costs for a remote monitoring program.}

The dynamics of acquiring remote monitoring devices differ widely, influenced by such factors as medical necessity, where an individual lives, and a provider's financial models. Some patients own their devices outright, while others rely on short-term rentals, in which providers purchase or lease the device and supply it to the patient.

CMS has a billing code for the provision of a remote monitoring device, but anti-kickback statutes can make it difficult for medical providers to offer devices to patients. The anti-kickback statute penalizes individuals or entities for financial transactions intended to influence referrals to federal health care services. Providers and payers face a fine of $100,000, a prison term of 10 years, or both for:

\begin{quote}
knowingly and willfully [offering or paying] directly or indirectly, overtly or covertly, in cash or in kind to any \texttt{person} to induce such \texttt{person}—to purchase, lease, order, or arrange for or recommend purchasing, leasing, or ordering any good, facility, service, or item for which payment may be made in whole or in part under a \texttt{federal health care program}.\textsuperscript{157}
\end{quote}

Some providers find financial sources outside of Medicare to avoid anti-kickback penalties and to ensure patient access to remote monitoring.\textsuperscript{158} Yet many medical practices cannot supply devices to their patients without coverage for the device itself. Without provider involvement, some patients might not be able to afford beneficial remote monitoring services.

In recent years, the HHS Office of the Inspector General (OIG) has taken several steps to refine and clarify anti-kickback safe harbors and expand access to remote monitoring, including:

\begin{itemize}
\item In 2019, OIG \texttt{published} an advisory opinion allowing a pharmaceutical company to loan smartphones to financially constrained patients “to receive adherence data from a sensor embedded in prescribed antipsychotic medication.”\textsuperscript{159}
\end{itemize}
• In 2020, OIG published an anti-kickback final rule, which notes that remote monitoring could fit under the safe harbor exception under certain circumstances. The final rule aims to protect “certain value-based arrangements that would improve quality, outcomes, and efficiency … with an aim to support innovative methods and novel arrangements, including the use of digital health technology such as remote patient monitoring and telehealth.” The rule grants safe harbor protection for the exchange of digital health tools by medical device manufacturers, but it excludes physician-owned distributorships from this protection. OIG outlined the following example of a qualifying agreement: A “technology company could provide the physician group with necessary digital health technology that improves the physician group’s ability to observe recovery and intervene, as necessary.”

• In 2022, OIG published another advisory opinion allowing a medical provider to lend limited-use smartphones to “certain existing patients … to facilitate access to telehealth services.” The office noted that under some circumstances, this agreement would violate the anti-kickback statute, but that it would not take action against the provider. OIG cautioned that the “opinion may not be relied on by any person other than Requestor.”

• In 2023, OIG provided an advisory opinion allowing a manufacturer of an FDA-approved noninvasive colon cancer test to provide a $75 Mastercard gift card to some beneficiaries for returning the sample. Although this approach would typically breach the anti-kickback statute, OIG chose not to enforce any administrative penalties.

Although OIG’s actions have been critical, Congress should clarify and create safeguards to eliminate the necessity for advisory opinions such as the ones outlined above. Any legislation should clarify which types of remote monitoring agreements and equipment are not subject to anti-kickback penalties and should specify lawful practices under the existing billing codes.

Congress has attempted to address anti-kickback safe harbors in several bipartisan bills introduced in the 118th Congress. The DIVERSE Trials Act (S.2706/H.R.5030) would allow clinical trial sponsors to provide participants with digital health technologies that would facilitate their participation in the trial. These actions would not violate the anti-kickback statute. The CONNECT for Health Act (S.2016/H.R.4189) would clarify fraud and abuse laws regarding a medical provider furnishing remote monitoring-related technologies.
C. Data Security and Privacy

The HHS Office of Civil Rights should identify whether existing privacy policies adequately protect personal health information gathered, stored, and transmitted through remote monitoring. If gaps remain, the office should assess whether it has the authority to close that gap and, if it does not, Congress should do so.

Some regulatory experts argue that there are few gaps in the regulation of personal health information, but others disagree.¹⁶⁸,¹⁶⁹ One witness at a Senate hearing highlighted concerns about “an increasing amount of personal health information that is circulated and not regulated,” noting wearable technology home medical devices.¹⁷⁰ And existing privacy and cybersecurity protections have not fully protected consumers from ransomware attacks on hospitals and other companies that retain sensitive information.¹⁷¹ At the same time, it is important that unfounded concerns regarding patient privacy do not hinder the appropriate use of medically necessary technology.

The HHS Office of Civil Rights (OCR) should determine whether existing privacy policies adequately protect personal health information gathered, stored, and transmitted through remote monitoring. OCR could start by reviewing FDA cybersecurity policies, HIPAA, and the FTC’s Health Breach Notification Rule.

- FDA cybersecurity policies: Medicare only covers remote monitoring services that meet the FDA’s definition of a medical device, and FDA-reviewed devices must adhere to a level of cybersecurity that provides reasonable assurance of security for users. In 2023, the agency gained authority to refuse to accept any premarket submission that did not meet its cybersecurity requirements; it also alerted health care providers to cybersecurity vulnerabilities in a genetic sequencing device.¹⁷²,¹⁷³,¹⁷⁴,¹⁷⁵ Yet many legally marketed devices fall within the category of devices for which the FDA is exercising enforcement discretion, and therefore they might not meet the FDA standards for cybersecurity.

- HIPAA: CMS-covered remote monitoring devices must also adhere to HIPAA privacy standards. Yet—as outlined in the “Cybersecurity is Patient Safety” report by the office of Sen. Mark Warner (D-VA)—HIPAA focuses on data in a provider or payer setting, and the act does not cover many types of data and actors, such as apps and consumer devices.¹⁷⁶ Although HIPAA applies to data gathered via CMS-covered remote monitoring devices once those data reach the health care provider, confusion remains as to whether the act applies to data generated before reaching the provider.¹⁷⁷

- FTC’s Health Breach Notification Rule: Many entities that are not subject to HIPAA are subject to the FTC’s Health Breach Notification Rule, which requires companies to share a notification publicly after a data breach.¹⁷⁸
BPC supports proposed changes to the Health Breach Notification Rule to further safeguard personal health information by encompassing a wider range of data and entities. Some provisions of the rule would also address the perceived regulation of personal health information and ensure that all stakeholders are aware of their responsibilities with respect to those data.

If OCR determines there is no gap in privacy protections, it should make that finding clear through subregulatory means, such as blogs, speeches, and other communications. If OCR determines there is a gap in privacy protections, it should assess whether it has the authority to close that gap and then do so, if possible. If it does not have the authority, the agency should call on Congress to do so.

Congress has already considered the need for additional privacy laws. The bipartisan American Data Privacy and Protection Act (H.R.8152) was introduced in the House of Representatives in 2022 to create a comprehensive federal consumer privacy framework.179 The House Energy and Commerce Committee, in its report on the act, expressed that the sector-by-sector privacy laws were insufficient; that the state patchwork of laws was confusing for both consumers and businesses, leaving gaps and making compliance difficult; and that a national privacy law would provide more consistency and the appropriate level of oversight.180

**HHS should study the use of cybersecurity safe harbor laws to determine their effectiveness.**

Cybersecurity safe harbor provisions exist at the state and federal level to protect companies that experience cybersecurity breaches despite complying with industry-recognized cybersecurity standards. Both Utah and Ohio have safe harbor laws.181,182 Other federal laws, such as those protecting children's privacy, have safe harbor provisions.183 HHS recently received authority from Congress to consider a company's use of industry-standard security practices when making decisions about HIPAA violations.184 It remains to be seen if this change is effective.

HHS should study the use of cybersecurity safe harbor laws to determine their effectiveness and whether additional laws are needed. Congress proposed other studies on cybersecurity safe harbor provisions in the American Data Privacy and Protection Act, introduced in 2022.185 The bill directs the FTC to analyze safe harbor provisions related to children's online privacy and provide regular recommendations regarding policy changes to improve the effectiveness of these provisions.

HHS should also continue to enhance the ability of the HHS chief information officer to address cybersecurity concerns, as highlighted by Sen. Warner's (D-VA) 2022 Request for Information and an anticipated OIG report. The chief information officer is responsible for all information technology efforts within the department, including cybersecurity.186 Sen. Warner's "Cybersecurity is
Patient Safety” report outlines the need to ensure the officer is adequately equipped to lead HHS work on cybersecurity in health care, including by advocating for necessary resources, coordinating with other agencies, and outlining expectations of external stakeholders. An OIG report expected in 2025 will evaluate HHS’ governance over programs and assess whether appropriate minimum safeguards are in place to prevent, detect, and recover from cyberattacks.

**HHS, through the Office of the National Coordinator for Health Information Technology, should continue to ensure the existence of appropriate data standards so that remote monitoring devices can be interoperable with Electronic Health Record (EHR) systems.**

Interoperability facilitates seamless sharing of patient data across various systems. In remote monitoring, interoperability enables devices and EHRs to share information. Such integration streamlines provider workflows and offers a central home for patients’ health data. Research links the interoperability of remote monitoring to patient satisfaction, engagement, and safety.

Nearly 90% of providers use EHRs, and the percentage of hospitals that have some level of interoperability in their health records is rising. Yet integrating data from remote monitoring with existing EHRs has been a challenge. CMS requires that remote monitoring devices be able to transmit data electronically. However, there is no requirement regarding interoperability for a provider to receive reimbursement.

Many EHRs were designed for episodic care, rather than regular monitoring. And some providers have invested in new or updated EHR systems that might not be compatible with remote monitoring devices. Providers, as a result, must either manually enter remote monitoring data into their EHRs or rely on third-party vendor software to link remote monitoring data with EHR systems.

Stakeholders BPC spoke with expressed concern about situations in which a single provider or practice has patients with different remote monitoring devices, potentially leading to inconsistencies in data retrieval across those devices.

In recent years, Congress and federal agencies have taken many steps to facilitate health data exchange and interoperability. In the 21st Century Cures Act, Congress directed HHS to establish the Trusted Exchange Framework and Common Agreement (TEFCA), which HHS released in January 2022. TEFCA “describes a common set of nonbinding, foundational principles for trust policies and practices that can help facilitate exchange” among health information networks. HHS has announced that it approved six health information networks to adopt TEFCA by the end of 2023. The success of TEFCA hinges on widespread adoption.
Stakeholders within Congress, federal agencies, and the private sector recognize the importance of interoperability between medical devices and EHR systems. Academic experts urge the FDA to form a public-private partnership to support the interoperability of medical devices. The Better Interoperability for Devices Act (H.R. 1557), introduced in March 2023 and supported by industry stakeholders, would require an FDA study of medical device interoperability. And the FDA is researching and testing standards to promote interoperable medical devices.

HHS should build on this work and collaborate with stakeholders across the public and private sectors to ensure appropriate data standards so that remote monitoring devices are interoperable with EHR systems.
Conclusion

Remote monitoring devices have the potential to revolutionize clinical treatment and bridge gaps in care for hard-to-reach populations. Some policy and medical experts, however, voice concern about a lack of robust evidence on the optimal use of remote monitoring and question whether we are effectively “rightsizing” the use of these services, ensuring access for patients who need it most, and spending health care dollars in effective ways. Additionally, many disagree on the extent to which existing privacy policies adequately protect patient health information.

Adoption of remote monitoring is increasing rapidly and likely to continue to increase as technology improves, providers establish manageable workflows, and patients become more familiar with its use. Now is the time for policymakers, payers, and providers to refine their approach to this technology to maximize safe, appropriate adoption for patients who stand to benefit.

BPC’s recommendations are evidence-based, viable solutions to help guide policymakers forward. This report synthesizes findings from across the available published literature, as well as from in-depth conversations with health policy experts, federal officials, technology leaders, vendors, medical providers, payers, consumers, and academics. BPC’s work can inform policies to fully realize the promise of remote monitoring by fine-tuning coverage, ensuring equitable access to the technology, and prioritizing patient security.
Appendix A: Differences Between Remote Physiologic Monitoring and Remote Therapeutic Monitoring

<table>
<thead>
<tr>
<th></th>
<th>Remote Physiologic Monitoring</th>
<th>Remote Therapeutic Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Codes</strong></td>
<td>CPT Codes 99091, 99453, 99454, 99457, and 99458</td>
<td>CPT Codes 98975, 98976, 98977, 98978, 98980, and 98981</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Evaluation and management</td>
<td>General medicine</td>
</tr>
<tr>
<td><strong>Billing Provider</strong></td>
<td>Physicians and nonphysician practitioner who can bill for evaluation and management services, as well as certain clinical staff under the general supervision of the physician</td>
<td>Providers eligible to bill general medicine codes</td>
</tr>
<tr>
<td><strong>Data Types</strong></td>
<td>Physiologic data is not yet defined by CMS or the AMA, but illustrative examples provided by the RPM code descriptors include weight, blood pressure, pulse oximetry, and respiratory flow rate</td>
<td>Nonphysiologic data, including respiratory system status, musculoskeletal system status, therapy adherence in cognitive behavior therapy, and therapy response for cognitive behavior therapy</td>
</tr>
<tr>
<td><strong>Clinical Use Cases</strong></td>
<td>The RPM device supply code (99454) is not restricted to data related to specific biological systems</td>
<td>The device supply codes are limited to respiratory system data (98976), musculoskeletal system data (98977), and cognitive behavioral therapy data (98978)</td>
</tr>
<tr>
<td><strong>Data Collection</strong></td>
<td>FDA-approved medical device must digitally (i.e., automatically) record and upload patient physiologic data</td>
<td>Requires the use of an FDA-approved device, but data may be digitally uploaded or manually self-reported</td>
</tr>
</tbody>
</table>

# Appendix B: CPT Code Descriptions and CY2023 Reimbursement Rates for Remote Physiologic Monitoring and Remote Therapeutic Monitoring

## Remote Physiological Monitoring

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Reimbursement Rate</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPT 99453</td>
<td>Initial setup and patient training on the use of equipment</td>
<td>$19</td>
<td>Billed once per device</td>
</tr>
<tr>
<td>CPT 99454</td>
<td>Supply of device and collection of data</td>
<td>$50</td>
<td>Billed once per 30 days if the patient takes at least 16 daily readings</td>
</tr>
<tr>
<td>CPT 99457</td>
<td>First 20 minutes of patient interaction to adjust treatment based on RPM recordings</td>
<td>$48</td>
<td>Billed once per 30 days</td>
</tr>
<tr>
<td>CPT 99458</td>
<td>Second (and third) 20 minutes of patient interaction to adjust treatment based on RPM recordings</td>
<td>$39</td>
<td>Can be billed multiple times in a 30-day period</td>
</tr>
<tr>
<td>CPT 99091</td>
<td>Time spent by provider to interpret information received from an RPM device (at least 30 minutes)</td>
<td>$54</td>
<td>Billed once per 30 days</td>
</tr>
</tbody>
</table>

## Remote Therapeutic Monitoring

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Reimbursement Rate</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPT 98975</td>
<td>Initial setup and patient training on the use of equipment</td>
<td>$19</td>
<td>Billed once per device</td>
</tr>
<tr>
<td>CPT 98976</td>
<td>Supply of device with scheduled recording and/or programmed alert(s) transmission to monitor respiratory system</td>
<td>$50</td>
<td>Billed once per 30 days if the patient takes at least 16 daily readings</td>
</tr>
<tr>
<td>CPT 98977</td>
<td>Supply of device with scheduled recording and/or programmed alert(s) transmission to monitor musculoskeletal system</td>
<td>$50</td>
<td>Billed once per 30 days if the patient takes at least 16 daily readings</td>
</tr>
<tr>
<td>CPT 98978</td>
<td>Remote therapeutic monitoring (e.g., therapy adherence, therapy response); device(s) supply with scheduled (eg, daily) recording(s) and/or programmed alert(s) transmission to monitor cognitive behavioral therapy</td>
<td>Code is contractor priced; no national data available</td>
<td>Billed once per 30 days if the patient takes at least 16 daily readings</td>
</tr>
<tr>
<td>CPT 98980</td>
<td>Time spent by provider to perform treatment or interpret data; requires patient interaction, first 20 minutes</td>
<td>$49</td>
<td>Billed once per 30 days</td>
</tr>
<tr>
<td>CPT Code</td>
<td>Description</td>
<td>Rate</td>
<td>Time Billed</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>98981</td>
<td>Time spent by provider to perform treatment or interpret data; requires patient interaction, each additional 20 minutes</td>
<td>$39</td>
<td>Can be billed multiple times in a 30-day period</td>
</tr>
<tr>
<td>95249</td>
<td>Patient-provided equipment, sensor placement, hookup, calibration of monitor, patient training, and printout of recording</td>
<td>$62</td>
<td>Billed once per device</td>
</tr>
<tr>
<td>95250</td>
<td>Ambulatory continuous glucose monitoring of interstitial tissue fluid via a subcutaneous sensor for a minimum of 72 hours; physician or other qualified health care professional (office) provided equipment, sensor placement, hookup, calibration of monitor, patient training, removal of sensor, and printout of recording</td>
<td>$147</td>
<td>Billed once per 30 days</td>
</tr>
<tr>
<td>95251</td>
<td>Ambulatory continuous glucose monitoring of interstitial tissue fluid via a subcutaneous sensor for a minimum of 72 hours; analysis, interpretation, and report</td>
<td>$35</td>
<td>Billed once per 30 days</td>
</tr>
</tbody>
</table>

**Note:** In the 2024 Physician Fee Schedule, CMS provides conflicting information regarding the 16-day data collection requirement for remote monitoring. Page 78883 lists RPM and RTM supply codes, RPM setup code, and RTM treatment codes: “only one practitioner can bill CPT codes 99453 and 99454, or CPT codes 98976, 98977, 98980, and 98981, during a 30-day period, and only when at least 16 days of data have been collected.” Yet on page 78884, CMS explicitly states that the requirement does not apply to RPM and RTM treatment management codes 99457, 99458, 98980, and 98981, emphasizing that these codes account for provider time spent in a calendar month and do not require 16 days of data collection in a 30-day period.

**Sources:**
# Glossary of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMA</td>
<td>American Medical Association</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare &amp; Medicaid Services</td>
</tr>
<tr>
<td>CPT</td>
<td>Current Procedural Terminology</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>FDA</td>
<td>Food and Drug Administration</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>FQHC</td>
<td>Federally Qualified Health Center</td>
</tr>
<tr>
<td>HHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>MedPAC</td>
<td>Medicare Payment Advisory Commission</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of the Inspector General</td>
</tr>
<tr>
<td>PCCP</td>
<td>Predetermined Change Control Plan</td>
</tr>
<tr>
<td>RHC</td>
<td>Rural Health Clinic</td>
</tr>
<tr>
<td>RPM</td>
<td>Remote Physiologic Monitoring</td>
</tr>
<tr>
<td>RTM</td>
<td>Remote Therapeutic Monitoring</td>
</tr>
<tr>
<td>TEFCA</td>
<td>Trusted Exchange Framework and Common Agreement</td>
</tr>
</tbody>
</table>
Endnotes


10 Ibid.


35 Ibid.


41 Center for Connected Health Policy, "Policy trend maps,” 2023. Available at: https://www.cchpca.org/policy-trends/.


Inter-American Development Bank, “At least 77 million rural inhabitants have no access to high-quality internet services,” October 29, 2020. Available at: https://www.iadb.org/en/news/least-77-million-rural-inhabitants-have-no-access-high-quality-internet-services#:~:text=Of%20the%20total%20amount%20of%20rural%20areas%20of%20the%20Americas.


89 Ibid.


Ibid.


South Carolina Department of Health and Human Services, "Why is this provider attestation form needed?" Available at: https://www.scdhhs.gov/sites/default/files/Provider%20Attestation%20Form%20User%20Guide%20v1.2.pdf.


130 Ibid.

131 Ibid.


134 Claudia Wallis, “Fixing Medical Devices That Are Biased against Race or Gender,” *Scientific American*, June 1, 2021. Available at: https://www.scientificamerican.com/article/fixing-medical-devices-that-are-biased-against-race-or-gender/.


Ibid.

Ibid.

164 Ibid.


167 S.2016—The CONNECT for Health Act, 118th Congress (2023-2024). Available at: https://www.congress.gov/bill/118th-congress/senate-bill/2016/all-info?s=2&r=1&q=%7B%22search%22%3A%22connect%22%7D.


The Bipartisan Policy Center helps policymakers work across party lines to craft bipartisan solutions. By connecting lawmakers across the entire political spectrum, delivering data and context, negotiating policy details, and creating space for bipartisan collaboration, we ensure democracy can function on behalf of all Americans.