CTRC 2026 Digital Health Summit
FAQ Document

Is RPM reimbursable at an FQHC?

Yes, in looking at the FQHC Fee Schedule for CMS, the following codes are billable at an FQHC: 99453, 99454, 99457, 99458.
Source: https://www.cms.gov/files/zip/rhc-fqhc-cy-2026-non-facility-payment-rates.zip
The HHS website also states RPM is covered by FQHCs:
https://telehealth.hhs.gov/providers/best-practice-guides/telehealth-and-remote-patient-monitoring/billing-remote-patient

If a participant is enrolled in the ACCESS model on the HT track, would they then be excluded from reimbursements for RPM for the same condition?

For ACCESS enrollees, it appears it depends on the beneficiary. An ACCESS provider who sees a beneficiary enrolled for ACCESS services and is paid by the ACCESS model can not also bill at FFS to Medicare.
Source: https://www.cms.gov/priorities/innovation/access-technical-frequently-asked-questions

Here's a question we recently received from one of our health centers: "Patients can choose not to have an AI scribe record their voice during the visit. However, this does not prevent the provider from using AI tools later to help complete the chart from their own notes or dictation. It's important to explain this clearly, as some patients may assume they are opting out of all AI use. any recommendations?"

Patient Opt-Out of AI Scribes vs. Other AI Use
When patients opt out of AI scribes, it's important to clearly explain the scope of that choice. The opt-out typically applies only to real-time ambient recording tools (e.g., voice capture during the visit), not to all downstream uses of AI.
Sample Script: "If you prefer, we won't use AI tools that listen during your visit. However, your provider may still use secure tools afterward to help organize their notes and complete your chart."

How can we determine where AI platforms are storing their data?

Understanding where data is stored is essential for compliance and risk management.
Review vendor documentation: Look for data hosting details, including geographic location (e.g., U.S.-based vs. international data centers).
Request a Data Processing Agreement (DPA) or Business Associate Agreement (BAA): These typically define storage, handling, and security responsibilities.

Ask direct questions:

- Where is data stored (region/cloud provider)?
- Is data used for model training?

Is it retained, and for how long?
Engage IT/security teams: They can validate architecture, encryption standards, and access controls.
Confirm certifications: Look for SOC 2, HITRUST, or other healthcare-relevant compliance frameworks.

How do we safely use AI to perform an analysis of organization reports?

AI can add value in summarizing, identifying trends, and generating insights—but must be used carefully.
Best practices:
Avoid sensitive data in non-approved tools: Only use AI platforms that are vetted and authorized by your organization.
De-identify data where possible: Remove patient identifiers before uploading any reports.
Use secure, enterprise-grade AI solutions: Prefer platforms with HIPAA alignment and contractual protections (e.g., BAAs).
Limit scope of inputs: Share only the minimum data needed to complete the analysis.
Validate outputs: Always review AI-generated insights for accuracy before using them in decision-making.
Document use: Maintain transparency about when and how AI is used in internal workflows.