HealthAxis

Understanding API Integrations: A Guide for Healthcare IT Leaders

For government health programs, application programming interfaces (APIs) have moved from technical mechanisms for developers to boardroom topics. Between CMS interoperability rules, ONC information blocking regulations, and rising expectations from members and providers, APIs now sit at the center of how Medicaid, CHIP, Medicare Advantage, and Marketplace plans will operate and compete in the next decade. [1, 2]

Use this guide to understand how a modern, API-enabled architecture can support your long-term roadmap, shaping data flow, member and provider experiences, and your current systems.

1. Why APIs are now a strategic priority in government programs

- Federal interoperability rules. CMS requires many regulated payers to implement FHIR-based Patient Access and Provider Directory APIs, and newer rules add Provider Access, Payer-to-Payer, and Prior Authorization APIs for certain programs in 2027. [1, 3, 4]
- ONC information blocking enforcement. The Office of Inspector General can now impose significant penalties for practices that unreasonably interfere with access, exchange, or use of electronic health information, using ONC regulations as the basis for enforcement. [5, 6]
- Shift to standards-based APIs. The HL7 FHIR standard is quickly going to become the dominant, API-focused standard not only for health plans but for providers for representing and exchanging health data and is referenced explicitly in multiple federal regulations and certification programs. [2, 7, 8]
- Security expectations. NIST and ONC emphasize that APIs are now core enterprise assets that must be secured across the entire lifecycle, from design to deployment and monitoring. [9, 10]

For CIOs and CTOs, this means APIs are no longer just implementation details. They shape compliance risk, member experience, partner strategy, and even how quickly your organization can respond to new benefit designs or policy changes.

2. API fundamentals for healthcare leaders

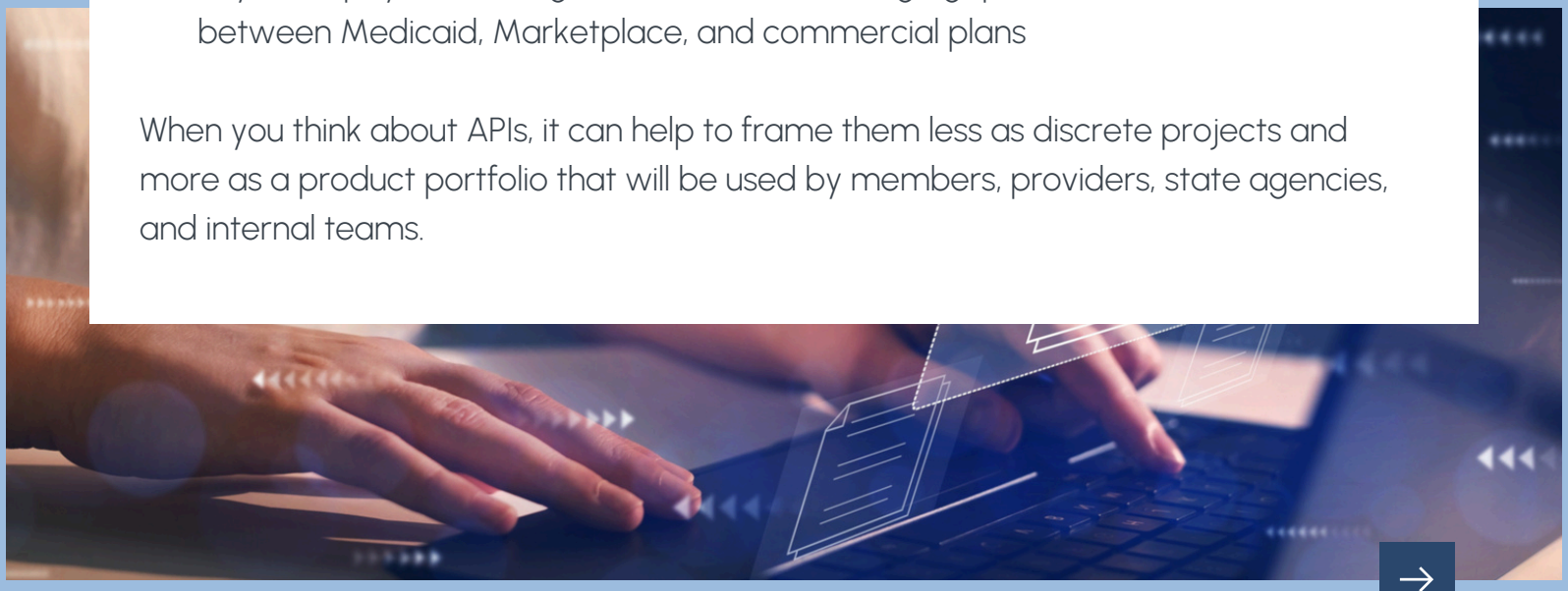
You do not need to be a developer to lead an API strategy, but having a mental model helps. At a high level:

- An **API** is a controlled way for one system to request or push data to another system.
- **RESTful APIs** are commonly used in health IT. They use standard web methods to read or write resources such as patients, claims, or coverage.
- **Fast Healthcare Interoperable Resources (FHIR) developed by HL7** specifically to address the needs of the healthcare industry defines the structure and meaning of those resources, plus how they should be exchanged via APIs, so different systems can interpret the data consistently.[7, 11]

For government insurance programs, the real value of APIs comes from what they enable:

- A mobile app that lets members see coverage, claims, and prior authorizations in near real time
- Real time data sharing between payers and providers to enable rapid resolution to patient care needs
- A provider portal that pulls eligibility, benefits, and panel attribution without manual file exchanges
- Payer-to-payer exchanges that reduce coverage gaps when members churn between Medicaid, Marketplace, and commercial plans

When you think about APIs, it can help to frame them less as discrete projects and more as a product portfolio that will be used by members, providers, state agencies, and internal teams.



3. The Evolving Regulatory and Standards Landscape

Several federal initiatives directly influence how you design and govern APIs:

CMS Interoperability and Patient Access rules
CMS has focused on FHIR-based APIs for Patient Access and Provider Directories for Medicare Advantage, Medicaid, CHIP, and certain Marketplace plans, and newer rules extend requirements to prior authorization and additional access APIs. [1, 3, 4, 12]

ONC certification and HTI-1
ONC's Health Data, Technology, and Interoperability (HTI-1) final rule updates certification criteria to require modern, standards-based APIs and support expanded information sharing. [2, 6, 13]

Information blocking enforcement
OIG enforcement of information blocking can lead to substantial penalties per violation, reinforcing the need for policies and technical controls that support appropriate API-based information sharing. [5]

Security and privacy guidance
NIST's 2025 special publication on API protection and ONC's privacy and security considerations for healthcare APIs provide frameworks for managing risks such as authentication, authorization, auditing, and third-party developer access. [9, 10]

For leadership teams, the takeaway is that API decisions cannot be made in isolation. Architectural choices directly affect whether your organization can comply efficiently and securely with current and future rules or will end up with fragmented one-off implementations.

4. High Value API use cases in Government Programs

Not every integration needs to become a formal API product. However, there are several high value areas where an API-first approach often pays off for Medicaid, CHIP, Medicare Advantage, and Marketplace stakeholders:

- **Member access across coverage transitions**
  FHIR-based Patient Access APIs can support continuity of information when members move between Medicaid and Marketplace coverage, which is especially relevant as eligibility rules evolve. [1, 3, 12]

- **Provider-facing integrations**
  Provider Access APIs can supply up to date member attribution, benefits, and prior authorization status into provider EHRs and care management tools, reducing manual lookups and call center volume. [3]

- **Payer-to-payer data exchange**
  Using APIs for payer-to-payer exchange can reduce reliance on batched file transfers and help support more accurate risk adjustment, quality reporting, and gap closure when members switch plans. [3]

- **Open provider directories**
  Public Provider Directory APIs help members and partners find in-network providers and support external tools that assist with network adequacy, access, and referrals. [12, 14]

- **Prior authorization automation**
  Prior Authorization APIs will open up real-time automated workflows between payers and providers and help reduce delays in care when combined with robust clinical policy engines. [3]

As you consider these use cases, an important question for leadership is whether your current claims, member, and provider systems can expose consistent APIs without extensive custom work each time.

5. Risks, Pitfalls, and What Leadership Should Watch

APIs offer major upside, but they also introduce new risks that executives should understand:

- **Security by design, not by inspection.** NIST emphasizes that APIs must be secured across the entire lifecycle, including design, coding, deployment, and continuous monitoring.[9, 15] Poor schema design, overly broad scopes, or missing rate limits can lead to incidents even if you have traditional perimeter defenses in place.
- **Privacy and app ecosystem governance.** ONC highlights issues such as third-party app vetting, user consent, and data minimization when enabling patient-directed API access.[10] Leadership teams should define clear policies for which APIs are open, which require registration, and how member education will occur.
- **Shadow APIs and duplication.** Without strong governance, it is easy for multiple teams or vendors to publish overlapping APIs, each wired into core systems differently. This increases cost and creates inconsistent experiences for providers and members.
- **One-off compliance builds.** Implementing APIs purely to meet a single rule, without an enterprise API strategy, can lead to fragile point solutions that are hard to extend to new use cases or programs.

Governance, architecture, and platform choices can help mitigate these risks, so APIs become an asset instead of another integration headache.

6. Key Questions to Shape your API Roadmap

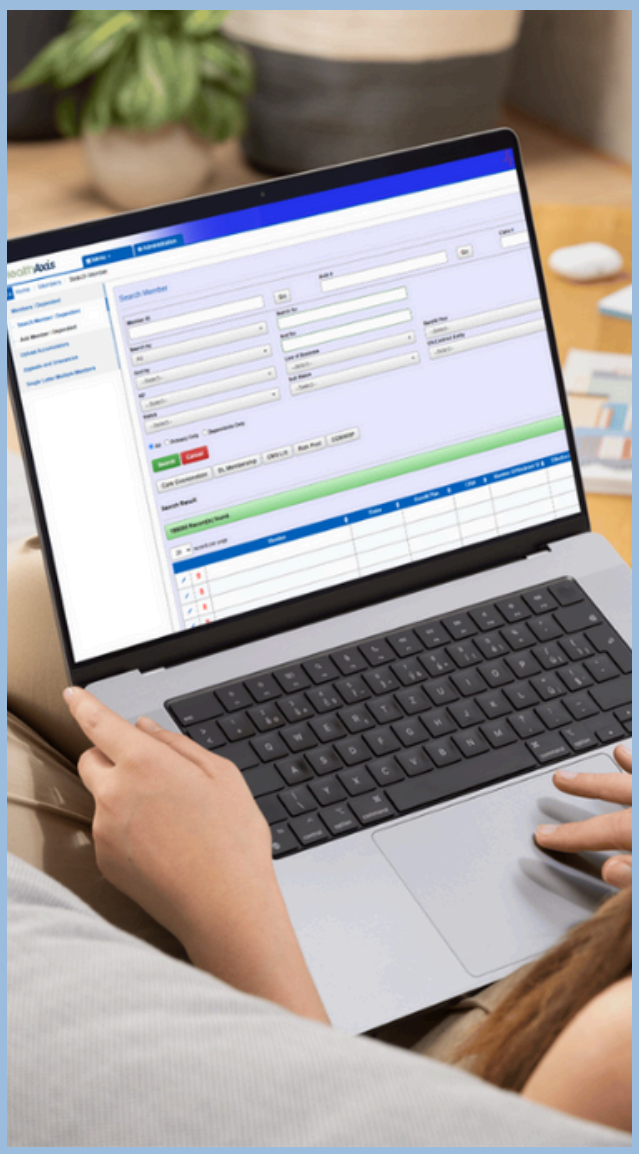
As CIOs, CTOs, and heads of application development look to expand their organization's API footprint, the most important work often happens before any additional APIs are deployed. Questions to consider include:

1. **Vision and scope**
   - Of the regulatory APIs (Patient Access, Provider Directory, Provider Access, Payer-to-Payer, Prior Authorization) that apply to us today, which will have the biggest impact on your business processes in the next three to five years? [1, 3]
   - Beyond compliance, which member, provider, and partner experiences would benefit most from API enablement?
2. **Standards alignment**
   - How closely do our data models and existing ReSTful APIs align with FHIR resource standards and ONC's United States Core Data for Interoperability (USCDI), and where are the gaps? [2, 13]
   - Do we have a plan to track and adopt future versions of relevant standards and implementation guides?
3. **Security and trust**
   - Have we adopted NIST and ONC guidance for API authentication, authorization, logging, and monitoring as part of our enterprise security architecture, not just individual projects?
   - How do we manage third party developer onboarding, app registration, and ongoing risk assessment? [9, 10, 16]
4. **Platform and architecture**
   - Are we able to leverage our core systems APIs instead of relying heavily on custom integration layers and one-off adapters?
   - Are we investing in an API management layer that handles versioning, throttling, and analytics so teams can innovate without re-solving those problems each time?
5. **Operating model**
   - Who owns API products internally, and how are they funded, prioritized, and measured?
   - How will we support parallel tracks for compliance-driven APIs and innovation-oriented APIs that serve new digital experiences?

These questions can guide an internal assessment or roadmap exercise, even before you select specific tools or vendors.

7. How HealthAxis and AxisCore Fit into the Picture

At HealthAxis, we see APIs as a central enabler of modern government program operations rather than a separate technical initiative. Platforms such as AxisCore are designed with an API first mindset so that core functions like eligibility, enrollment, claims, and provider data management can participate in FHIR-based and other standards-based exchanges without extensive custom work every time a new policy or partner requirement emerges.



For technology leaders, the specific product you choose matters less than whether it supports:

- Standards-based ReSTful APIs aligned with FHIR and relevant CMS and ONC rules
- A unified data model that avoids fragmentation between member, provider, and claims data
- Governance, versioning, and security practices that are consistent with NIST and ONC guidance

AxisCore is one example of a platform designed with these principles in mind, but the broader point is that your API strategy should be tightly coupled with your core platform roadmap, not layered after the fact.

Closing Thoughts

API integration is no longer optional for government-focused health plans and agencies. It touches compliance, security, member and provider experience, and your ability to adapt to policy and market changes. The most successful organizations will treat APIs as strategic products, grounded in standards like FHIR and informed by evolving CMS, ONC, and NIST guidance, rather than as isolated technical projects.

If your team is beginning or revisiting an API roadmap, HealthAxis can share perspectives from work with payers and partners across government programs. Chat with one of our Medicaid experts today!

Visit healthaxis.com/schedule-a-discovery-call/

Sources

1. Centers for Medicare & Medicaid Services. "CMS Interoperability and Patient Access Final Rule (CMS-9115-F)." CMS
2. Office of the National Coordinator for Health IT. "Fast Healthcare Interoperability Resources (FHIR)." HealthIT
3. Centers for Medicare & Medicaid Services. "Application Programming Interfaces (APIs) and Relevant Standards and Implementation Guides." CMS
4. CMS. "Patient Access API – Frequently Asked Questions." CMS
5. HHS Office of Inspector General. "Information Blocking." Office of Inspector General
6. ONC. "Health Data, Technology, and Interoperability (HTI-1) Final Rule." HealthIT
7. CMS. "Learn About FHIR." CMS
8. American College of Physicians. "Summary of the Office of the National Coordinator for Health IT's (ONC) Information Blocking and Health IT Certification Program Final Rule." American College of Physicians
9. NIST. "Special Publication 800-228, Guidelines for API Protection for Cloud-Native Systems." NIST Computer Security Resource Center
10. ONC. "Key Privacy and Security Considerations for Healthcare Application Programming Interfaces (APIs)." HealthIT
11. HL7. "FHIR Overview." HL7
12. Health Management Associates. "Interoperability and patient access final rule: the next phase in the data exchange journey." Health Management Associates
13. HIMSS. "Final ONC Interoperability Regulation: What You Need to Know." HIMSS
14. CMS. "Provider Directory API – Frequently Asked Questions." CMS
15. ExecutiveGov. "NIST Publishes New Guideline on Securing APIs for Enterprise IT Systems." Executive Gov
16. NIST. "Health Information Technology (IT) – NIST for Healthcare." NIST