*Integrated code quality and security for healthcare*

# Leading healthcare organizations use SonarQube to build life-critical software with absolute confidence

Healthcare organizations operate under a zero-failure imperative: the need to accelerate digital transformation while maintaining life-critical legacy infrastructure and strict regulatory standards. AI-driven development promises to break through structural barriers, but simultaneously introduces new risks to patient safety and data privacy. Sonar provides the essential code verification layer that empowers teams to modernize systems and deploy AI with confidence, ensuring innovation never comes at the cost of compliance.

- **Centralize quality management:** Bridge the legacy-digital divide. SonarQube unifies diverse teams on one platform, ensuring that maintaining legacy systems doesn't stall future innovation.
- **Streamline compliance:** Turn verification into a deployment accelerator. Automated quality gates help you enforce code quality, security, and coverage standards, logging findings and making audit readiness a natural part of daily development.
- **Secure AI adoption:** Modernize with confidence. SonarQube analyzes AI-generated code for bugs and security flaws, ensuring that new code meets strict standards before it touches patient data.
- **Fortify the supply chain:** Safeguard your entire digital ecosystem against third-party risk. SonarQube provides deep visibility into open source dependencies and generates SBOMs, ensuring that vulnerabilities in external code do not compromise patient data or critical infrastructure.
- **Manage technical debt:** Stop letting maintenance block innovation. SonarQube identifies debt across 35+ languages, freeing up engineering resources to focus on clinical breakthroughs.
- **Simplify modernization:** Retain top talent by removing toil. Real-time feedback in the IDE helps developers navigate complex legacy migrations or maintenance without burnout.

## What leading businesses from the healthcare industry say about SonarQube

*"SonarQube has definitely brought in compliance for the organization. The code coverage enforcement has resulted in less number of defects. Also, security team has more confidence in software deliveries."*

**Director, Medium Enterprise Health Care Providers & Services Company**

*"Previously we were flying blind, creating software with varying quality and no common standards. Use of code quality scanning was at best an afterthought and differing groups had differing standards. Now we have a common platform, with enforced quality in our pipelines, and common definitions."*

**Chris Blake, Principal DevOps Engineer, Werfen**

AstraZeneca novo nordisk BAYER CVSHealth Johnson&Johnson Optum

# Key SonarQube features for the healthcare industry

**Automated code review across 35+ languages:** SonarQube covers the entire healthcare stack—from the "geological layers" of legacy C++ and COBOL backends to modern Python and React. This unified analysis ensures consistent code quality whether you are maintaining a 20-year-old EHR or building a new telehealth microservice.

**Support for regulatory compliance:** Eliminate the manual "compliance tax" of the traditional V-Model. SonarQube generates detailed reports on code security, quality, and coverage that help organizations align with regulatory frameworks. This makes compliance a continuous byproduct of development rather than a pre-release bottleneck.

**Vulnerability detection:** Protect sensitive data by identifying critical flaws before they reach production. SonarQube detects risks such as SQL injection and cross-site scripting (XSS), which are particularly dangerous in the fragile "glue code" used to parse HL7 messages and interconnect disparate hospital systems.

**Seamless CI/CD integration:** Strengthen regulatory compliance by automating code quality and code security gates within your existing pipelines. This allows development teams to adopt modern DevOps practices and release updates faster without compromising the rigorous validation required for SaMD (Software as a Medical Device) and other standards.

**Secure AI tooling:** Safely leverage AI agents to assist in code generation or refactor legacy logic. SonarQube automatically inspects AI-generated code for security holes and quality issues, providing the guardrails needed to modernize sensitive clinical algorithms without introducing risk.

**Software supply chain security:** Safeguard patient data against risks hidden in the open-source libraries. SonarQube Advanced Security detects known vulnerabilities within third-party dependencies and manages license compliance, ensuring that the external components integrated into your products meet the same rigorous safety standards as internal code.

**Improved code maintainability:** Systematically pay down technical debt. By identifying high-complexity "spaghetti code" in monoliths, SonarQube guides refactoring and maintenance efforts, making systems more stable and easier to update with new essential features.

**Custom security rules:** Adapt to the unique constraints of your environment. Healthcare organizations can configure custom policies to enforce specific coding standards, ensuring code meets internal security postures.

**Code coverage visibility:** Provide the evidence required for regulatory audits. Centralized code coverage metrics prove that your software—including critical device firmware and diagnostic algorithms—has been rigorously tested, helping satisfy the testing evidence requirements of GxP validation.

## Sonar's approach: Actionable code intelligence

### Analyze

Deep insight on architectural, quality, and security issues in all code, no matter the source

**Code Quality**
Deliver high-quality code, whether human, AI-assisted, or agentic.

**Code Security**
Prevent security risks early, both within your code and from 3rd parties.

### Review

Define, apply, and attest to code standards and policies as a team

**Code Orchestration**
Automate governance and compliance while establishing standards across teams.

### Act

Agentic or on-demand issue remediation

**Code Remediation**
Resolve issues before they become problems. Modernize old code with AI.

← *Vibe* with better context → ← then *Verify* every line of code, anywhere →