Nava

Understanding what open source means

What does "open source" mean for your state?

OSCER is open source software, which means Nava has made the core application code publicly available for any state to use without ever paying any licensing fees. When a state implements OSCER, a state will deploy it entirely within their own environment—state's infrastructure, state private repositories, and it's under state control. The code belongs to the state to use and customize as needed.

What benefit does OSCER provide as an open source solution?

The benefit of open source is that you don't have to build a community engagement reporting system from scratch or build the features into existing systems. OSCER provides a ready-to-use front end, a rules engine to calculate exemptions and compliance, and case management capabilities. Instead of spending months developing these components, the team can focus on integration with your existing systems and state-specific customizations. With the tight deadlines many states face for work requirements reporting, this approach can save significant time and resources.

Common questions about open source security and implementation

States considering OSCER may have questions about how open source solutions meet security requirements, maintain compliance, and integrate with existing systems. The points below address common concerns.

Security & compliance

How are community contributions vetted for security?

Every contribution to OSCER goes through rigorous automated and manual review:

- Automated security scans, linting, unit tests, and end-to-end tests run on all proposed changes
- Vulnerability scanning is built into the development pipeline
- Final approval required from trusted Nava staff before any code is merged

Contributions by the community follow the same standards of review that our Nava team uses internally, ensuring consistent security practices across all implementations.

See our detailed processes:

- Contributing guidelines and code review process
- Code review standard operating procedures
- Vulnerability management

How does OSCER protect data?

OSCER is deployed entirely within the state's infrastructure:

- All data remains in the state's environment and under state control
- No protected health information (PHI) or personally identifiable information (PII) leaves the state systems
- System connections happen within the state's existing security boundaries
- A state's implementation code, infrastructure configuration, and any customizations remain completely private in the state's own repositories. Only Nava's core OSCER application code is open source and publicly visible. Your state-specific code never needs to be shared publicly.

Does OSCER align with HIPAA regulations?

OSCER can support HIPAA-aligned deployments (it has the kinds of controls you'd expect in a system handling sensitive data), but HIPAA compliance is determined by how the deploying organization configures, hosts, and operates it.

OSCER supports HIPAA-aligned deployments with documented safeguards:

Administrative Safeguards:

- Attribute-based access control
- User provisioning and deprovisioning guidance

Technical Safeguards:

- Authentication and authorization mechanisms
- Audit logging capabilities
- Encryption (in transit and at rest)
- Session management

View comprehensive documentation:

- Application security approach
- Security guidance
- All OSCER documentation

Maintenance & operations

What's involved in ongoing maintenance?

While OSCER accelerates initial development, states maintain operational responsibility:

Vulnerability Scanning:

- Nava provides extensive automation for the core OSCER instance
- Most package updates are highly automatable (using tools like Dependabot or Renovate)
- Vulnerabilities in application code are fixed and rolled out before public announcement
- We support configuring the state's own vulnerability scanners to work with the state’s OSCER deployment

Patching:

- Nava can provide container images for new versions ready to deploy
- We recommend a container workflow for easier automation and auditability
- If the state environment requires VM deployment, that's supported but involves higher maintenance.

Audits:

- Documentation available to support audits
- Nava can provide direct audit support as needed

How do states adopt updates from the community?

States maintain full control over which updates to adopt:

- Review tagged releases and decide what to pull into the state’s own instance
- Tooling available to help manage version control
- Security review updates before adoption into the state’s environment
- The state determines the timeline for implementing changes

Hosting & integration

What are the hosting requirements?

OSCER is a monolithic web application with flexible deployment options:

- Requires: PostgreSQL database and file storage
- Recommended: Container runtime (for automation, auditability, ease of deployment)
- Hosted entirely within the state's cloud infrastructure
- No exotic infrastructure requirements

How does OSCER integrate with existing systems?

Multiple integration approaches are available depending on your needs:

Batch Integration:

- Easier implementation requiring fewer changes to existing systems
- Great starting point for proof of concept
- Can layer on API integration later

API Integration:

- Supports real-time user experiences
- Offers operational flexibility (automated retries, etc.)
- Can be implemented after starting with batch

Single Sign-On (SSO) – coming soon:

- Integrates with the existing state SSO systems
- Covers both member and case worker experiences
- No need to manage additional authentication systems
- Uses roles and attributes from state's SSO for authorization

Notifications:

- Customizable to use different notification services
- Can configure to use your cloud communication services
- Can route notification requests to your existing Medicaid system

Implementation teams provide support throughout the integration process.

Frequently asked questions

Will our data be exposed to the public because OSCER is open source?

No. Open source refers to the code being public. Your deployment, configuration, and data remain in your environment and under your access controls.

Do we have to accept changes from the open-source community?

No. You choose what to adopt. Many organizations use release-based upgrades and pull in upstream changes only after review.

How do we know community contributions are safe?

OSCER uses automated checks plus human review, and changes are only merged when approved by trusted maintainers. You can also apply your internal review processes before adopting any upstream release.

Can we run our own security tools and scans?

Yes. Organizations commonly integrate their standard scanners into their own CI/CD pipelines and hosting environments.

Who is responsible for HIPAA/security compliance?

Compliance is a shared responsibility. OSCER provides secure patterns and documentation, but your organization’s deployment, operations, and governance determine the compliance posture of the running system.