NSA Checklist for Payers
What Payers Need To Know

The No Surprises Act (NSA) introduces significant new regulatory requirements that will increase the administrative burden on payer organizations. As payers work to comply with these complex provisions, including the need for transparent billing practices and timely dispute resolution, they face heightened pressure to maintain precise and up-to-date provider data.

Inaccurate or outdated information can lead to costly penalties, member dissatisfaction, and strained provider relationships. To navigate these challenges effectively, payers must prioritize robust provider data management solutions that can ensure accuracy, streamline operations, and mitigate compliance risks under the NSA.

See below for a list of non-negotiables when evaluating provider data management solutions

Data Accuracy and Verification

LOOK FOR:

- ☐ **Automated Verification Processes:** Ensure the solution offers automated and frequent verification of provider information, reducing manual errors and ensuring up-to-date data.
- ☐ **Data Integrity Monitoring:** Look for tools that continuously monitor and flag discrepancies in provider data, allowing for quick corrections before they impact compliance.

Centralize Provider Data & Contracting

LOOK FOR:

- ☐ **Streamlined Contract Management:** Centralizing contracting information allows for easier management and tracking of provider agreements, ensuring that all contracts are up-to-date and compliant with NSA requirements. This reduces the risk of overlooked contract renewals or inconsistencies in terms.
- ☐ **Improved Data Consistency:** By housing provider data and contracting details in one centralized system, the risk of discrepancies between different systems is minimized. This ensures consistent information across all platforms, aiding in accurate reporting and compliance while optimizing cycle time.

© 2026 symplr | All rights reserved.

Integration Capabilities

LOOK FOR:

- ☐ **Seamless Integration with Existing Systems:** The solution should easily integrate with your current systems, including credentialing, billing, and member services, to ensure consistent and accurate provider data across platforms.
- ☐ **Interoperability with Third-Party Systems:** Evaluate the ability of the solution to communicate with third-party platforms and regulatory databases, ensuring compliance with both federal and state NSA requirements.

Real-Time Data Updates

LOOK FOR:

- ☐ **Frequent and Automated Updates:** The solution should support real-time updates of provider data, ensuring that any changes are promptly reflected across all systems and directories.
- ☐ **Member Accessibility:** Ensure the solution provides timely updates to provider directories and claims accessible to members, reducing the risk of outdated information leading to compliance issues.

Compliance Reporting & Audit Trails

LOOK FOR:

- ☐ **Comprehensive Audit Trails:** The solution must provide detailed records of all data updates, changes, and verification processes, including the ability to capture the reason for change to ensure transparency and readiness for audits.
- ☐ **Customizable Compliance Reports:** Look for features that allow the generation of customized reports demonstrating compliance with NSA requirements, particularly concerning accurate provider data management.

Scalability & Future-Proofing

LOOK FOR:

- ☐ **Scalability to Meet Growing Needs**: Assess whether the solution can scale with your organization's growth and increasing data management demands without compromising performance.
- ☐ **Adaptability to Regulatory Changes:** Ensure the solution is flexible and can adapt to future changes in NSA regulations or additional compliance requirements, reducing the need for significant future investments.

Learn more about
our Payer solutions

© 2025 symplr | All rights reserved.