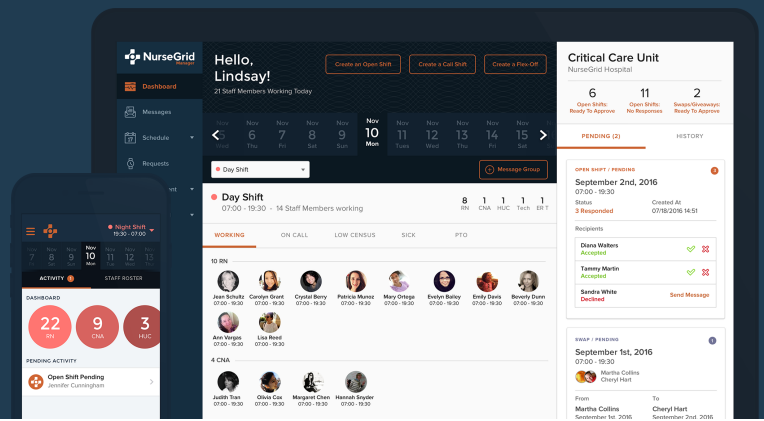




Secure data. Minimal IT investment.



The healthcare industry maintains the highest standards for technical compliance and data security, which is why we've made it a priority for our products from Day 1. With the costly, resource-intensive rollouts of on-premise technologies at most facilities, we've created low-cost, cloud-based technology that requires minimal time from your IT team for implementation and ongoing support, both of which are included in our subscription cost.

Implementation & Interoperability

We know that your hospital IT department's time is valuable, so we made sure NurseGrid's cloud-based solutions allow for fast implementation at low costs and require little to no onsite support.

- **Out of the box implementation:** We can create and grant you access to the solution within 24 hours.
- **Support:** Our Customer Success team is available whenever users have questions via phone, email, and chat, so your IT team will not need to provide any ongoing support.
- **Data import:** Our simple schedule import feature allows nurse leaders to populate the data from their core scheduling software directly into NurseGrid within seconds by uploading a CSV or Excel file.
- **Technical integration:** NurseGrid is designed to operate independent of other software systems; technical integration with existing hospital enterprise systems is not required. If your team is interested in a custom integration, our integrations engineers will work with you to build secure and reliable two-way integration with your existing software at an additional cost.

Security

Protecting customer data is NurseGrid's top priority and we rely on industry-leading Amazon Web Services (AWS) to host our product. In addition, we guarantee:

- **Encryption:** All customer data, whether at rest or in transmission, is encrypted. Data is transmitted with RSA 20489 encryptions and the TLSv1.2 Protocol.
- **Infrastructure:** Encrypted customer data is stored in a Virtual Private Cloud and secured independently from our front-end web application and API.
- **Two-way confirmation:** Required before data is shared between accounts and users.
- **Password protection:** All accounts are password-protected.





Compliance

- **PHI & PII:** Our products do not require PHI or PII. NurseGrid can integrate customized legal warnings to remind users about avoiding PHI in their communications on non-approved technologies.
- **Regular audits:** We use audited third-party analysis tools and system-wide vulnerability tests to evaluate our structure on a regular basis.
- **Service Organization Control (SOC) reports:** AWS backbone infrastructure complies with SOC 1, SOC 2, SOC 3 compliance.
- **Logs:** Web server logs are maintained for a minimum of 90 days.

Reliability

- **Reverse proxy:** We use a reverse proxy to protect our backend servers by ensuring they are not visible outside of our internal network while also providing load balancing for our web applications and APIs.
- **Failover:** Automated recovery and re-deployment scripts to immediately restore data from the most recent backup. We maintain a 24/7 alert system for system failures.
- **Backups:** Backups run daily for 7 days, weekly for 5 weeks, monthly for 1 year, and yearly for 5 years. We maintain a quick restore backup and four separate, geographically diverse, backups on separate remote servers.
- **Adverse events:** Our systems have never crashed, and we maintain industry-leading uptime percentages. Our robust Business Continuity Plan prepares us for continued operation during adverse events.
- **Uptime:** We maintain a 99.9% uptime standard.