Mindray Data Sovereignty and Access Control Cybersecurity Brief

mindray
NORTH AMERICA

Intellectual Property Statement

mindray, MINDRAY and MINDRAY are the trademarks, registered or otherwise, of Mindray in China and other countries. All other trademarks that appear in this document are used only for informational or editorial purposes. They are the property of their respective owners.

Manufacturer’s Responsibility

Contents of this document are subject to change without prior notice.

All information contained in this document is believed to be correct. Mindray shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

Mindray Data Sovereignty & Access Control

Executive Summary

Mindray is committed to safeguarding patient data and ensuring compliance with global data protection regulations, including HIPAA (U.S.) and GDPR (EU). Our approach centers on data sovereignty and robust access control, ensuring that sensitive information remains protected throughout its lifecycle

Regulatory Alignment & Certifications

Mindray’s Corporate cybersecurity program is built on internationally recognized standards, including ISO/IEC 27001 for information security and ISO/IEC 27701 for privacy. Regular third-party HIPAA risk assessments and annual security/privacy training reinforce our commitment to compliance and continuous improvement.

Data Sovereignty

- ☐ On-Premise Storage: Patient data is stored exclusively within hospital-managed environments. No patient data is stored in Mindray-managed cloud or data centers.

- ☐ No Internet Dependency: Mindray devices do not require internet access, minimizing exposure to external threats.

- ☐ Remote Access: Only enabled at customer request for installation, testing, expansion, or troubleshooting. Persistent remote access is not required.

- ☐ Encryption: PHI and PII are protected at rest with AES256 encryption and in transit with TLS 1.2 cryptographic protocol.

- ☐ Network Segmentation: Devices operate within segmented networks to reduce attack exposure.

- ☐ Maintenance: During post go-live support, system logs are anonymized and encrypted, containing no PHI/PII.

- ☐ Maintenance Data Management: During post go-live support, the PHI/PII free logs are stored in Mahwah NJ on a Secure Server isolated from general Mindray network. All log reviews occur on this server via remote login, no data can be removed from this server, and it is automatically deleted after an investigation is completed. ~~completion~~.

- ☐ Secure Decommissioning: Data wiping and factory reset procedures ensure no hospital data remains on decommissioned systems.

Access Control

- ☐ Role-Based Access: Integration with hospital Active Directory enforces secure login, password policies, and session management.
- ☐ Certificate Authentication: All nodes accessing data require certificate authentication using TLS 1.2 cryptographic protocol.
- ☐ Audit Logging: Comprehensive logging of all access events supports traceability and compliance auditing.
- ☐ Data Export: Access to data export is password protected.

Conclusion

Mindray’s approach to data sovereignty and access control is comprehensive, proactive, and aligned with industry’s best practices. By embedding security and privacy into every aspect of our products and operations, we empower healthcare providers to deliver safe, compliant, and resilient patient care.