Mindray Clinician Authentication Service

Identity Management

Traditionally, caregivers were limited in how and where they could view and manage patient information. Clinicians today have adaptable solutions that enhance workflow, providing access to comprehensive patient data from almost anywhere – within the department, facility, even remotely. This greater capability comes at a time when requirements for securing patient data, limiting access according to least privileged principal, and auditing of access are required to ensure the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) compliance.

The Mindray Clinician Authentication Service acts as a bridge extending a hospital's traditional IT authentication technologies into the medical device world. Password management, user access control, verified vital signs, and access audit logs linked to the hospital identity management system elevate the security and compliance of the Mindray patient monitoring system. The Mindray Clinician Authentication Service allows implementation of the policies of today, while simplifying continued evolution as hospital identity management requirements change.

User Access Control

- User Access Control is vital in protecting remote access of data from hospital PCs and mobile devices
- Utilizes User Accounts defined within the facility Active Directory
- Custom medical device role definition with over 22 Rights to select from. Clinical Rights such as "view a patient" or "change an alarm setting", as well as Administrator Rights such as "configure system" and "push software updates"
- Access Rights are assigned by facility and department

Password Management

- Eliminates local, role-based passwords within Mindray devices
- Enables centralized account management
- Adopts hospital password complexity and history requirements
- All authentication is done by the hospital identity management system

Validated Vital Signs

- Eliminates the need to validate vital signs within the EMR, simplifying clinical workflow and improving efficiency
- Enables user authentication at the point of care using login or Imprivata OneSign badge tap
- Data is transmitted to the EMR using HL7 marked as “final”, along with the verification record of the clinician storing the vitals

Audit Logs

- Provides centralized log access across the Mindray Medical Device enterprise
- Audit logs include Login/Logout, Remote Data Access, and Data Export
- Audit logs are exportable for storage outside the Mindray system or for integration into a multivendor report

The Mindray Clinician Authentication Service can be configured to accomplish integration into the hospital system using many of the industry standard common protocols such as LDAP, Secure LDAP, or AD (Kerbose). Additionally, when implementing validated vital signs, Imprivata OneSign Enterprise Single Sign-on can be used. Within the Mindray Enterprise, BeneVision N-Series and ePM Patient Monitors, Accutorr 7 and VS9 Vital Signs, BeneVision TM70 and TM80 Telemetry Monitors, BeneVision Distributed Monitoring System (DMS), CMS Viewer, and Mobile Viewer are supported by the Mindray Clinician Authentication Service.

The Mindray Clinician Authentication Service eliminates the need for local medical device identity management, secures data, enhances workflows, and provides audit logs. These benefits are achieved by leveraging the facility’s identity management system through increased capabilities and security within the Mindray medical device system.

Mindray North America
800 MacArthur Blvd., Mahwah, NJ 07430
Tel: 800.288.2121 Tel: 201.995.8000 Fax: 800.926.4275 **www.mindray.com**