# Cybersecurity Preparedness & Mitigation

## An Essential Priority within the BeneVision Distributed Monitoring System

mindray

## Mindray is committed to protecting patient data and ensuring privacy.

We promote deeply-embedded partnerships with our customers to assist in driving the implementation of strategies to mitigate cybersecurity risk. Mindray North America maintains ISO/IEC 27001:2013 certification, further demonstrating our commitment to industry best practices, risk management, training, and robust security policies and systems for managing corporate, employee, customer, and partner information. Cybersecurity within our products focus on three key areas – **Endpoint Security**, **Patient Privacy** and **Security by Design**.

The digitization of healthcare in the U.S. continues to accelerate. From Electronic Medical Records (EMRs) to millions of connected medical devices, the flow of patient information is increasing exponentially.

With such an increase in the volume and modes of data transmission, there comes a greater vulnerability to cybercrime. As a result, cybersecurity is an ever-growing concern within the healthcare sector.

- Cyberattacks have proven particularly damaging to the healthcare sector. In 2020, UHS suffered a cyberattack compromising 250 facilities nationwide and the VA experienced a data breach that compromised the sensitive information of about 46,000 veterans.[1]
- According to Fortune, an industry watchdog, a ransomware attack in Germany caused network outages that forced a clinic to reroute patients in need of emergency care. One 78-year-old patient who required immediate attention for an aneurysm died after being sent to another city, perhaps serving as the first recorded death linked to a ransomware attack.[2]
- The financial impact on healthcare can be significant. A study outlined in Security, an industry communication, found healthcare companies are incurring the highest average breach cost of any industry, $7.13 million per incidence, a 10% increase over the 2019 study.[3]

[1] https://www.securityinfowatch.com/healthcare/article/21209720/healthcare-cybersecurity-sets-new-course-of-action-in-2021

[2] https://fortune.com/2020/09/18/ransomware-police-investigating-hospital-cyber-attack-death/

[3] https://www.securitymagazine.com/articles/93770-healthcare-cybersecurity-strategy-start-at-the-end

# Endpoint Security

Endpoint security focuses on minimizing the threat of unauthorized access through devices such as laptops, workstations, mobile and bedside medical devices. Mindray starts by reducing the network attack surface by segmenting the network, eliminating unnecessary pathways, and restricting access to communications on the network. Finally, locking down and securing these medical devices is the definitive and core component of Mindray Endpoint Security.

In addition to requiring secure firewalls and antivirus protection for network deployment, Mindray applies Whitelisting and Operating System (OS) Hardening for further safeguarding.  Whitelisting is a security practice that, by design, allows access or privilege to a known user or application and denies this same access or privilege to an unknown user or application. OS hardening is the process of making the operating system more secure. This is done through various steps such as removing unnecessary services, executables and registries from the operating system, while aggressively blocking unneeded ports.

One of the most challenging aspects of Endpoint Security for healthcare institutions is the staggeringly high number of devices requiring safeguarding.

Mindray alleviates this challenge by providing Endpoint security coverage for Mindray devices deployed within the BeneVision Distributed Monitoring System.

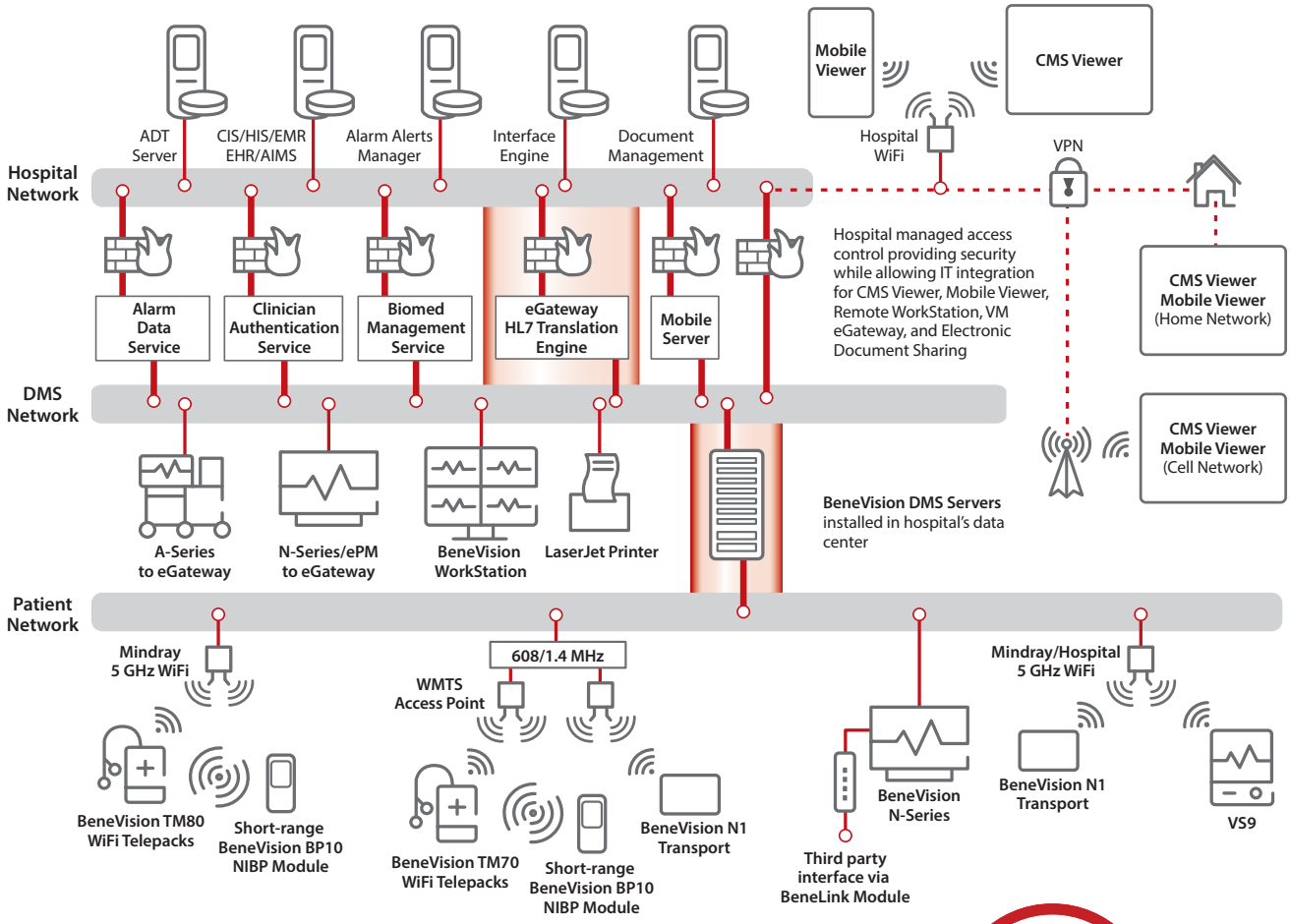
Mindray's approach to protecting PII incorporates secure encryption, password management, and secure data deletion.


## Patient Privacy

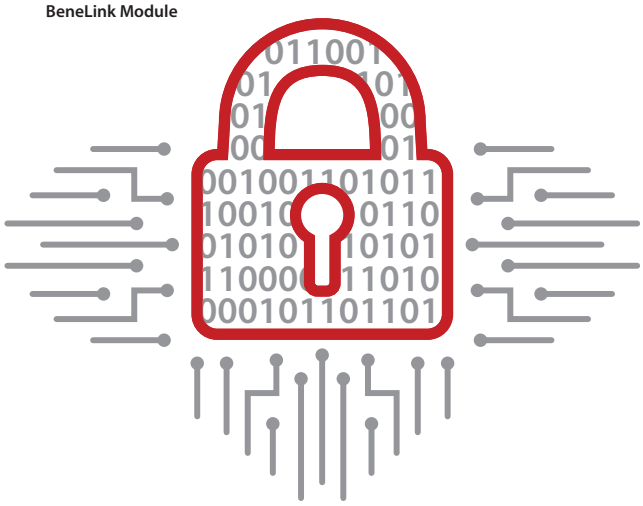
Since 1996, compliance with the Health Insurance Portability and Accountability Act (HIPAA) has been a mandate for all hospitals. Since its introduction, the associated terms have evolved some — electronic Patient Health Information (ePHI) has morphed to Personally Identifiable Information or PII. This shift in language reflects a broadened definition of any data that can establish identity. PII can be either non-sensitive or sensitive. Non-sensitive PII might include data found in a phone book or a government listing. Sensitive PII is data that, when disclosed, could violate an individual's privacy and potentially cause harm. This is PII that must be securely protected for the sake of patient privacy.

The BeneVision Distributed Monitoring System (DMS) utilizes user access controls and customized screen configurations to support patient confidentiality. Data displayed on the screen or in reports is configurable to limit patient information. Patient data is securely encrypted on the DMS Servers and in transit. Logs obtained for troubleshooting are extracted without PII or encrypted to protect patient information. Lastly, Mindray integrates with the hospital's Active Directory to centrally manage user accounts, rights, and permissions to comply with secure password policies. When deployed simultaneously, these various strategies prove effective in supporting patient privacy.

# Security by Design Throughout the Network




This type of security focuses on elements that are inherent in the device or system with the explicit purpose of maintaining security. It all starts during product development, where security risk management, security design practices, and security code analysis are performed. Rigorous testing such as Fuzz testing repeatedly bombards a computer application with erroneous random data to look for system crashes and memory leaks. Data obtained from this type of testing can identify any system instability in very challenging circumstances so that these instabilities can be addressed in the design phases before product release. Like Fuzz testing, Penetration testing is another automated technique that simulates a cybersecurity attack to identify both vulnerabilities and strengths within a software application or system. Security by design continues well beyond product release; Mindray continuously evaluates patches and security updates to ensure product security over time.



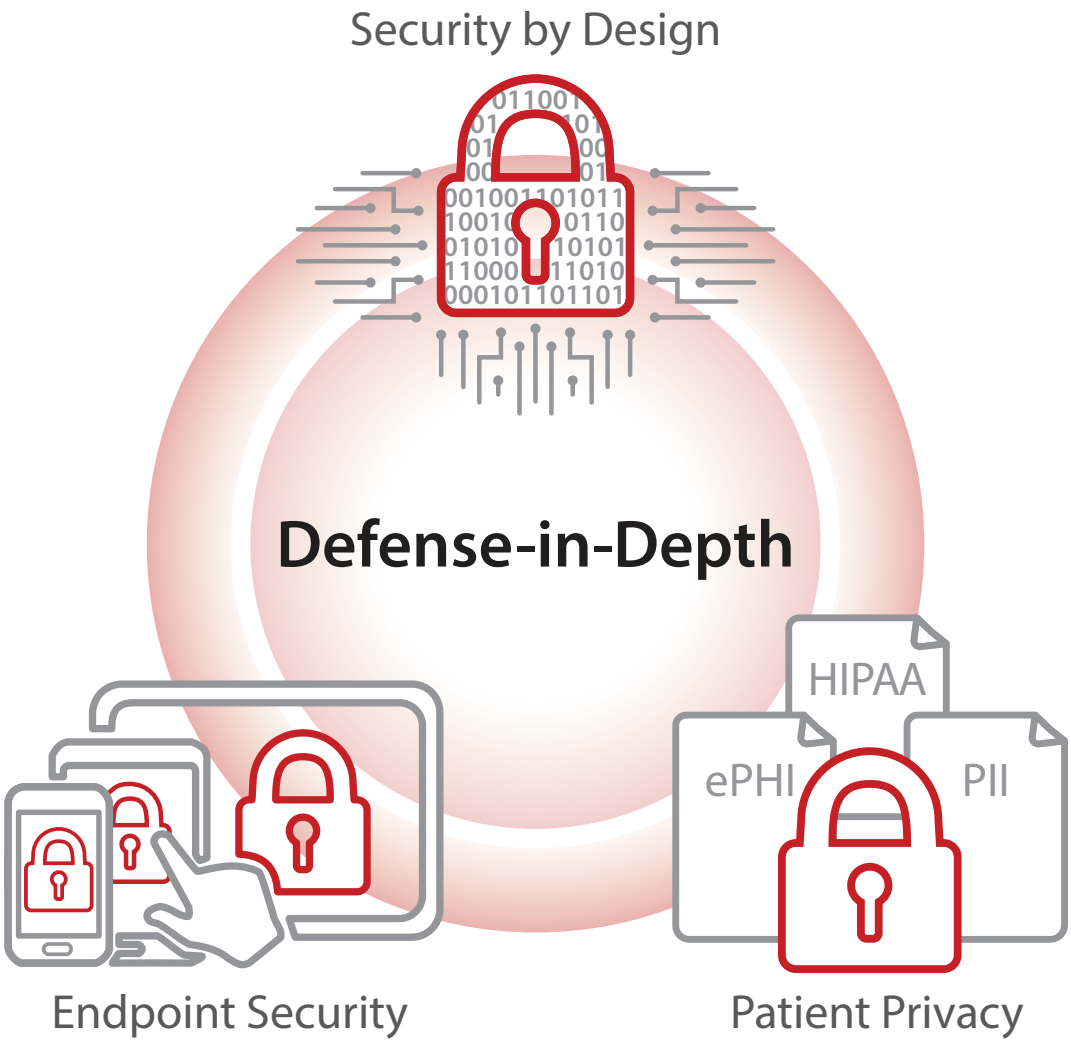
This strategy of Security by Design is indicative of the critical emphasis Mindray places on the security of the BeneVision Distributed Monitoring System and all its associated devices.

# Defense-in-Depth

Mindray's multifaceted cybersecurity strategies can best be described as Defense-in-Depth. There is no single solution for cybersecurity, but rather a series of measures working together in unison to have a net positive effect. All of the strategies described here are methods that complement existing institutional efforts to reduce the incidence of cybercrime.

The Mindray BeneVision Distributed Monitoring System has been designed and developed with a focus on cybersecurity.

Mindray, in partnership with our valued customers, proactively implements these measures and techniques to combat cybersecurity threats and better protect patient privacy.



# Defense-in-Depth Measures within Mindray BeneVision DMS

## Mindray Endpoint Security Components

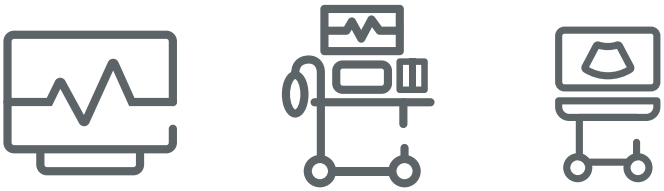
| Component | Description | Endpoint Device |
|---|---|---|
| Whitelist | A program that acknowledges and allows predefined and preapproved applications to access a particular service. A Whitelist is the opposite of blacklist which tracks known malware. | DMS WorkStations, DMS Servers, eGateway |
| Anti-Virus | A program that monitors a computer or network to identify all major types of malware (viruses) and prevent, detect and remove them. | Virtual eGateway, Mobile Viewer |
| OS Hardening | Encompasses all efforts made to make the operating system more secure. This includes removing unnecessary services, executables, and registries while aggressively blocking all ports. | DMS WorkStations, DMS Servers, Patient Monitors, eGateway, Anesthesia |
| Digital Signature | All Mindray software applications provide a digital signature for increased protection. | DMS WorkStation, Mobile Viewer, eGateway, MLDAP, CMS Viewer and eICU Multi-Patient Viewer |
| Encryption | All PII is encrypted with AES on the device at rest and with TLS 1.2 in transit. | DMS WorkStation, Mobile Viewer, eGateway, Patient Monitors, Clinician Authenticatin Services, CMS Viewer and eICU Multi-Patient Viewer |
| Secure Data Deletion | Utilizes built-in tools to securely remove patient data across all Mindray devices | Patient Monitors, DMS WorkStations, DMS Servers, eGateway |
| Firewall | An application or device that effectively creates a barrier, preventing unauthorized communication to pass into a server. | Firewall deployed on Patient Monitors. Windows OS Firewall deployed with DMS WorkStations, DMS Servers, and eGateway. |

## Personally Identifiable Information

| Component | Description | Endpoint Device |
|---|---|---|
| Protect PII on all Displays and Reports | The configurability of BeneVision DMS allows the end user to customize what data is displayed on screen and reports. | Patient Monitors, DMS WorkStations, eGateway, Anesthesia, and Mobile Viewer |
| Protect PII in Logs | All logs used for troubleshooting are extracted without PII or encrypted to protect valuable patient information. | DMS WorkStations, DMS Servers, eGateway, Anesthesia, Patient Monitors |
| Audit Logs | Fully encrypted audit logs available for review. | eGateway, DMS Servers and Mobile Viewer |
| Password Management | The BeneVision DMS supports the use of strong and editable passwords, roles, access timeouts, as well as integration into the Active Directory to adopt hospital policies. | Patient Monitors, DMS WorkStations, DMS Servers, eGateway |
| User Access Control | BeneVision DMS integration into the Active Directory to provide access to centrally-managed user accounts, permissions and password policies | Patient Monitors, DMS WorkStations, DMS Servers, software only eGateway or Virtual eGateway |
| User Account Control (UAC) | UAC can be enabled on a customer managed host running Mindray's HL7 translation engine. | eGateway customer host |
| Protecting Discharge List | BeneVision DMS has the ability to automatically remove patients. | DMS WorkStations, DMS Servers, and Patient Monitors |

## Cybersecurity by Design

| Component | Description | Endpoint Device |
|---|---|---|
| Risk Management | Identification and mitigation of security risk before development and after product release | All Mindray devices |
| Code Analysis | Automated analysis of source code looking for common implementation issues which lead to vulnerabilities. | All Mindray devices |
| Patching Policy | An ever-vigilant approach to monitoring Microsoft® Patch release to shore up vulnerabilities in the Microsoft Operating System | All Mindray devices |
| Fuzz Testing | Automated software testing techniques that subject a software application to intentionally invalid or erroneous messages for the purpose of testing application stability | All Mindray devices |
| Penetration Testing | An automated testing technique that simulates a cybersecurity attack to identify both vulnerabilities and strengths within a software application or system | All Mindray devices |



monitoring | anesthesia | ultrasound

# Your Trusted Partner

We are driven by a desire to provide unyielding service. When you purchase Mindray equipment, you gain access to an entire service organization dedicated to maximizing your uptime and minimizing your total cost of ownership.

The CARE Team is a service organization dedicated solely to ensuring you get the most use out of your equipment. With a dedicated team of clinical technology specialists, field service engineers, and in-house technical support specialists, we are committed to ensuring your systems operate smoothly and provide a timely and effective response when necessary.

At Mindray, your mission is our foundation. You strive to provide patients with the best care possible and rely on outstanding medical devices to provide exceptional care. We were founded on the goal of increasing access to outstanding healthcare by delivering high-quality, technology-rich, accessible medical devices that exceed clinicians' expectations and needs. Together, we can provide better healthcare for all.

## Our Vision

Better healthcare for all

## Our Mission

Advance medical technologies to make healthcare more accessible

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



mindray
healthcare within reach