Mindray Product Cybersecurity Whitepaper

November 2024

Table of Contents

Executive Summary

In the ever-evolving landscape of healthcare and medical devices, the imperative of robust cybersecurity measures cannot be overstated. As the industry continues to embrace technological advancements and digitization, the necessity for secure, resilient, and trustworthy healthcare services and medical devices becomes paramount. This white paper outlines Mindray's comprehensive approach to cybersecurity, detailing the principles, values, and practices that drive our efforts in ensuring patient safety, safeguarding customer data, and ensuring the resiliency and continuity of our device's operation.

The principles and values underpinning Mindray's cybersecurity initiatives emphasize **transparency, accountability, and continuous improvement.** We believe enabling our stakeholders to make informed decision through transparent sharing of security measures implemented in our devices, relevant risk considerations, and sensitive data handling procedures is the key to establishing **trust** and confidence in Mindray. By embedding privacy protection and cybersecurity into every stage of our product development lifecycle, Mindray accountably provides products and services to achieve not only innovation but also resiliency.

At Mindray, a strong **enterprise information security** framework is essential to delivering secure and reliable medical **devices and services.** This foundation is built on the expertise and unified vision of our well-trained **employees,** whose commitment to cybersecurity drives our ability to innovate securely.

Mindray's commitment to cybersecurity transcends mere **compliance** with international standards and regulations. It is about cultivating a culture of security that permeates every aspect of our organization. From the initial design phase to post-market surveillance, Mindray integrates cybersecurity considerations into every step of the product lifecycle. Mindray's **attainment of certifications** underscores our dedication to achieving the highest levels of security and privacy. These certifications are not mere accolades. They are a testament to our relentless pursuit of excellence and our commitment to safeguarding the wellbeing of the patients and their sensitive data entrusted to be handled through our devices.

In the context of **shared responsibility,** Mindray acknowledges that cybersecurity in healthcare is a collaborative effort. We actively engage with healthcare providers, regulators, and other stakeholders to create a secure environment for patient care. This collaboration is essential for identifying potential vulnerabilities, responding to incidents, and enhancing the security posture of the global healthcare environment. By fostering open communication and cooperation, we aim to build a formidable defence against cyber threats.

The pillars of **Mindray Product Cybersecurity Model**—Governance and Risk Management, Secure Design and Development, Protective Measures and Controls, Maintenance and Lifecycle Management, Incident Management, and Data Protection—reflect a holistic strategy that addresses the multifaceted nature of cybersecurity. Each pillar represents a critical component of our comprehensive security framework, ensuring that our devices are not only compliant with current standards but also resilient against future threats.

We understand that the trust placed in us and our devices is a responsibility that we must uphold with unwavering dedication. As we navigate the complexities of the digital age, Mindray will continue to lead with integrity, innovation, and a steadfast dedication to protecting the healthcare community.

Navigating Healthcare Digitization: A Path to Secure Innovation

The medical device and healthcare industry has undergone a significant transformation over the past few decades, driven by rapid technological advancements and digitization. Innovations such as telemedicine, wearable health monitoring devices, and remote diagnostic tools have revolutionized patient care, making it more efficient, accurate, and accessible. Patients now benefit from personalized treatment plans, real-time health monitoring, and minimally invasive procedures, significantly improving health outcomes and overall quality of life.

However, as the industry becomes increasingly reliant on interconnected digital technologies, it also faces heightened cybersecurity risks. The integration of medical devices with hospital networks and cloud-based platforms has created new vulnerabilities that highlight the critical need for robust security measures to ensure the reliability of devices and protect sensitive patient data.

Similar to the WannaCry incident, numerous significant cybersecurity breaches have impacted the healthcare sector in recent years. For instance, the Springhill Medical Center ransomware incident[1] disabled hospital systems, contributing to the death of an infant after critical monitoring systems failed during delivery. The 2020 ransomware attack on the University of Vermont Health Network[2] caused significant operational disruptions, delaying patient care and forcing hospitals to revert to paper records. The Medjack attacks[3] , which targeted medical devices, such as infusion pumps and MRI machines, exploited outdated software and inadequate security measures to gain control and penetrate broader hospital networks. The NotPetya ransomware[4], severely impacted the global healthcare operations through employing the EternalBlue[5] exploits and encrypting critical data and disrupting services. All these incidents underscore the severe impact that cyberattacks can have on healthcare systems, compromising patient confidentiality and disrupting essential medical services.

In light of these challenges, Mindray aims to navigate this path of innovation while achieving a balance between leveraging technological advancements and ensuring robust security in our medical devices. Through the establishment of stringent standards, compliance with international requirements, and promotion of transparency and shared responsibility, Mindray seeks to ensure that the benefits of innovations are realized in a secure and trusted manner, allowing enhanced patient care without sacrificing security.

[1] https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges
[2] https://coverlink.com/case-study/uvm-health-network-ransomware-attack/
[3] https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf
[4] https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
[5] https://www.avast.com/c-eternalblue

Mindray Cybersecurity Position

Recognizing the increasing risk of cybersecurity threats, Mindray is committed to continuously enhancing our processes and systems to integrate cybersecurity and privacy protection into every aspect.

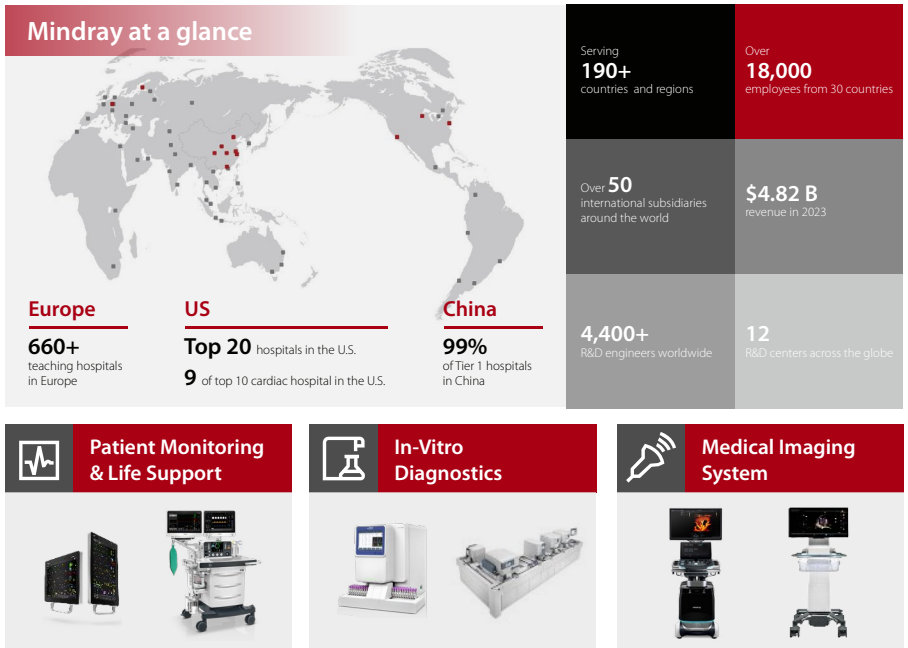
- Lead with Impact
- Secure with Transparency and Trust
- Deliver with Robust Enterprise Security Foundation
- Comply and Uphold With Standard
- Protect in Partnership: Shared Responsibility

Mindray Cybersecurity Position

Lead with Impact

Mindray is a leading global designer, developer, and manufacturer of medical devices and solutions, dedicated to making better healthcare more accessible to humanity. Since its foundation in 1991, Mindray has focused on establishing three primary product lines: Patient Monitoring & Life Support (PMLS), Medical Imaging (MIS), and In-Vitro Diagnostics (IVD).

With corporate headquarter located in Shenzhen, China, and 42 international subsidiaries with branch offices in 32 countries, Mindray has approximately 7,500 employees worldwide supporting diverse healthcare providers and creating values to the society. The company's commitment to innovation is demonstrated by its 12 global R&D centers and an industry-leading investment of 10% of annual revenue into research and development.



Secure with Transparency and Trust

At Mindray, our product security principles and values are rooted in an unwavering commitment to safeguard patient safety, fortify the integrity of our medical devices, and protect sensitive data. Guided by the highest international standards and best practices, we strive for transparency, accountability, and relentless improvement. Our endeavors aim to create a safer, more reliable healthcare landscape, where cutting-edge technology and uncompromised security coalesce to protect and empower those we serve.

" Trust is built when we show not just what we do, but how we do it. Mindray's transparent approach to cybersecurity gives our customers complete visibility into our security practices. By ensuring that our cybersecurity practices are clear and open, we provide our customers with the confidence they need. "

Cheng Minghe
Vice Chairman, Member of Mindray Compliance Committee

"At Mindray, security is built into the DNA of every device we create, ensuring resilience and reliability in even the most critical healthcare environments. Cybersecurity isn't just a feature; it's a core principle that drives the way we design, develop, and deploy every medical device."

Li Zaiwen
Senior Vice President, Member of Mindray Compliance Committee

As a medical device manufacturer in the healthcare industry, the notion of 'Transparency' is at the heart of our principles and values. Our vision transcends mere compliance. It embodies a profound dedication and accountability to prioritize the enablement of informed decision-making by our users. The FDA[6] advocates for clear and open communication about device cybersecurity features and potential risks, in order to build trust with healthcare providers, regulators, and patients. Through diverse forms of information sharing, including whitepapers, user manuals, and technical documentations, Mindray strives to relentlessly improve our commitment to maintain transparency on the implemented security measures, risk considerations, and our methods in protecting patient and handling sensitive data.

By embedding Security and Privacy by Design into our product development lifecycle, we strive to ensure that cybersecurity and privacy are woven into the very fabric of our medical devices from the conception, so to enable unhindered continuity of essential medical services and uphold the sanctity of data confidentiality. Our meticulous risk management framework tirelessly assesses and mitigates potential security threats, ensuring that our devices are not only secure but also resilient and dependable. Through close collaboration with healthcare providers, regulators, and industry partners, we aim to foster a culture of security that reinforces trust and confidence in global healthcare ecosystem.

Security and Privacy by Design

[6] https://www.fda.gov/media/119933/download

Deliver with Robust Enterprise Security Foundation

At Mindray, our approach to cybersecurity permeates our entire organizational ethos, which translates to individual products and services. We understand that a robust enterprise information security of the **Company** is foundational for developing and maintaining trust in us and our devices. Such a strong backbone can only be achieved by well-informed and meticulously trained **People**, who designs and delivers secure and reliable services and **Products**. This comprehensive security strategy that cyclically reinforce our company's security practices, our people's expertise, and our product innovations illustrates the symbiotic relationship necessary to ensure both our enterprise operations and our products are shielded from cyber threats, providing assurance to our customers and stakeholders.

Unified Security Culture: Mindray's corporate culture is built on a bedrock of security awareness and best practices. We foster a security-first mindset among all employees, from the executive suite to the development labs. This culture of vigilance is formed through regular training programs that encompass not only security and privacy by design principles but also broader information security and privacy protection. This robust training regime enables the embedment of advanced security and privacy features into the daily operations and the product designs, fortifying the trustworthiness and compliance of our company and devices.

Resilient Infrastructure: Our enterprise security infrastructure is designed to ensure operational stability and data confidentiality, which are critical for the continuity and reliability of our business operation and customer support. By safeguarding our data centers, networks, and software architectures against disruptions and breaches, we ensure that the systems supporting our product development and maintenance services are always available and secure.

Proactive Incident Response and Continuous Improvement: Mindray's dynamic incident response capabilities and continuous security assessments ensure that we can rapidly address potential cyber-attacks and vulnerabilities, both at the enterprise and product levels. This proactive stance not only mitigates risks but also informs ongoing improvements in our enterprise and product security features, based on real-world data and emerging threat landscapes.

Stakeholder Engagement and Transparency: At Mindray, we strive to maintain an open dialogue about our security processes and developments. By being transparent about our enterprise and product security strategies, we aim to build deeper trust with our customers, assuring them of our commitment to high security standards, patient safety, and the protection of their sensitive information.

Company: Strategic Defense

Maintaining robust enterprise security with comprehensive incident response plans and resilient infrastructure. This ensures operational stability and continual improvement in safeguarding internal systems and data.

People: Empowered Protectors

Through extensive training in security practices and privacy standards, our people uphold and advance our security-first culture.

Product: Secure Innovation

Embedding advanced security features into every medical device from design through development, fostering trust and reliability among our customers.

Comply and Uphold with Standard

At Mindray, we acknowledge and respect the significance and value of adhering to international standards and certifications in ensuring the highest levels of product quality, safety, and cybersecurity. Our commitment to adhering to these standards is not merely for the purpose of legal compliance or obtaining certifications, but to provide our customers and users with a profound sense of trust and assurance. It reassures our stakeholders that we operate with the utmost integrity, ensuring that our products meet stringent quality and safety benchmarks. This sense of trust is crucial in the healthcare sector, where the reliability and security of medical devices directly impact patient care and outcomes. Hence, these standards and certifications serve as a testament to our dedication to ensure the security of our company and products and our efforts in continuous growth and improvement, driving us to constantly elevate our practices.

Relevant standards and requirements that Mindray aligns with include but not limited to TIR57, ISO 14971, ISO 31000, IEC/TR 80001-2-2, FDA pre- and post-market requirements and guidelines, MDCG 2019-16, IMDRF principles and practices, European General Data Protection Regulation (GDPR), US Health Insurance Portability and Accountability Act (HIPAA), or China's Personal Information Protection Law (PIPL). These standards guide our processes, from risk management and cybersecurity to overall product development and lifecycle management. By adhering to these standards, we ensure that our organizational risks are managed and our products are designed, developed, and maintained with the highest levels of safety and security.

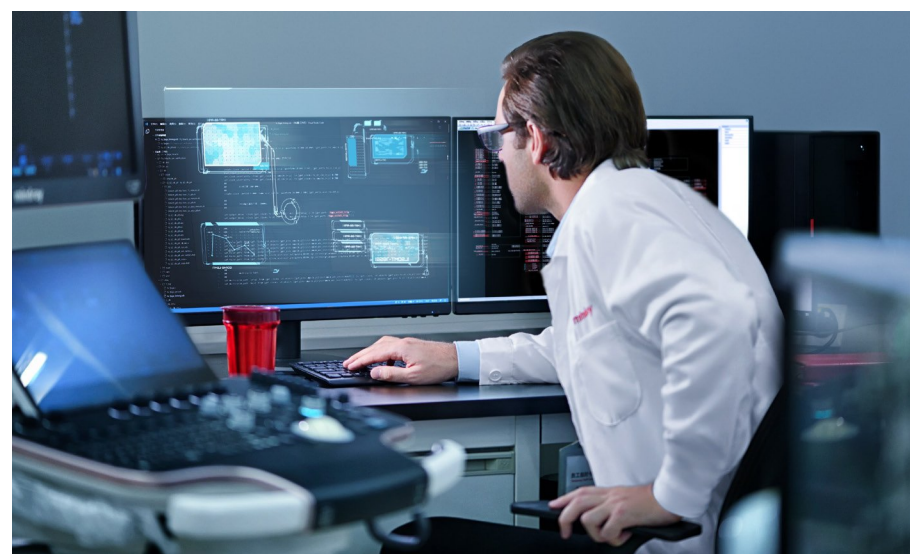
In terms of certifications, Mindray has attained several prestigious recognitions, including ISO/IEC 27001:2022 for information security management and ISO/IEC 27701:2019 for privacy information management. These certifications cover various aspects of our operations, such as R&D, sales, service, IT, and more, ensuring a comprehensive approach to compliance and security. Other certifications also include NEN7510 for healthcare information security, UL2900-2-1 addressing network-connectable devices, etc.

UL Solutions

The applicability of certain standards and certifications depends on the specific product and the marketed regions. For example, applicable FDA requirements are fulfilled on devices in accordance with regulatory pathways and guidance, such as the 510(k) premarket notification. Through thorough research and monitoring, we ensure that our products meet the relevant regulatory requirements based on their intended markets and uses.

By achieving and maintaining these standards and certifications, Mindray strives to demonstrate its unwavering commitment to excellence, to enhance our credibility, and to motivate us to continuously innovate and improve, ensuring that we consistently deliver safe, secure, and reliable medical devices and services to healthcare providers and patients worldwide.

> Our commitment to adhering to these standards is not merely for the purpose of legal compliance or obtaining certifications, but to provide our customers and users with a profound sense of trust and assurance.

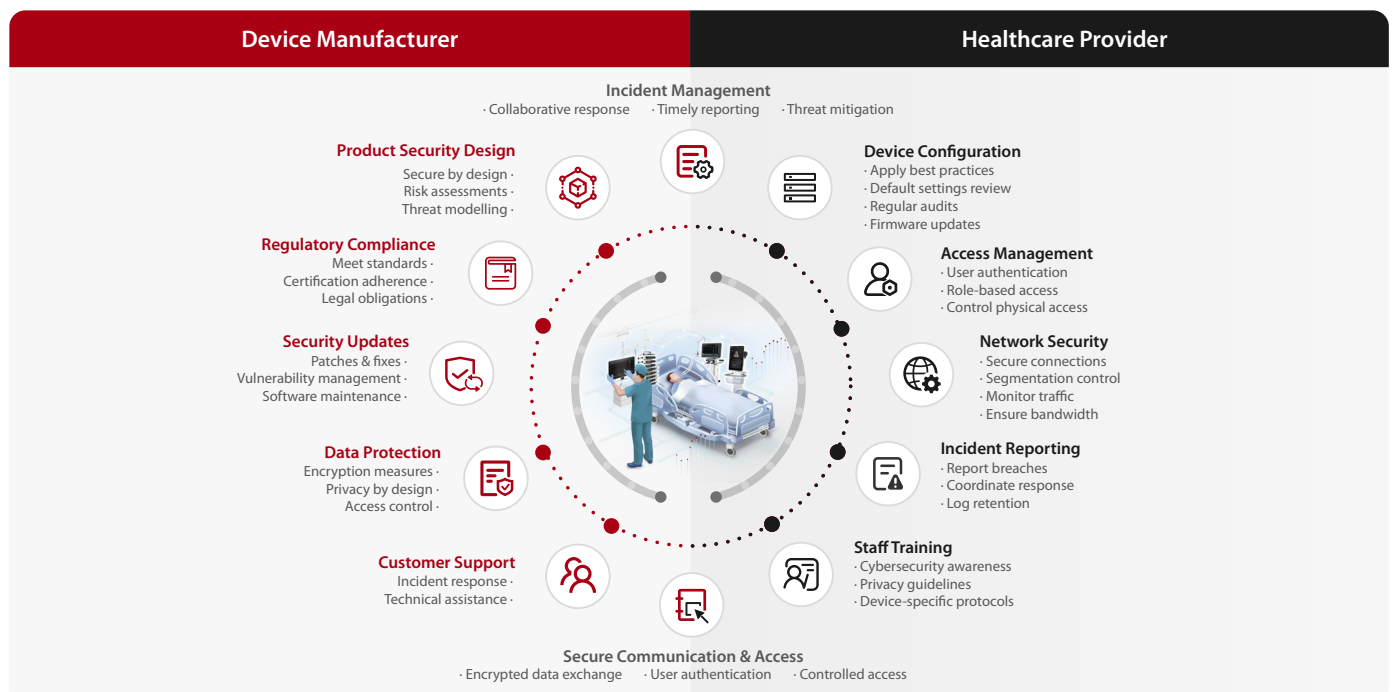


Protect in Partnership: Shared Responsibility

Mindray believes that cybersecurity in the healthcare and medical device industry is a shared responsibility. The interconnected nature of medical devices necessitates collaboration between manufacturers and healthcare providers to ensure robust cybersecurity practices. Device manufacturers are responsible for building secure products by adhering to industry regulations, integrating robust security features during design and development, conducting rigorous testing, and providing timely software updates and patches to address vulnerabilities. They must also offer clear guidelines on secure use of the devices and provide maintenance. On the other hand, healthcare providers play a crucial role in managing the security after the device is deployed within their systems. This includes implementing proper network configurations, controlling physical access to the devices, and continuously monitoring for potential threats. Healthcare organizations must also ensure that staffs are properly trained on security best practices, raise baseline understanding on technical features, and follow protocols to protect both the devices and the sensitive data they handle. Through this collaboration, both manufacturers and healthcare providers contribute to a secure ecosystem, balancing innovation with patient safety and data protection.

This principle is not only advocated by Mindray alone but also supported by numerous research institutions, academia, and industry peers. According to the International Medical Device Regulators Forum (IMDRF)[7], cybersecurity of medical devices necessitates close collaboration between device manufacturers and healthcare providers, highlighting the applicability of shared responsibility throughout the entire device lifecycle. This approach ensures that all parties involved in the use and management of medical devices are equipped to prevent cybersecurity threats, thereby enhancing overall resilience. The FDA[8] further emphasizes that safeguarding from and responding to cyber intrusions is a shared responsibility across the medical device ecosystem, including healthcare facilities, patients, providers, and device manufacturers. This collaboration helps in identifying and mitigating risks, as well as in responding to and recovering from incidents more effectively.

By promoting such notion of shared responsibility, Mindray strives to closely collaborate with all relevant stakeholders, especially the healthcare providers, to well-equip all parties on preventive and responsive measures against cybersecurity challenges, ultimately safeguarding patient health and safety.



[7] https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
[8] https://www.fda.gov/media/119933/download

Mindray Product Cybersecurity Model

Mindray implements a robust framework developed in-house to ensure comprehensive protection of medical devices, guiding and aligning cybersecurity efforts across Mindray's diverse teams and divisions.

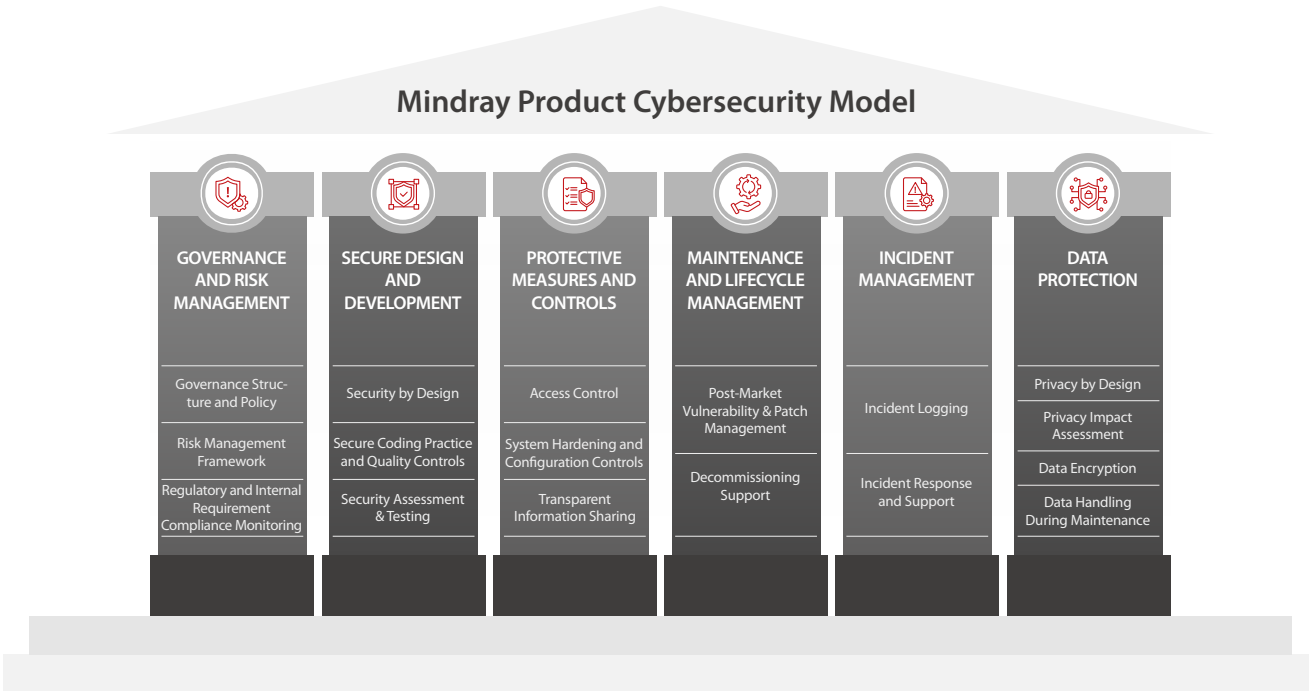
- Governance and Risk Management
- Secure Design and Development
- Protective Measures and Controls
- Maintenance and Lifecycle Management
- Incident Management
- Data Protection

Mindray Product Cybersecurity Model

Mindray's product cybersecurity is governed through the Mindray Product Cybersecurity Model, a robust framework developed in-house to ensure the comprehensive protection of our medical devices, guide and align the cybersecurity efforts across Mindray's diverse teams and divisions. Our model is founded on the principles of the NIST Cybersecurity Framework (CSF)[9], which emphasizes six core elements: **Govern, Identify, Protect, Detect, Respond, and Recover.** By building on this well-regarded foundation, we have tailored our model to address the challenges and requirements of the medical device industry.

The model comprises six pillars and seventeen elements. Each pillar integrates and aligns with international standards and regulatory requirements to ensure thorough coverage of all critical aspects of product cybersecurity.

The Governance and Risk Management pillar ensures a structured approach to managing cybersecurity risks, aligning with industry standards and regulatory requirements. **Secure Design and Development** embeds security practices into the product lifecycle from the outset, leveraging best practices such as secure coding and rigorous testing. **Protective Measures and Controls** implement technical safeguards such as access controls and system hardening to protect against unauthorized access and cyber threats. **Maintenance and Lifecycle Management** focuses on the continuous management of device security through effective vulnerability management and secure decommissioning. The **Incident Management** pillar establishes processes for detecting, responding to, and analyzing cybersecurity incidents, emphasizing the shared responsibility between Mindray and healthcare providers. Finally, the **Data Protection** pillar enables the confidentiality, integrity, and availability of patient data through privacy by design, privacy impact assessment, encryption, and robust data handling controls.



This comprehensive framework is our commitment to maintain robust cybersecurity standards across the company, ensure the safety and reliability of our medical devices, and protect our users and their data. Through this model, we strive not only to meet but exceed global regulatory and industry standards, positioning Mindray as a proactive leader in the field of medical device cybersecurity.

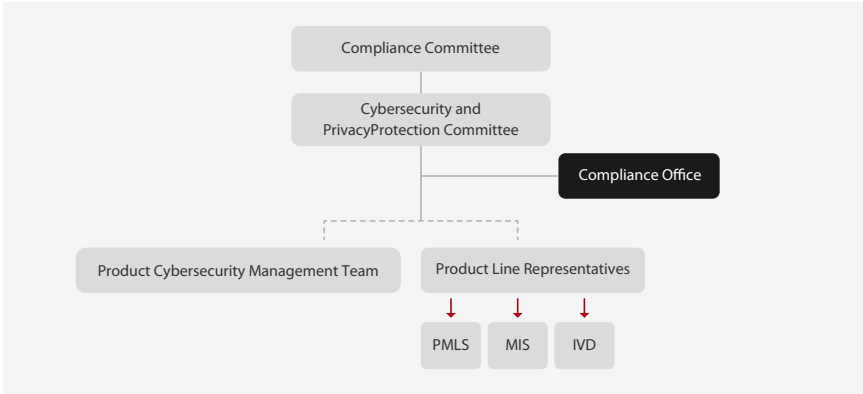
[9] https://www.nist.gov/cyberframework

Governance and Risk Management

Mindray's product cybersecurity is built upon the solid foundation of structured governance policies, risk management frameworks, and compliance monitoring methodologies.

Governance Structure and Policy

Through streamlining the strategic decision-making and policy implementation process, we established clear accountability and communication channels.



The Compliance Committee, composed of the company's highest-level management, guides and supervises the cybersecurity at Mindray. It oversees various areas, including strategies and plans for cybersecurity and privacy protection compliance. The Committee leads the company's overall initiatives and relevant compliance and makes decisions on the major roadmap.

The Cybersecurity and Privacy Protection Committee formulates the company's cybersecurity and privacy protection principles and objectives in both enterprise and product level. This Committee guides and reviews the relevant internal policies and frameworks and manages and supervises the full implementation into business units across regions.

The Compliance Office supports the daily operation of Committees' efforts, keep the team up to date on diverse laws and regulations, and coordinates the formulation policies and frameworks. This office assists the Committees' supervision and audit on the proper implementation of cybersecurity and privacy protection measures, taking the hands-on lead in ensuring the effective adaptation of policies by the business units and departments across the regions.

Product Cybersecurity Management Team plays a crucial role in supporting the committee and compliance office by addressing the technical aspects of device cybersecurity. This team is responsible for establishing internal requirements and standards for cybersecurity. Key responsibilities include identifying, promoting, and applying essential cybersecurity technologies and testing methods, monitoring and assessing vulnerabilities, and providing technical support for research in critical areas like vulnerability response and secure software development

Product Line Representatives, as the front-line entity for product development, is responsible for implementing the requirements and standards formulated by the Committee, the Office, and the Product Cybersecurity Management Team throughout the entire product life cycle, such as development, production, maintenance, etc. They ensure that the established cybersecurity measures are integrated into each product. They also provide timely feedback to the management on cybersecurity-related needs and issues, and cooperate in enhancing the group's overall product cybersecurity management capabilities.

Risk Management Framework

A robust risk management framework is the cornerstone of Mindray's cybersecurity strategy, enabling us to identify, assess, and mitigate potential cybersecurity vulnerabilities in a systematic manner throughout the product lifecycle.

Our risk management framework begins with detailed threat assessments utilizing the STRIDE threat modeling framework, which categorically identifies potential threats related to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This process allows us to comprehensively understand possible forms of threats and assess their potential impact on device security.

Our risk management efforts extend to the establishment of detailed risk management plan, Software Bill of Materials (SBOM), known vulnerability risk assessment, and penetration and scanning test reports. These documents provide a thorough overview of the security measures implemented and serve as a testament to our commitment to product security. The results of these analysis allow us to better design our risk controls that are integrated into specific product security requirements that guide subsequent design and testing phases.

Our cybersecurity risk analysis is not a one-time effort but a continuous process that runs through the entire product lifecycle, thereby ensuring that potential threats are identified and mitigated early and promptly, reducing the likelihood of security breaches post-deployment.

Regulatory and Internal Requirement Compliance Monitoring

At Mindray, regulatory compliance monitoring is a critical component of our cybersecurity strategy, ensuring that the internal standards align with the regulatory requirements and industry expectations. The Cybersecurity and Privacy Protection Committee ensures that regulatory requirements are continually assessed, and any relevant changes are promptly integrated into the product development standards and requirements. To take a step further from minimum compliance, Mindray conducts ongoing research and benchmarking against industry best practices. This proactive approach allows for the company's security measures to be robust and up to date, reflecting the latest advancements and trends in cybersecurity.

To ensure the designed security standards are implemented as intended, Mindray also employs a systematic "R&D Cybersecurity and Data Compliance Matrix" to verify that development and manufacturing practices comply with established guidelines and requirements. This matrix serves as a checklist for internal audits, providing assurance to quality control.

Secure Design and Development

Security by Design

As illustrated before, Security by Design is Mindray's foundational ideology that integrates security principles and requirements from the very beginning and throughout every stage of product development. This core philosophy is embedded and reflected through our robust systems and policies that ensure security specifications are considered right from the start and rooted into the product design culture. The security development lifecycle (SDL) activities are deeply integrated with our overall product development process, guiding us with the best product cybersecurity development practices.

Embedded as a foundation for all our products, a key component of our Security by Design approach is the principle of **Defence-in-Depth.** This multi-layered defence strategy ensures that even if one security measure fails, additional layers of protection remain in place to secure the device and its data.

Secure Coding Practice and Quality Controls

Building on the principles of Security by Design, we have established **comprehensive and systematic secure coding standards** based on International Electronic Commission (IEC) standards, industry best practices, and our extensive software development experiences. Our secure coding standards cover various critical aspects of coding, **including input validation, error handling, and authentication.** These principles allow potential security flaws to be addressed during the coding phase, significantly reducing the risk of carrying vulnerabilities in our final products.

The **process control** and **quality assurance standards** are also key parts of secure coding. Through our **3-step code review procedure,** which include the checklist assessment utilizing the established baseline standards, static code review leveraging advanced tools, and manual human validation, Mindray ensures all software development engineers adhere to secure coding standards throughout the development process.

Additionally, Mindray emphasizes continuous improvement and knowledge sharing among its developers. All developers undergo regular training on secure coding techniques, staying updated with the latest security exploits and mitigation methodologies. This proactive approach ensures that our engineers are well-equipped to address emerging risks.

Security Assessment & Testing

Together with secure coding practices, Mindray conducts robust security assessment and testing to ensure that potential vulnerabilities are identified and mitigated, and implemented security measures are tested and validated.

- **Vulnerability Scanning:**
  Advanced tools are utilized to regularly scan our products and systems for potential vulnerabilities, proactively identifying risks efficiently and apply necessary fixes promptly.
- **Penetration Testing:**
  Simulated comprehensive cyberattacks are conducted to test the resilience of the devices under real-life circumstances.
- **Third-Party Security Assessment:**
  Independent third-party organizations are engaged for security assessments, providing an additional layer of validation and assurance, and ensuring our products meet the industry and regulatory standards.

By integrating rigorous security assessment and testing practices with our design principles, Mindray strives to ensure that our medical devices are secure by design and resilient against potential cyber threats. This comprehensive approach underscores our commitment to delivering secure, reliable, and compliant medical devices, thereby providing confidence to our users in the ever-evolving cybersecurity landscape.

Protective Measures and Controls

Resonating with the notion of Shared Responsibility, equipping necessary security functions and capabilities within medical device configurations is the core responsibility of Mindray as a device manufacturer.

Access Control

Access control, including mechanisms such as **authentication, authorization, and accounting**, is a critical security component for medical devices, ensuring that only authorized individuals can access sensitive information and system functionalities. Mindray's medical devices are equipped with **role-based access control (RBAC)** functionality, which assigns access permissions based on the roles of individual users within the organization. This allows organizations to provide only the minimum access to users depending on their operational necessity, thereby reducing the risk of unauthorized access to files or arbitrary configuration changes.

Mindray devices, while may vary depending on the model, feature several additional protective measures to further enhance access security. These include but not limited to:

Locking Mechanism	After a certain number of continuous incorrect login attempts, the device will be locked, preventing unauthorized access through brute force attacks.
Automatic Logout	To prevent unauthorized access when a device is left unattended, sessions are terminated after a period of inactivity.
Password Management	Mindray devices allow customizable password policies. We also advise users to conduct regular password changes.
Centralized and Secure Authentication	Mindray leverages advanced and secure systems to store credentials and conduct authentication. These systems adopt encryption technology to protect credential data and manage privileges, ensuring authentication is securely conducted and reducing the risk of credential theft or misuse.
Controlled Major Configuration Changes	Major changes, such as operating system upgrade, are controlled with stringent access controls, allowing only authorized personnel to conduct upgrades.

System Hardening and Configuration Controls

System hardening is another critical step to fortify our devices through minimizing the attack surface. Key components of Mindray's system hardening practices, though may vary by model, include:

Operating System (OS) Hardening Guideline	A detailed set of configuration methods and requirements is laid out for various functions of the OS. These requirements ensure that the OS is configured securely in a unified manner across all development teams, effectively implementing the requirements in a structured manner.
Application & Process Whitelisting	Only approved applications and processes are allowed to run on the devices, preventing unauthorized software or activities from executing and potentially compromising the system.
Anti-Virus and Malware Programs	Mindray devices are designed to work seamlessly with industry-standard anti-virus and malware protection programs, ensuring continuous protection against malicious software.
Firewall	Microsoft Windows-based Mindray devices utilize the built-in firewall to restrict external access and control the applications running within the device.
Disabling Unnecessary Risk Vectors	Depending on business needs and circumstances, unnecessary services, ports, and features, such as remote login and USB auto-run, are disabled to minimize exposure to potential attacks.
Kiosk Mode	Devices with Kiosk mode significantly reduces the attack surface by limiting user access to only essential functions, preventing unauthorized activities and minimizing access to sensitive patient information.
Controlled OS and Software Upgrades	The upgrade of the operating system and device software can only be carried out through controlled upgrade packages verified and released by Mindray. Only authorized personnel can perform upgrades and automatic OS upgrades are disabled to prevent unauthorized changes.

Transparent Information Sharing

Mindray strives to relentlessly improve our commitment to maintain transparency on the security measures implemented in our devices. Our key efforts to promote transparency include but not limited to:

Cybersecurity Whitepapers

We provide comprehensive cybersecurity whitepapers for each product line, detailing our security measures, controls, and practices, and offering stakeholders a clear understanding of our cybersecurity efforts. Please contact Mindray for the whitepaper on your particular product.

Product User Manuals

Our user manuals include detailed descriptions and recommendations for the cybersecurity features of our products, allowing users to understand the security mechanisms in place and how to effectively utilize them.

Manufacturer Disclosure Statement for Medical Device Security (MDS2)

Mindray provides the MDS2 upon request, in order to help healthcare providers assess the cybersecurity risks and mitigations associated with our devices. This document outlines the security capabilities of our medical devices, offering transparency about how our products comply with necessary security requirements and operational standards.

Software Bill of Materials (SBOM)

For applicable devices, we also offer the SBOM upon request. The SBOM provides a detailed list of software components used in our medical devices, allowing stakeholders to identify any third-party libraries or dependencies that may pose risks. This transparency is crucial for understanding potential vulnerabilities and maintaining the integrity of the device's software architecture.

Assisting with Deployment Plans

We assist healthcare providers with deployment plans, ensuring that the security features of our devices are correctly integrated into the deployed environment and managed effectively. This support includes guidance on installation, configuration, and ongoing maintenance.

Maintenance and Lifecycle Management

Post-market maintenance underscores Mindray's accountability in safeguarding patient, their data, and the healthcare operations from deployment to decommissioning.

Post-Market Vulnerability & Patch Management

Mindray products use third-party operating systems (OS), such as Microsoft Windows and Linux. To ensure the use of these OS do not pose any risks, we developed **a comprehensive patch management strategy** to continuously monitor relevant vulnerabilities, assess their impact on our devices, and deploy patches to address these issues.

For products running on Microsoft Windows, impact assessment of newly released security patches and hotfixes typically begin within 48 hours of Mindray becoming aware of the new security patch. We assess the impact of patches to determine if patches need immediate application or can be integrated into scheduled updates. For critical patches requiring immediate attention, we provide **detailed operation instructions for expedited updates**. This ensures that urgent vulnerabilities are addressed promptly and securely. In other cases, patches are released within a few weeks and notified to the device users, ensuring users are kept informed and our devices remain protected. For our Linux-based products, we conduct an analysis every six months. Given that Linux platforms in medical devices are usually customized for specific usages, patch release is commonly in a full software update format. If threat cannot be resolved by installing OS patches alone, system software update may be released.

Upgrade packages undergo **checksum validation** before installation. This ensures the integrity and authenticity of the upgrade package, preventing unauthorized modifications. Furthermore, our upgrade process is strictly controlled, allowing only authorized personnel to perform upgrades using a Mindray-developed, password-protected tool. Automatic OS upgrades are disabled to prevent unauthorized changes.

End-Of-Life & Decommissioning Support

While it may vary from markets, we proactively provide customers with detailed **End-Of-Life (EOL) letters** when a product is reaching the end of its serviceable life. These letters include crucial information about the discontinuation of repair services, parts availability, and technical support timelines, allowing customers ample time to plan for replacements or upgrades. This transparent approach ensures that customers are well-informed and can maintain operational continuity while transitioning away from older models, reinforcing Mindray's commitment to excellent service and customer support.

For devices that are to be decommissioned, it is crucial to handle the process securely and responsibly, preventing unauthorized access to sensitive information and ensuring that devices do not pose any risks after they are taken out of service. Mindray assists and enables healthcare providers to securely decommission devices through providing in-person guidance or user manuals on secure disposal practices, such as instructions on data wiping procedure. We also advise healthcare providers in complying with local regulations as well as international guidelines, including those from the FDA and NIST, regarding the disposal of electronic devices, ensuring that decommissioned devices are disposed of in a secure and legally compliant manner.

INCIDENT MANAGEMENT

In the context of the healthcare and medical device industry, incident management is recognized as a shared responsibility. Effective prevention and response to cyberattacks can only be achieved through collaboration between the healthcare providers and the medical device manufacturers. Through below approaches, Mindray aims to foster a collaborative effort in cybersecurity, ensuring that both Mindray and healthcare providers are well-equipped to respond to and mitigate potential security threats.

Incident Logging

Effective incident logging is a crucial element that medical device manufacturers can bring to the table. Mindray's medical devices are equipped with dedicated logs to record security-related operations, providing a comprehensive trail of activities that can be crucial for incident analysis and response. We work closely with healthcare providers in the process of exporting, managing, and analysing the security logs under their specific environments and needs.

Our devices are also designed with diverse data backup and recovery mechanisms to ensure that critical security information is preserved and can be restored in case of any system failures or incidents. This resilience helps maintain the integrity and availability of the security logs and supports ongoing security efforts.

Incident Response and Support

Mindray established dedicated teams to oversee the incident response process and continuously monitor and research emerging incidents that could impact our devices. In the event of a detected or reported security incidents, the teams, in collaboration with the business units, assess risks, design response plans, and implement remediation measures. The 'Cybersecurity Incident Response Guideline' has been established to allow standardized and unified approach across diverse stakeholders. When regulatory reporting is required, we work closely with the relevant authorities to ensure timely and accurate communication. Throughout the entire process, we maintain close communication with our customers, working together to swiftly assess the situation and implement necessary remediation measures to minimize impact and maintain device security.

As additional support capabilities, Mindray's medical devices are equipped with features that enable business continuity even during cybersecurity incidents. While depend on the capability, certain devices employ mechanisms such as backfilling and data synchronization to ensure no critical patient information is lost during network outages. Some devices also feature a layered network design that can isolate risks between the device and the hospital network. Furthermore, by running in redundant wired and wireless network environment, even when one of the network devices fails, the devices can maintain normal operation.

By assisting healthcare providers with systematic incident response and technical support measures, Mindray strives to enable our partners to effectively manage and mitigate cybersecurity incidents and enhance operational resilience.

DATA PROTECTION

Privacy by Design

From the enterprise level, Mindray has benchmarked against international standards and industry best practices to establish a risk-oriented information security and privacy protection compliance management system. This system manages the entire data lifecycle, including collection, transmission, use, sharing, storage, and deletion, adhering to principles of legality, fairness, honesty, openness, and transparency, aiming to protect the **confidentiality, integrity, and accuracy** of all personal data handled in Mindray. Through such robust management system, Mindray acquired ISO/IEC 27001 and ISO/IEC 27701 certifications and is continuously refining its privacy requirements.

Grounded on such enterprise culture and awareness on privacy protection, and with the commitment to protect and respect the privacy and the data of our customers and patients, Mindray has embedded the core principles of "**Privacy by Design**" and "**Privacy by Default**" into the product development process (Please refer to Please refer to the figure in Page 6.). Such principles are incorporated at the early concept and planning stages of product development through the implementation of baseline guidelines for permissions, logging, encryption, and de-identification/anonymization, etc. By embedding privacy protection into the design from the outset, we ensure that privacy measures are not merely an add-on but are integral part of the product architecture, thereby proactively addressing privacy concerns, enhancing user trust, and complying with regulatory requirements.

Mindray strives to embed privacy protection as a core value into very fabric of its product development process.

Mindray's commitment to privacy by design has enabled us to build trust with healthcare providers and patients, allowing the sensitive data of our users to be handled with the highest standards of security and privacy.

Privacy Impact Assessment

For Mindray, complying with data protection and privacy regulations is not merely a legal obligation, but a guiding cornerstone that helps us to mitigate risks associated with data breaches and enhances the trust of our stakeholders. With the aim of comprehensively identifying compliance gaps and risks in privacy and data protection, we introduced the **"Privacy Impact Assessment" (PIA)** into the product development process to ensure that effective control measures are implemented in accordance with relevant compliance requirements. The PIA process involves thorough analysis and documentation of potential privacy risks, followed by the implementation of appropriate mitigation strategies. Such robust assessment and control implementation not only enables Mindray but also our customers to comply with relevant laws and regulations, such as the **GDPR, HIPAA, or PIPL.** We also published a detailed **GDPR whitepaper**[10], which outlines how Mindray complies with one of the most robust international standards for data protection. The whitepaper provides insights into Mindray's corporate governance, internal controls, and mechanisms for handling personal data, demonstrating our dedication to maintaining high standards of data security and privacy.

[10] https://www.mindray.com/content/dam/xpace/en/legal/GDPR.pdf

Data Encryption

Building on the principles of Privacy by Design, data encryption stands as the cornerstone of Mindray's approach to data protection. Data encryption serves as a critical defence mechanism to protect sensitive information from unauthorized access and breaches. Mindray employs comprehensive encryption methods tailored to secure data in transit and at rest. Each product line within Mindray utilizes protocols and methods most suitable to their own device design and specific business needs, ensuring that all data is adequately protected.

Data in Transit

DICOM and HL7 standards are adopted during data transmission, which supports a variety of encryption protocols, including TLS 1.2 with AES-256 encryption. For wireless communication, Mindray devices support WPA/WPA2 Enterprise, which provides robust encryption on data transmitted over Wi-Fi networks.

Data at Rest

While we promote the minimization of personal data logging and storing, under necessary circumstances, Mindray devices implement secure algorithms, such as AES-256, to encrypt data at rest to prevent the misuse of data in case of unauthorized access.

Data on Display

Personally Identifiable Information (PII) on monitor display or in exported reports can be configured to be hidden. This flexibility allows enhanced control over PII access management.

Data Export

For backups to USB, 7z compression with strong encryption is utilized to safeguard archived data, ensuring datasets are securely compressed and stored. Mindray devices also support anonymization and pseudonymization techniques when exporting or backing up sensitive media to hard disks.

By employing advanced encryption technologies and maintaining rigorous data protection standards, Mindray devices allow users to protect data appropriately at all times, whether when it is being transmitted, stored, displayed, or exported.

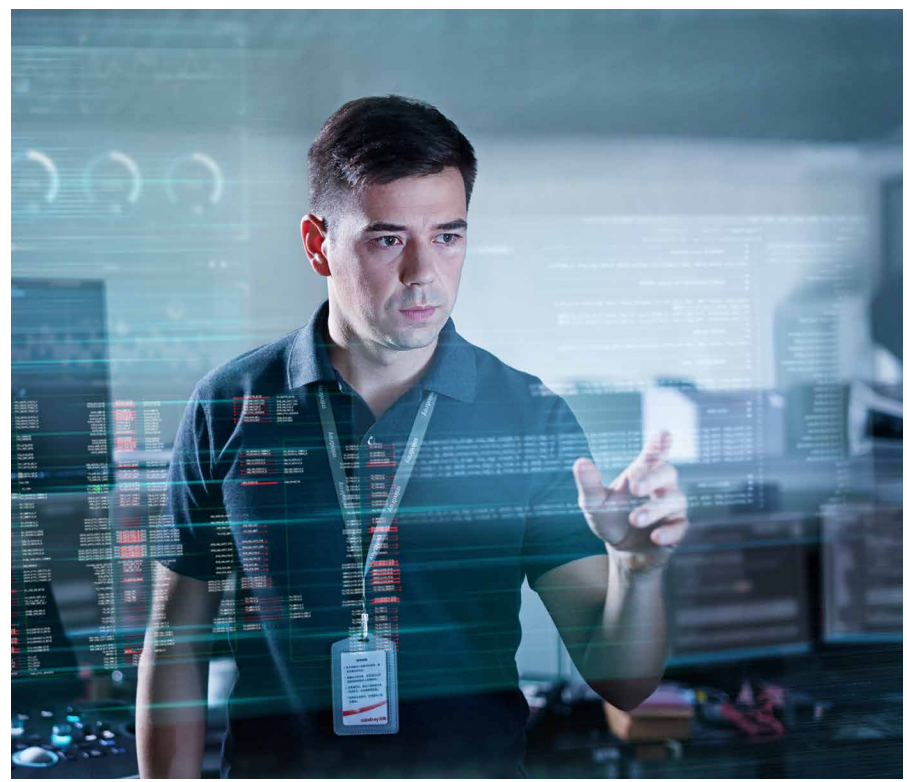
Data Handling During Maintenance

In times of necessary maintenance, devices may need to be accessed by our personnel or be sent to our repair facilities. In case the data on devices is not fully wiped, anonymized, or desensitizes, Mindray has established stringent protocols and robust internal regulations for data handling during maintenance to ensure that sensitive information is properly protected or destroyed to prevent unauthorized access.

Mindray provides comprehensive guidance to healthcare providers on secure data management during device maintenance. A key measure includes secure data wiping capability, which is strongly recommended to ensure that no sensitive information remains on serviced devices.

In each region, local teams serve as the first line of assessment, determining if issues can be resolved at their level. In regions where the return of devices and logs back to China is prohibited, all issues are resolved locally. In cases where returning of devices and logs to China for troubleshooting is not prohibited and is inevitable, the local team conducts a thorough review to confirm that sensitive data has been properly deleted, ensuring compliance with international data protection and cross-border transfer regulations. Alternatively, data desensitization methods may be applied, modifying sensitive information to make it untraceable or unidentifiable while retaining its utility for diagnostics. This can include masking or altering personally identifiable details, with anonymization tests verifying that remaining data cannot be linked back to individual patients.

Meanwhile, our personnel adopt **strict access control measures**, following the principle of least privilege. This ensures that only authorized personnel have access to the device and the data within, and their access is limited to what is necessary for their roles. All in-house or authorized third-party personnel are bound by confidentiality obligations, ensuring that they handle the residual data with the highest level of discretion and security.



In the cases of remote maintenance, Mindray uses secure tools under strict management by the Risk and Control Management Team. Customer authorization is required before any remote maintenance activities are conducted. Furthermore, adhering to the principle of minimal necessity, only the essential data required for maintenance is accessed to minimize the risk of data exposure. Session control and termination procedures are in place to ensure that remote access sessions are securely managed and terminated once the maintenance tasks are completed.

Mindray is committed to maintaining the highest standards of data protection throughout the entire lifecycle of its medical devices. This approach not only safeguards sensitive information but also provides sense of trust and confidence to the users of our devices, resonating with Mindray's dedication to advance medical technology while prioritizing the security of our customers and users.

Closing Remark

As we move forward, Mindray remains steadfast in its mission to advance medical technologies while ensuring the highest standards of cybersecurity. We understand that the trust placed in us and our devices is a responsibility that we must uphold with unwavering dedication. By continually enhancing our cybersecurity measures and staying ahead of emerging threats, we strive to provide healthcare solutions that are not only innovative but also secure.

In conclusion, this white paper is a testament to Mindray's comprehensive and proactive approach to cybersecurity. It underscores our commitment to safeguarding patient data, ensuring the integrity of our medical devices, and fostering a culture of security that is integral to our mission. As we navigate the complexities of the digital age, Mindray will continue to lead with integrity, innovation, and a steadfast dedication to protecting the healthcare community.