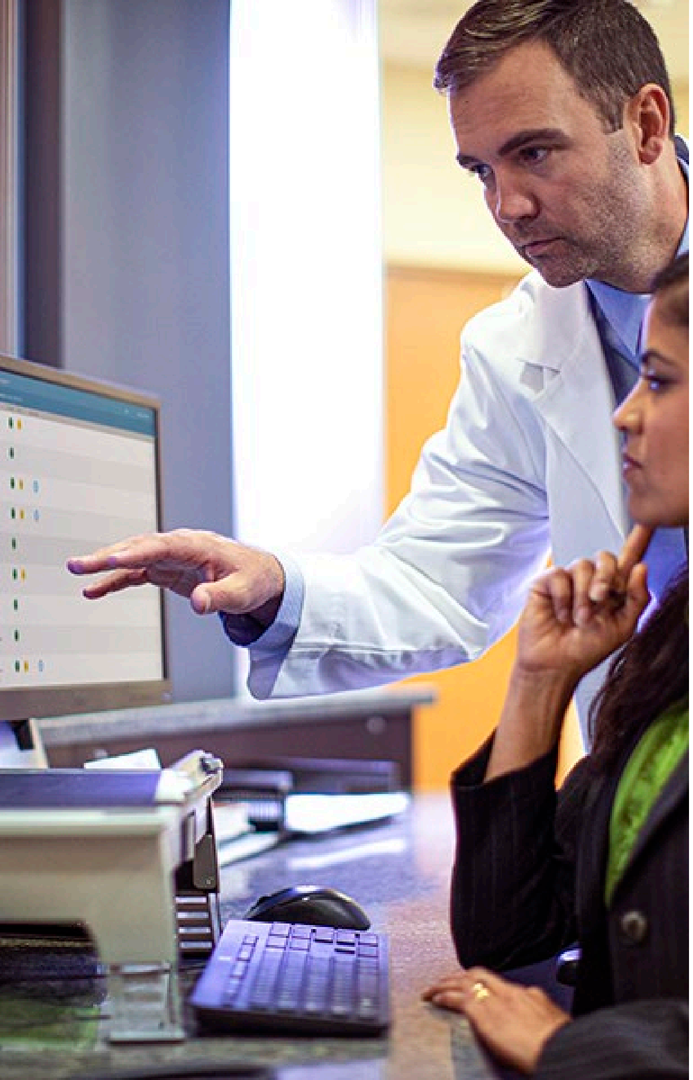
Heartstream

Heartstream and Cybersecurity

We treat cybersecurity as a fundamental responsibility, ensuring that every product, service, and process is built with security and privacy by design.

Table of contents



Why cybersecurity matters in healthcare

Protecting patients. Securing innovation.

Healthcare is one of the most targeted industries for cyberattacks, with consequences that extend beyond financial loss. A cyber incident can disrupt medical device performance, compromise patient safety, and expose sensitive health data. For patients and providers, cybersecurity is inseparable from quality of care.

At Heartstream, we recognize that medical devices are not just technologies — they are life-critical systems. Cybersecurity ensures that our devices perform as intended, data remains private, and healthcare delivery is uninterrupted.

Why it matters for customers

Patient safety and trust	Data privacy and HIPAA compliance	Operational continuity	Regulatory confidence	Defending against evolving threats
A secure medical device ecosystem ensures patients can rely on device accuracy, integrity, and availability without fear of tampering or disruption.	Healthcare generates vast amounts of electronic Protected Health Information (ePHI). We safeguard that data with encryption, strict access controls, and compliance with HIPAA, GDPR, and global privacy frameworks.	Cybersecurity prevents downtime that could delay diagnosis, treatment, or monitoring of patients.	Our cybersecurity program aligns with FDA guidance, ISO/IEC 27001, and NIST standards, helping customers meet their own compliance obligations.	From ransomware to nation-state adversaries, healthcare is a high-value target. We actively monitor, detect, and respond to threats before they impact patients.

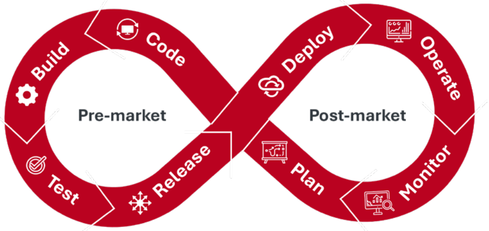
Cybersecurity is not an afterthought — it is the foundation of patient safety, regulatory compliance, and customer trust. That is why we evolve together with cybersecurity and technologies to provide solutions that our patients can rely on.

Security by design in our products

Product security from Day One.

At Heartstream, we follow a Security by Design philosophy. This means cybersecurity is built into our medical devices from the earliest stages of development — not treated as an add-on.

Every line of code, every integration, and every update is evaluated through a security lens to ensure resilience, safety, and compliance throughout the product lifecycle.



Key lifecycle practices

Secure software development lifecycle (SSDLC)	Third-party component assurance	Encryption everywhere	Authentication and access controls	Security testing and validation	Patch and update program
Threat modeling, secure coding standards, automated vulnerability scanning, and code reviews ensure security flaws are addressed early.	All open-source and third-party libraries are vetted, monitored, and updated regularly to eliminate supply chain risks.	Strong encryption protects device data both at rest and in transit, using modern cryptographic standards aligned with NIST guidelines.	Devices implement robust authentication (multi-factor where applicable), role-based access, and least-privilege principles.	Penetration testing, fuzz testing, and ongoing vulnerability assessments confirm device resilience before release.	Risk assessments to identify high risks to our products prioritizing a secure update mechanism to rapidly deploy patches, ensuring devices remain protected against emerging threats.

Customer value

Safety and reliability
Prevents device compromise that could impact patient health.

Compliance assurance
On top of FDA, EU MDR, and other global regulatory expectations for medical device cybersecurity.

Transparency
Customers receive clear product security documentation, and lifecycle support details.

Long-term trust
Security updates and monitoring ensure that devices remain protected well into their operational lifetime.

By **embedding cybersecurity into every stage** of product design, we ensure innovation never comes at the cost of patient safety or trust.

Our information security program

Enterprise-wide security you can trust.

Cybersecurity is not just about protecting devices — it’s about securing the entire enterprise environment that supports them. At Heartstream, our Information Security Program ensures that every system, process, and employee is aligned to protect sensitive data and maintain trust in our products.

Program foundations

Governance and risk management	Policies and controls	Employee awareness and training
Oversight by a cross-functional Cybersecurity Steering Committee, aligning business, regulatory, and security objectives. Risks are continuously identified, assessed, and mitigated in line with ISO/IEC 27005.	A full suite of policies and procedures aligned with ISO/IEC 27001, NIST SP 800-53, and the HIPAA Security Rule. These cover access control, encryption, incident response, vendor management, and more.	Security culture is reinforced through regular training, phishing simulations, and role-based awareness programs. Every employee is a stakeholder in protecting patient data.

Core security capabilities

Identity and access management (IAM)	Cloud security	Data protection	Threat detection and monitoring	Incident response and recovery	Vendor and supply chain security
Centralized authentication, strong MFA, and least-privilege access controls across all platforms.	Secure-by-default cloud architectures with continuous compliance monitoring, log aggregation, and automated alerts.	End-to-end encryption, data loss prevention (DLP) controls, and strict segregation of environments handling sensitive health information.	24/7 monitoring with SIEM, IDS/IPS, and behavioral analytics to detect suspicious activity in real time.	Playbooks tested regularly through tabletop and red-team exercises, ensuring rapid response and minimal disruption.	Third-party providers undergo rigorous due diligence, security assessments, and contractual obligations for compliance.

Customer value

Compliance confidence
Demonstrates readiness for audits and alignment with regulatory frameworks like HIPAA, FDA, GDPR, and ISO/IEC 27001.

Operational resilience
Ensures business continuity even in the event of cyber incidents.

Transparency and assurance
We take customer queries seriously and we encourage our customers to connect with us to know more about our cybersecurity program

Our Information Security Program is a **living system of defense** — continuously improving, adapting to new threats, and ensuring that every interaction with our company is protected. By choosing Heartstream, customers gain a trusted partner that treats cybersecurity as essential to patient safety and healthcare innovation.

Heartstream

© 2025 Heartstream