

Syntermed Vulnerability Disclosure Policy

Version 1.26 | Effective date January 1, 2026

Publication note: Confirm and activate the reporting address, assign a policy owner, approve the response targets, and confirm the MedISAO submission arrangements before publication. Remove this note when the policy is approved.

Purpose and scope

Syntermed, Inc. welcomes reports of potential security vulnerabilities affecting its software and related services. We use coordinated vulnerability disclosure to investigate reports, reduce cybersecurity risks, and protect patient safety and the confidentiality, integrity, and availability of information.

This policy covers Syntermed-developed software, including Cardiac Toolbox (eCTB), NeuroQ, and associated components and services maintained by Syntermed. Reports involving older versions are also welcome; available remediation may include upgrading to a supported version. For software supplied through an OEM or reseller, we will coordinate with the relevant partner. This policy does not authorize testing of systems owned or operated by customers or other third parties.

How to report a vulnerability

Report suspected vulnerabilities to security@syntermed. Use the subject line “Security Vulnerability Report” and identify Syntermed and the affected product. This channel is for security reports; routine support requests should use the normal customer support channel.

Include the product and version, affected component or configuration, a description of the vulnerability, steps to reproduce it, and its potential impact. If available, include a proof of concept, relevant logs or screenshots with sensitive information removed, any known exploitation, and a suggested mitigation. Include contact information if you would like a response and indicate any confidentiality or attribution preferences.

Anonymous reports are accepted, although we may be unable to request clarification or provide updates.

Do not send patient information, passwords, private keys, or other sensitive data in ordinary email. Contact us first to arrange a secure transfer for sensitive technical material or attachments. If the issue involves active exploitation or a potential immediate patient safety risk, clearly mark the report “Urgent” and notify your established Syntermed support contact as well. This reporting channel is not an emergency response service.

Expected response and handling

We will log each report and assign it to the designated product security lead, who will coordinate with engineering, quality and regulatory personnel, and affected partners as needed. Our response targets are:

- Acknowledge receipt within five business days when the reporter provides a usable contact method.
- Provide an initial assessment or request for additional information within ten business days of receipt.
- Provide a status update at least every thirty calendar days while the investigation or remediation remains open, or at another interval agreed with the reporter.

We will assess whether the issue is reproducible, identify affected products and versions, and evaluate exploitability, exposure, data security, and potential effects on clinical performance and patient safety. We may use the Common Vulnerability Scoring System (CVSS) together with product-specific safety and risk assessments. Reports suggesting active exploitation or serious patient safety risks will receive expedited escalation.

For a confirmed vulnerability, we will determine appropriate mitigation or remediation, validate changes, and coordinate delivery and deployment instructions with affected customers and partners. We will communicate the planned next steps and an estimated timeline when available. Resolution times depend on severity, technical complexity, validation needs, and partner dependencies; acknowledgment and update targets are not guarantees of a fix within a fixed period. We will explain material delays and communicate closure or the reason no further action is planned.

Sharing vulnerability information with MedISAO

Syntermed will share confirmed product vulnerabilities and relevant threat information with the Medical Device Information Sharing and Analysis Organization (MedISAO) to support coordinated disclosure and protection of the healthcare community. We may also share credible suspected vulnerabilities before validation when early coordination could reduce risk. Sharing will occur promptly after validation, or earlier when warranted by active exploitation or potential patient harm, and will continue as material findings, mitigations, or remediation become available.

We will submit information through MedISAO's secure reporting mechanism or another secure channel agreed with MedISAO. The submission will identify Syntermed, affected products and versions, the vulnerability and potential impact, available severity information, known exploitation, and mitigation or remediation status. We will provide updates and coordinate the timing and content of advisories as appropriate.

Each submission will include an explicit Traffic Light Protocol (TLP) designation and any additional handling restrictions, consistent with MedISAO's current submission procedure. We will coordinate permitted distribution with MedISAO so that information can reach appropriate stakeholders while protecting confidential details. Patient information, credentials, and unnecessary personal data will be excluded. Reporter identities and nonpublic research details will be protected and shared only with permission or where necessary for handling the report or required by law. We will explain relevant sharing needs to the reporter when practicable.

Coordinated disclosure and customer communication

We ask reporters to allow a reasonable opportunity for investigation and mitigation before publishing technical details that could enable exploitation. We will work with the reporter, MedISAO, affected OEMs or resellers, and other relevant parties to agree on a disclosure plan. Timing will reflect exploitation risk, patient safety, availability of mitigations, and the needs of affected customers. Coordination will not delay necessary safety communications or legally required reporting.

Where appropriate, we will issue a security advisory identifying affected versions, potential impact, available workarounds or updates, and recommended customer actions. We will coordinate a CVE identifier when appropriate. With the reporter's permission, we will acknowledge their contribution. This policy does not establish a paid bug bounty program.

Responsible research

Conduct testing only on systems you own or are expressly authorized to test. Do not test products in active clinical use or interfere with patient care. Avoid denial of service, destructive testing, social engineering, persistence, and unauthorized access to or alteration of data. Limit testing to what is necessary to demonstrate the issue. If you encounter sensitive data or a safety risk, stop testing and report what you observed without copying or exposing that data.

Syntermed supports good faith reporting and will not pursue legal action against researchers for research conducted within this policy and applicable authorization. This commitment applies to Syntermed's actions only and cannot authorize research on behalf of third parties or bind them. Contact us before proceeding if you are unsure whether proposed testing is authorized.

Policy oversight

The designated product security lead owns report handling and coordination with MedISAO. Syntermed will retain records of reports, risk assessments, communications, information sharing, and remediation under its applicable quality and security procedures. We will review this policy at least annually and after significant changes to the products or disclosure process. The published version will identify its effective date and reporting channel.