Natus Neuro
Product Security
Disclosure Statement

Product Security Disclosure Statement

Natus Neuro

This statement describes our position on securing medical products in our customer and patient environments. It also discusses our internal processes and procedures for ensuring that the products we offer are safe, secure, and perform to the highest levels of quality in the industry.

Introduction

At Natus Neuro we understand that the security of our products and services is an important part of our customer's expectations. As such, we are committed to proactively addressing security as an integral part of our medical device design and customer service processes.

To ensure we fulfill our commitment to you, Natus Neuro is in the process of developing and implementing a program to:

- Design, develop, and implement Product Security features and functions in our medical products and services;
- Safely handle the confidentiality, integrity, and availability of any Protected Health Information generated and maintained by the hardware and software products we manufacture;
- Continuously evaluate our products against identified threats and vulnerabilities in medical technology;
- Secure our Global Supply chain through collaboration with trusted business partners; and
- Monitor regulatory and consumer feedback channels to manage security events in the field.

In addition to these activities, Natus Neuro rigorously verifies and validates changes to its medical products to assure that only the highest standards of safety and performance are delivered.

Product Security Activities

Medical Device Disclosure Statements

As part of our commitment to product security and customer service, Natus Neuro provides our customers with detailed information to help assess and address the vulnerabilities and risks associated with products and services we manufacture and deliver.

Specifically, Natus Neurology provides Manufacturer Disclosure Statements for Medical Device Security (MDS²) to provide security information about our products.

Originally developed by HIMSS and the American College of Clinical Engineering (ACCE), and then standardized through a joint effort between HIMSS and the National Electrical Manufacturers Association (NEMA), the MDS^2 provides medical device manufacturers with a means for disclosing to healthcare providers the security related features of the medical devices they manufacture.

The MDS² statements contain product specific security information such as:

- Device Description;
- Management of Private Data; and
- Detailed Product Security capabilities

Product Security Support Organization

Natus Neuro maintains Product Security procedures that are executed as part of our product development process as well as risk assessment and incident response activities for vulnerabilities identified in existing products.

At Natus Neuro, the Product Security Officer is responsible for overseeing the implementation of these procedures, working with business unit product security teams, and reporting compliance status directly to the Natus Neuro executive management team. This organization is also responsible for managing product security incidents and coordination of responses to customers for security related concerns/inquiries.

Security Monitoring

Product security teams within Natus Neuro monitor new security vulnerabilities on an ongoing basis, including those identified by our supply chain partners, internal verification and validation activities, our customers, and other third-parties.

These teams evaluate potential and confirmed threats/vulnerabilities with a security risk assessment and develop incident response plans as necessary.

As part of our ongoing monitoring program, we want to inform you, our customers, of vulnerabilities that may impact your systems and provide timely responses/mitigations where needed.

Depending on the nature of the threat and the affected product in question, a verified and validated patch or software update may be released. If the recommended response requires a change to the software of a medical device, a software update may be released. Information concerning the availability and applicability of such updates is available via the Natus Neuro Technical Service Organization.

Secure Development

Natus Neuro routinely conducts Security assessments to identify potential security vulnerabilities in software driven medical products. This information is used by our engineering teams to define design changes and remediation efforts that will improve our product protection profiles against external threats.

We also work to continuously improve our own internal Information Technology security, including the product development and service delivery environments. This ensures that secure software development is maintained throughout our product development life cycle.

Where applicable, Natus Neuro utilizes secure coding practices based upon current industry standards to deliver high security assurance of the medical device software we develop and maintain. Natus Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code.

Security Inquiries

Customers with specific product security questions or concern may send an e-mail to natusneurologyproductsecurity@natus.com or contact their Natus Neuro Technical Service Representative for further assistance.