COORDINATED VULNERABILITY DISCLOSURE STATEMENT

Remington Medical, Inc. (RMI) understands the importance of cybersecurity and how it is an integral component of what it means to deliver safe products and services. We also acknowledge the importance of work performed by security researchers and customers, with respect to unsolicited, proactive vulnerability identification and proposed risk mitigation. The collective goal of security researchers and RMI should always be to reduce risk.

If you believe you have identified a potential security vulnerability in one of our commercially available devices, please contact us at **quality@remmed.com**.

REPORTING PRE-REQUISITES

Security researchers must adhere to the following:

- Ensure submissions do not contain sensitive information, such as Patient Health Information (PHI) or Personally Identifiable Information (PII);
- Do not test RMI products in clinical settings or other active environments where they are used for any type of patient diagnosis, treatment, care or monitoring, or could inadvertently be used in this way;
- Do not use a vulnerability to take disproportionate action,
- Do provide us with details of communication with regulatory organizations or other third parties about any discovered vulnerability, without delay.
- Do not disclose vulnerability details to the public before a mutually agreed-upon timeframe has expired;

IMPORTANT: We encourage you to coordinate with us public release dates for information on discovered vulnerabilities. We ask that you do not disclose vulnerability details to the public before this mutually agreed upon timeframe expires. Please inform us of your disclosure plans, if any, prior to public disclosure.

WHAT SHOULD BE SENT TO RMI:

Your contact information including; name, organization name, email address and phone number.

Technical description of the concern or vulnerability, including:

- When, where and how you obtained the product.
- What RMI product it impacts, including; exact model, serial number as well as firmware / software version (if known).
- Whether you were able to access any protected health information or other sensitive information. Please do NOT include any protected health information or other personally identifiable information about others in your email submission.

- Any additional information regarding possible or theoretical impact to patient safety if the vulnerability were to be exploited
- Any additional information you think will be helpful to us, including details on the testing environment and tools used to conduct the testing.
- Any intentions for public disclosure.

Reports should only be submitted in English.

WHAT YOU CAN EXPECT FROM RMI:

We will acknowledge receipt of your message within five (5) business days; and inform you of the contact person within our organization.

An appropriate member of RMI may reach out to you to:

- Better understand what you've found,
- Confirm technical details,
- Request additional information,
- Communicate an expected process and timeline.

We may notify that the reported vulnerability is not accepted due to not meeting requirements or provision of enough details;

- Once sufficient information has been collected, we will:
- Investigate the potential vulnerability.
- Conduct a risk assessment to determine appropriate action and remediations.
- Communicate throughout the process, with clear expectations on timeline.
- Communicate our final conclusion.

Once determined, we will provide you with a summary of our findings.

We may provide public recognition for the security researcher (if requested) and if the report results in a public disclosure.

WHERE NECESSARY: RMI may request a neutral third party to assist in resolution of the report. By submitting a report, you acknowledge that RMI may use, in an unrestricted manner (and allow others to do the same), any data or information that you provide to RMI. Your submission does not grant you any rights under RMI intellectual property or create any obligations for RMI.