# Relay Announces Engagement with Canadian MedTech Leader, StarFish Medical, to provide Cybeats Integrated Security Platform for Connected Medical Devices

TORONTO, July 22, 2021 (GLOBE NEWSWIRE) -- Relay Medical Corp. ("**Relay**" or the "**Company**") (CSE: RELA, OTCQB: RYMDF, Frankfurt: EIY2) announces an engagement to provide the Cybeats integrated cybersecurity platform to StarFish Product Engineering Inc. ("**StarFish Medical"**), the largest medical device design consultancy in Canada.

Cybeats is a robust cybersecurity system that uses a proprietary approach to protect connected devices against cyber-attacks. Under the engagement, Relay will provide the Cybeats cybersecurity platform to StarFish Medical for high-valued connected medical devices. The purchase order includes an annual subscription to Cybeats' Software as a Service (SaaS) solution for IoT security and embedding the Agent Integration. The agreement includes the right for StarFish Medical to apply the Cybeats SBOM software to monitor security of the products they design. The SBOM cybersecurity can also be licensed by StarFish clients for continued protection.

StarFish Medical is Canada's leading medical device design, development and contract manufacturing company with ISO 13485 certified engineering and finished manufacturing services. StarFish partners with many successful innovative manufacturing companies to create breakthrough products for several medical specialty areas.

"Our new contract with StarFish, a globally recognized medical technology company, aims to address the market demand for medical device cybersecurity and regulatory compliance - a market we believe is at an inflection point," said Yoav Raiter, CEO of Relay Medical. "Medical systems are now the target of cyber-threats and the integration of North America's leading medical device design companies with our Cybeats cybersecurity solution is a significant endorsement. As regulators worldwide, including the U.S. Food & Drug Administration, recommend cybersecurity standards and guidelines, Cybeats intends to establish a leading role in medical device cybersecurity through a robust and cost-effective cybersecurity defense solution."

Cybeats Integrated Cybersecurity Platform has been designed for securing the internet of things (IoT) and other connected devices. The proprietary approach to cybersecurity starts with a trusted device profile that defines the normal behavior of a device and adds a device sentinel which sits on each device, identifying any abnormal behavior that might be a cyber-attack. Traditional cybersecurity technologies are designed to protect information technology systems running in a data center, but not connected devices. If a device becomes infected, the only remediation is to quarantine and potentially create downtime of the device. This is costly and unacceptable for mission critical applications, like the ones found in healthcare delivery organizations or utilities, that require uninterrupted operation of their devices.

StarFish Medical will be collaborating with Relay to conduct a Regulatory Product Offering and Medical Device Compliance Software Review. This comprehensive review includes a validation package for the cybersecurity solution to support client applications for medical device regulation.

John Walmsley, VP of Strategic Relationships explains the value, "By using Cybeats cybersecurity solution, we are able to build secure and protected devices that meet strict security standards and government regulations, while eliminating downtime of a connected device that may have been infected. It streamlines the process of building a secure device to accelerate time to market, all while managing and maintaining devices so they continue to be secure once deployed."

Validation procedures are a key component to receiving regulatory approval, such as FDA and Health Canada, for new medical devices before they can be sold. Cybeats will collect and manage exhaustive certification data necessary for medical device manufacturers to submit for regulatory approval. The Company expects that providing a comprehensive validation package report will ease adoption and reduce development time for new medical devices implementing the Cybeats integrated cybersecurity platform.

**Important Developments: FDA and SBOM**

Due to the recent increase in cybercrime attacks on health care systems amid the COVID-19 pandemic, there has been a greater emphasis on the importance of connected operational technology and connected devices. 2021 cybercrime examples include the Iowa-based Peoples Community Health Clinic (PCHC) notified patients about a recent cyberattack which may have impacted patients' private information,[1] and New Jersey-based Bridgeway Senior Healthcare faced a ransomware cybersecurity attack that affected large amounts of patient data.[2]

In May 2021, the U.S. Food & Drug Administration outlined recommendations for cybersecurity standards and guidelines to enhance software supply chain security. The FDA states that increasingly common ransomware attacks on healthcare "highlight the ungraceful failure of perimeter-based firewalls and the safety consequences of not separating operational technology from information technology by design."

On July 12, 2021, U.S Regulators stated new software minimum requirements that apply to software on IoT devices.[3] This news follows the Executive Order (EO) on Improving the Nation's Cybersecurity,[4] as President Biden identified the prevention, detection, assessment and remediation of cyber incidents as a top priority of his Administration. The Commerce Department and National Telecommunications and Information Administration (NTIA) were directed by the EO to publish the minimum elements for a Software Bill of Materials (SBOM), a key tool to help create a transparent and secure software supply chain.[5]

**Market Opportunity**

The Global Internet of Medical Things (IoMT) market is expected to grow at a CAGR of 18.5% to reach USD $284.5 billion by 2027.[6] The security of these connected medical devices is of critical political and economic importance. Cybeats aims to offer software solutions to target the software security of this rapidly expanding IoT device market. Both the FDA and Health Canada regulate medical device software, such as in Canada's 2019 guidance document for Software as a Medical Device (SaMD)[7] where it states that medical device manufacturers shall perform continuous analysis of possible vulnerabilities existing in devices.[8]

The Company announces that it has granted an aggregate of 6,000,000 options to purchase common shares of the Company at $0.25 per common share and expiring five (5) years from the date of grant, to certain officers, directors and consultants of the Company.

**SUBSCRIBE**: For more information on Relay or to subscribe to the Company's mail list visit: https://www.relaymedical.com/news

**About StarFish Medical**

StarFish Medical provides award-winning design, development, and flexible manufacturing outsourcing services —100% dedicated to the medical device and life science marketplace. StarFish Medical partners with innovative companies to create and manufacture breakthrough products for a full range of medical specialty areas including: Digital Health, Cardiovascular, Neurology, Urology, Gastroenterology, Otology, Ophthalmology, and In Vitro Diagnostics. StarFish Medical's technical expertise includes electronics, mechanical, software/firmware systems engineering, in addition to industrial design and human factors. Regulatory Affairs (RA) and Quality Assurance (QA) consultants at StarFish Medical provide regulatory assistance for FDA, CE Mark and Health Canada submissions. Services include QA support for setting up QMS for start-up companies with implementation at the client's site, and assisting with ISO 13485 certification audits.

Website: www.starfishmedical.com

**About Relay Medical Corp.**

Relay Medical is a technology innovator headquartered in Toronto, Canada focused on the development of novel technologies in the diagnostics and AI data science and IoT security sectors.

Website: www.relaymedical.com

**Contact:**

Destine Lee
Media & Communications
Relay Medical Corp.
Office. 647-872-9982
TF. 1-844-247-6633
Media Inquiries: media@relaymedical.com
Investor Relations: investor.relations@relaymedical.com

**Forward-looking Information Cautionary Statement**

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the technology described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Additional information identifying risks and uncertainties that could affect financial results is contained in the Company's filings with Canadian securities regulators, which filings are available at www.sedar.com

[1] https://healthitsecurity.com/news/patient-info-exposed-in-health-clinic-cyberattackdata-breach

[2] https://healthitsecurity.com/news/ransomware-extortion-threat-actors-post-data-from-4-healthcare-entities

[3] https://www.ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

[4]https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] https://www.ntia.gov/blog/2021/ntia-releases-minimum-elements-software-bill-materials

[6] https://www.prnewswire.com/in/news-releases/internet-of-medical-things-market-to-reach-us-284-5-billion-by-2027-globally-cagr-18-5-univdatos-market-insights-850218832.html

[7] https://www.pharmainbrief.com/2020/01/health-canada-provides-guidance-on-regulation-of-software-as-a-medical-device-samd/

[8] https://www.regdesk.co/canada-cyber/