ottobock.

Cybersecurity & Data Privacy Statement

At Ottobock, we recognize the critical importance of cybersecurity in safeguarding sensitive information, particularly in the healthcare sector. Our commitment to maintaining the highest standards of data privacy extends to the prevention of the unauthorized disclosure of employee, customer, or patient data. This includes a steadfast focus on protecting patient privacy, electronic health records, and overall cybersecurity.

Our cybersecurity measures include, but are not limited, to the following:

- **Patient Privacy**
  We are dedicated to upholding the privacy rights of patients by implementing robust measures to ensure the confidentiality of their health information.
- **Employee and Customer Data**
  The protection of employee and customer data is a top priority. We employ state-of-the-art security protocols to safeguard personal and sensitive information.
- **Access Controls**
  Strict access controls are implemented to ensure that only authorized personnel have access to sensitive data. This includes regular reviews and updates to access permissions.
- **Network Security**
  Our network and cloud infrastructure is fortified with advanced security technologies to detect and prevent any unauthorized access, ensuring the integrity of our systems.
- **Cybersecurity Training**
  All employees undergo regular cybersecurity training to stay informed about the latest threats, best practices, and the importance of data protection.
- **Incident Response Training**
  Our team is equipped with the knowledge and skills to respond swiftly and effectively to any cybersecurity incidents, minimizing potential damage.
- **Legal Compliance**
  We strictly adhere to all relevant data privacy regulations, including but not limited to HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation).

- **Regular Assessments**
  Periodic assessments are conducted by 3rd-party-experts to ensure ongoing alignment with our cybersecurity standards and regulations.
- **Monitoring and Adaptation**
  We are continuously monitoring our infrastructure as well as the cybersecurity landscape, adopting proactive measures to address emerging threats and vulnerabilities.
- **Feedback Mechanism**
  Employees and cybersecurity specialists are encouraged to report any security findings or concerns, fostering a culture of shared responsibility for cybersecurity.
- **Transparency and Communication**
  In the event of a data breach or security incident, we are committed to transparently communicating with affected parties, including patients, employees, and customers. Clear communication and swift resolution are paramount in maintaining trust.

This Cybersecurity Statement reflects our dedication to the highest standards of data privacy and cybersecurity. We understand the gravity of the risks associated with the unauthorized disclosure of employee, customer, or patient data and remain unwavering in our commitment to mitigating these risks to the best of our ability.

Duderstadt, January 12, 2024

Martin Böhm
CXO