OUR COMMITMENT TO CYBERSECURITY

Data technologies are transforming modern medicine. The growth of connected medical devices, products, diagnostics platforms and systems provides healthcare professionals and their patients smarter and more effective treatment. The ability to analyze large amounts of healthcare data allows scientists and providers to unlock potential solutions to some of the most difficult healthcare challenges we face.

The values of patient safety and integrity long associated with healthcare require a strong focus on cybersecurity to protect the promises inherent in an interconnected, data-driven healthcare model. At Abbott, we create and provide products, devices, and systems that help people live their best lives through good health. Our goal is to ensure our devices, products, and systems meet the highest security standards and that commitment governs how we approach cybersecurity across our business.

To protect the devices, products, and systems that connect patients to healthcare professionals and institutions, we take a broad and deep approach to ensuring safety and security. Our cybersecurity program is built on four pillars. Because technology and threats continue to evolve, we are constantly evaluating and adapting security measures with the goal of ensuring our patients receive the highest quality care.

Cybersecurity-embedded design – When we develop new products, or update existing products or systems, we conduct a cybersecurity review and analysis to ensure that we are actively considering security and including appropriate control measures as we build our products.

Constant threat and risk analysis – Threats and associated risks continue to evolve. Through collaboration with external experts, information sharing agreements with specialists in the healthcare and cybersecurity fields, and our continuing analysis, we quickly identify new threats and deploy cybersecurity controls to improve patient safety.

Testing by internal and external experts – To maintain the trust of our patients, we use a regular testing program to ensure that our devices, products, and systems are appropriately aligned with current cybersecurity standards.

Partnering with industry – The risks posed by cyberattacks are felt by the entire industry. Working together with industry partners, including security experts, academic institutions and the research community, we are able to assess trends, share

threat information, and establish standards that protect patients. Working together on cybersecurity challenges is critical to maintaining patient trust in our industry.

DATA PROTECTION

Abbott's privacy policy sets out our commitment to our patients around the collection and use of patient data. Our cybersecurity program protects not only our products, but also the data we collect and use to improve healthcare outcomes. In addition to the four pillars above, we also use data-specific protections to live up to the trust our customers place in us, such as encryption protocols and strict controls around anonymization.

CYBERSECURITY COORDINATED PRODUCT DISCLOSURE PROGRAM

As part of our commitment to protecting our devices, products, and systems, we have a Cybersecurity Coordinated Product Disclosure Program. The reporting process covers medical devices, software as a medical device, and mobile medical applications. If you have identified a potential security vulnerability or privacy issue with Abbott's devices, products, or systems, please visit our Cybersecurity Coordinated Product Disclosure page here.

PRODUCT SECURITY UPDATES

Access the most recent product security updates from Abbott and its suppliers here.

- Product Security Bulletin: VxWorks IPNet Vulnerabilities
- Product Security Bulletin: Microsoft RDP
- Product Security Bulletin: Meltdown/Spectre