Medical Device Software CyberSecurity Processes, Policies & Protections

Security is paramount.
At Bayer, we leverage more than a century of patient-centered trust in anchoring a security stance that puts vigilance, innovation and data integrity in between you and a risk-filled world.

It starts with world-class innovation.
Bayer is a world-class innovation company focused on improving the health of humans, animals and plants. Bayer directs that innovative energy to transform insight into support for our customers to enable them to provide better patient care and improve productivity in computed tomography (CT), magnetic resonance imaging (MRI), angiography, and positron emission tomography (PET).

Our comprehensive and continually evolving portfolio includes medical devices, contrast media, integrated dose-management software (radiation dose and contrast dose), and equipment service. Customers rely on us for our dedicated partnership and advanced solutions that meet the challenging needs of today's radiology environment.

Software as a security solution.
Bayer recognizes the imperative of patient safety and healthcare data integrity in all its forms. We maintain a cybersecurity function dedicated to developing and evolving cybersecurity requirements as an integral component of our product development lifecycle.

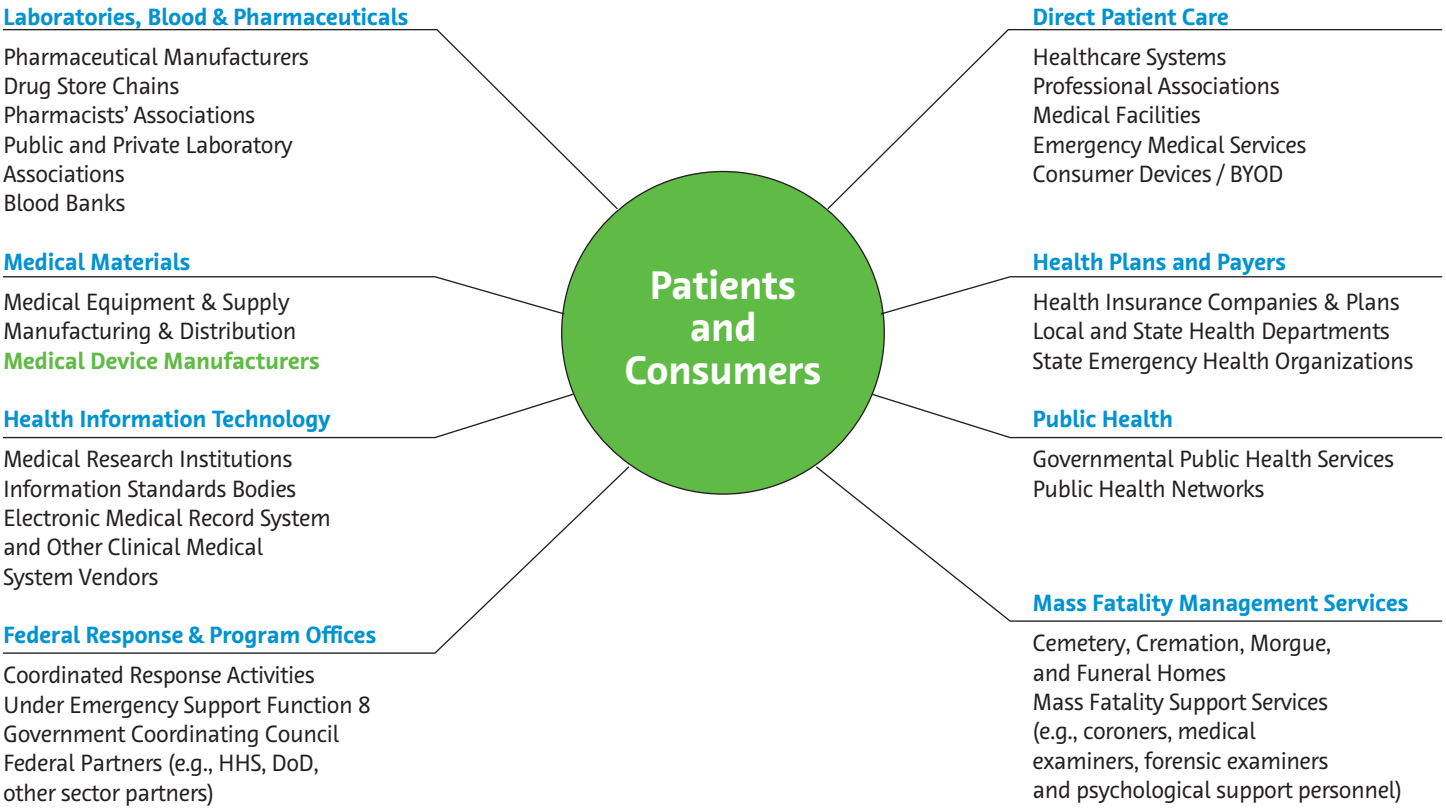
The Medical Device Software CyberSecurity Team continuously monitors and assesses vulnerabilities which are used to inform product design, development, support and implementation. Our processes include continuous monitoring for cybersecurity signals and detailed incident response plans, reviewed and tested annually by the Medical Device Software Incident Response Team to enable coordinated and efficient reaction.

Bayer actively participates on several industry cybersecurity workgroups, including DITTA (Global Diagnostic Imaging, HealthCare IT and Radiation Therapy Trade Association), MITA (Medical Imaging Technology Alliance), and others, and helps to promote patient safety in new legislation and published standards.

CyberSecurity as a shared responsibility.
Healthcare ecosystem stakeholders share responsibility for protecting patients and safeguarding data. Across all industry stakeholders, financial investments in cybersecurity have been steadily increasing. Bayer, as a device manufacturer, invests in infrastructure and developing policies and procedures that support evolving cybersecurity requirements and industry best-practices. At end user sites, cybersecurity protection and defense against the latest attack is strengthened through proper maintenance of networks and environments in which medical devices are deployed. Hospital networks that are monitored and patched quickly provide the first line of defense for deployed medical devices.

The Healthcare Ecosystem

CyberSecurity is a shared responsibility



Bayer process and policies. Responsive. Reliable.

Cyber Response Policy

Bayer maintains a cyber response policy which is designed to facilitate the activities performed in response to a cybersecurity signal with potential impact to marketed and distributed medical devices. The cyber response policy and process ensures appropriate activities are performed with timely escalation in alignment with FDA Guidance on Postmarket Management of Cybersecurity in Medical Devices. It also incorporates concepts from domestic and international privacy laws, regulations and guidelines, as applicable.

Monitoring Cybersecurity Signals

An integral element of the Bayer cyber response process is the ongoing global monitoring for cybersecurity signals. Bayer maintains a testing and monitoring infrastructure, complete with assessment and vulnerability analysis tools, that enables continuous awareness of industry threats and conducts ongoing risk and vulnerability assessments of products in order to determine potential impact. In addition to proactively monitoring for signals, Bayer is also an active member of mission-critical services such as the United States Computer Emergency Readiness Team (US-CERT) and Defense Information Systems Agency (DISA), among others, that provide real-time information via alerts and special announcements.

Commercial Software Monitoring and Patch Management Policy

Some of our products integrate commercially available software components, and Bayer stays current with announcements and releases by performing assessments on the most recently released updates and assessing the potential impact. Through continuous monitoring of third-party components and associated lifecycles, Bayer strives to maintain secure products and to mitigate potential risks as early as possible, in alignment with industry and regulatory expectations.

MDS2, DICOM Conformance and Technical Whitepapers

Bayer maintains "Manufacturer Disclosure Statement for Medical Device Security" (MDS2) documentation for our products, which enables the assessment of the risk associated with electronic Protected Health Information (ePHI) and the mitigation of that risk within our products. In addition, Bayer has developed DICOM (Digital Imaging and Communication in Medicine) conformance statements that enable assessment of our products' capabilities with respect to this industry standard. Bayer also offers technical whitepapers that cover many of our varied product functions, including remote support capability, and provide additional product-specific technical details with respect to security and risk mitigation.

Malware Protection

Some Bayer products are delivered with additional malware protection in the form of a pre-loaded anti-virus application and virus definitions. Other Bayer products offer the option for installation of supported anti-virus software, provided the software is installed and configured in alignment with Bayer recommendations.

VirtualCare™
Remote Support

The VirtualCare™ Remote Support solution.

VirtualCare™ Remote Support solution allows Bayer support personnel to provide secure remote service over the Internet for devices installed behind customer firewalls. The solution leverages secure web services to communicate over the Internet and links the VirtualCare application to a central server hosted in an ISO/IEC 27001:2005 compliant data center. The solution has been designed for high performance and security at every level of its architecture with a goal to provide faster overall recovery time and maximize uptime of Bayer products. Faster response time through remote diagnostics, increased first-time fix rate through diagnosis before dispatch and improved product performance with immediate access to the latest product software and enhancements through remote software updates are a few of the benefits made possible by VirtualCare.

VirtualCare is powered by industry standard technology and provides remote service and monitoring at hospitals, clinics, and laboratories all over the world.

A partnership to rely on.

As technology advances enable faster, more-efficient communication among devices that coexist on more accessible networks, product safety and security continue to be our primary focus. From the development of cyber policies and procedures integrated within our risk management framework, to continuous monitoring for the latest potential threat, Bayer is committed to designing and developing safe, secure products.

Bayer HealthCare LLC
100 Bayer Boulevard
P.O. Box 915
Whippany, NJ 07981
U.S.A.
Phone: +1-412-767-2400
+1-800-633-7231
Fax: +1-412-676-4120

Manufacturer
Bayer Medical Care Inc.
1 Bayer Drive
Indianola, PA 15051-0780
U.S.A.
Phone: +1-412-767-2400
+1-800-633-7231
Fax: +1-412-676-4120

More information on
radiologysolutions.bayer.com

PP-CP-US-0476 February 2018