WHITEPAPER

CYBERSECURITY MEASURES FOR STARLIMS Quality Manufacturing Solution

This whitepaper has been developed for version QM12.0 of STARLIMS Quality Manufacturing Solution, released Jun. 2019. Depending on the version of the product you have procured, there may be differences in the fielded features of the product. In addition, as this whitepaper was created at a point-in-time, changes may have occurred to the Medical Device Cybersecurity Program to address evolution and maturation in the medical device cybersecurity ecosystem.

We understand and we are addressing security across the organization.

The threat of cyber-attacks to medical devices is constantly evolving. With this in mind, we proactively established a Medical Device Cybersecurity Program focused on reducing the cybersecurity risk associated with our medical devices, vigilance towards emerging threats and continuous improvement of product security.

We recognize the importance of incorporating cybersecurity considerations early and throughout our product development process. To accomplish this, we established a cross-functional Medical Device Security Working Group, including representatives from engineering/software development, security, information technology, and quality assurance. This Working Group guides the Medical Device Cybersecurity Program, ensuring that we address cybersecurity considerations throughout the product lifecycle and in our Quality Management System (including through appropriate design controls and risk management).

Our Medical Device Cybersecurity Program was designed, developed, and implemented based on industry best practices, regulatory guidance (e.g., the United States Food & Drug Administration's (FDA) pre and post-market guidance for medical device cybersecurity), and government agency and customer procurement requirements. Additionally, our program has been developed in a way that we can adapt to integrate new elements (e.g., new standards and laws (including the EU's GDPR), guidelines, and practices). We leverage a data protection by design approach for our products and have included our medical device security processes in our Quality Management System to facilitate consistent, high-quality performance across our organization.

Our Medical Device Cybersecurity Program:

- **Security Risk Management:** We proactively manage the cybersecurity risk of products throughout each product's lifecycle. Particular attention is paid to security engineering. Our program involves security risk assessments, product security requirements, technical security testing, and third party component security.
- **Security Event Handling and Incident Response**: Since cybersecurity is a constantly changing landscape, new threats, vulnerabilities, and knowledge must be collected from a number of sources including customer feedback, information from third party component suppliers, and threat intelligence. Security events and incidents must be responded to in a consistent manner and in compliance with regulatory obligations (including HIPAA, US state laws, and the EU GDPR). Our program includes threat intelligence, patch and vulnerability management, and product security information and event management.

- **External Communications:** We value external interaction and communication as an important tool for maintaining a good relationship with external stakeholders and for providing consistent messages on security attributes, vulnerabilities, software updates, and cybersecurity events. Our program involves product security attribute documentation, vulnerability communication, inquiry response, regulatory submission, and security authorization.
- **Security Education and Training:** Our personnel are trained in the skills needed and appropriate to their roles to design, produce, and support secure and safe products. In addition, personnel are effectively trained to fulfill their responsibilities within the Medical Device Cybersecurity Program. Team members attain the required skills or knowledge for their assigned roles through targeted training or classroom learning. Our program includes training on security awareness, secure development, organization processes, and product lifecycle.
- **Program Monitoring:** Processes for monitoring and reporting on the Medical Device Cybersecurity Program facilitate our decision making and improve the performance and accountability of the program. To ensure our program operates as intended, relevant performance-related data is collected, analyzed, and reported to the leadership so that it can be compared to the program's intended goals. Program monitoring enables management to understand the progress, effectiveness, and efficiency of the organization and take corrective action if necessary. Our program includes both continuous monitoring and periodic detailed audits and assessments of performance indicators, product inventory, the program audit framework, and the program assessment framework.

We identify security risks using robust risk management processes.

Abbott is committed to mitigating security risks in the connected medical devices that we design, develop, and maintain. As required by the EU GDPR, we practice a "data protection by design" process and conduct in-depth assessments of our products so that we can implement appropriate risk mitigation measures. We have developed a product risk profiling tool, which allows us to select the most effective level of assessment to be conducted on our products based on the associated risk of the product and its functionality. Based on the risk level identified using the risk profiling tool, as well as the functionality of the product, the below two (2) methodologies are applied.

- **Security Risk Assessment (SRA):** The SRA process is conducted on Abbott's high risk products as identified by our risk profiling tool. Our end-to-end security risk assessment process includes conducting planning and information gathering, identifying applicable product profiles, developing a component register, identifying a security control set and performing a controls analysis, conducting threat modeling, identifying vulnerabilities and pairing with threats, calculating the risk rating of the vulnerability, identifying the additional recommended mitigating controls, and calculating the residual risk rating. The security risk assessment leverages industry-leading practices and security risk management frameworks including, but not limited to, NIST 800-53, NIST CSF, CLSI AUTO11-A2, and ISO 80001. In addition, this assessment process aligns with the NIST 800-30 and the FDA's guidance by providing:
  - Identification of assets, threats, and vulnerabilities
  - A specific list of cybersecurity controls that were considered
  - A "traceability matrix" that links the actual cybersecurity controls to the cybersecurity risks that were considered
  - Assessment of the impact of vulnerabilities on product functionality and end users/patients
  - Assessment of the ability to exploit a threat and vulnerability
  - Determination of risk levels and suitable mitigation strategies
- **Technical Security Testing (TST):** We determine whether to conduct the TST process based on the functionality of the product and its associated risk level as identified by our risk profiling tool. The testing conducted includes both active and passive testing, including:
  - Application Security Testing: application architecture security, common risks in applications, web application and services security testing, security of application transactions, and security of external libraries and application programming interfaces

- Network Security Testing: network services security testing, wireless security testing, and security testing of communication protocols
- Firmware Security Testing: firmware extraction and file system analysis, firmware/patch management analysis, firmware protection security testing, and firmware source code analysis
- Hardware Security Testing: physical security analysis, anti-tamper protection testing, debugging interfaces security testing, and security Cybersecurity features of the product.

Cybersecurity features of the product.

We aim to protect your data and patients in the design and maintenance of our products. As a result of our data protection by design approach to product development, in conjunction with the results of the in-depth assessment conducted, we have implemented the following non-exhaustive security controls in the STARLIMS Quality Manufacturing Solution.

- **Limited processing of PII:** The STARLIMS Quality Manufacturing Solution utilizes sample IDs to track samples.
- **Application audit log:** The application logs select security events including, but not limited to, login attempts and failures, user history and deactivation, or transactions within the application.
- **Protection of data-in-transit:** The technology platform has a tamperproof mechanism in place that detects communication tampering, and is efficient against automated penetration tools. The mechanism works by injecting a header in all requests and responses that represents a hash of the content. In addition, session- based authentication is in place.
- **Integrity and authenticity is maintained:** Logic is in place that can detect evidence of tampering and reject any such requests. A procedure to check integrity is in place that validates extensions against a predefined list. Users must have access to the system in order to upload data and uploaded data is checked against a predefined list of file extensions.
- **User accounts:** STARLIMS user management functionality supports role based access control. Roles are used to restrict user access to applications and forms within the product.
- **Secure account/password policy:** The application supports the customer setting limits on the number of days before reusing the same password, changes before reusing the same password, days before changing the password, password lifetime, grace logins, failed password attempt lockout, and password complexities.
- **Identities and credentials are managed:** Rather than storing passwords in clear text, a salted hash of passwords are stored.
- **Secure remote desktop connections:** Remote desktop connections initiated by Abbott are password protected and initiated over secure encrypted communication channels.

Cybersecurity responsibilities of the customer.

As part of our assessments, we have identified risks that are dependent on how the product is fielded. The securing of the products we provide to our customers is a shared responsibility among all stakeholders. Based on the assessment conducted on the STARLIMS Quality Manufacturing Solution, we expect that you will take the following security steps to protect the product:

- **Physically secure the product and its operating environment:** Protect the physical security of the product and operate it in a secure manner. Control and monitor physical access to the system through the use of mechanisms such as security cameras and security badges. In addition, shut down physical ports of network equipment that is not in use to prevent unauthorized access to the application. Web Server and Database security is customer responsibility.
- **Securely operate and protect your network:** Secure the customer network through the use of a network intrusion detection and prevention mechanism, using adequately hardened network/application firewalls, and network segmentation. Additionally, secure all remote access technologies as well as disposing of data in an appropriate manner.

- **Limit access to authorized users:** Restrict access to STARLIMS Quality Manufacturing Solution to authorized users in accordance with your organization's security policies.
- **Manage and protect your sensitive data:** Reports or other data exported from the application should be controlled with appropriate laboratory practices.
- **Detect malicious and mobile code:** Select and implement anti-virus/anti-malware protection for the host machine.
- **Secure data at rest:** Secure the application data via database and file system encryption.
- **Monitor for security incidents:** Proactive monitoring of audit logs/trails in accordance with organization's policy.
- **Secure removable media:** Use encrypted removable media products when exporting sensitive data.
- **Protect client end-points:** Select, implement and update anti-virus and anti-malware protection for the server and client machines.

If you have any questions or concerns about the risks as they are described, please do not hesitate to contact your local support organization.

****