# Medical and Research Device Risk Assessment

**Vendor Packet Instructions**

# Executive Summary

Mayo Clinic’s primary value is “The needs of the patient come first”. It is built into our daily work and we continually strive to make improvements and changes in all areas that impact our value. This includes clinical, administrative, as well as in the areas of safety and security. In the areas of safety and security, Mayo Clinic is now taking leadership in promoting and requiring cybersecurity of medical/research devices.

We believe that this fits into our core values and is something we need to do to prepare for the changing, and increasingly dangerous, environment. There have been multiple incidents of cybersecurity issues in both commercial and healthcare areas that we have taken notice of and wish to proactively work with our vendors and partners to prevent any patient harm or disruption of our care processes. To do this we have used accepted standards and developed processes so we can partner with our vendors to improve the cybersecurity of medical/research devices moving forward. Our desire is to not only do this for Mayo Clinic, but for all patients who use medical/research devices and to provide a benefit to vendors.

We look forward to being able to partner to make substantial changes to the cybersecurity of medical/research devices and provide a safe and secure experience for our patients.

# Vendor Packet Instructions for Medical and Research Device Risk Assessment

The goal of the Medical/Research Device Risk Assessment is to analyze and remediate the risk of medical/research device being acquired by Mayo Clinic. The artifacts MUST match the EXACT system version being acquired for Mayo Clinic.

At a high level, the steps for acquiring a Medical/Research Device are:



1. If a full SPAD assessment is required, the Healthcare Technology Management (HTM) contact sends the Vendor contact the Vendor packet to complete.
2. Vendor contact completes artifacts within Vendor packet and returns to HTM contact.
3. HTM contact reviews the Vendor artifacts for completeness and forwards to the appropriate SPAD assessment teams. A meeting may be scheduled with the Mayo Proponent and appropriate Vendor team members to review the findings report.
4. A risk assessment is completed based on the artifacts received. A meeting may be scheduled with the assessment team member(s) to complete follow-up questions and as applicable review the assessment report. The Vendor contact and appropriate team members should participate.
5. If Vendor action is required, a copy of the final risk assessment report is sent to the Vendor. The Vendor may be required to collaborate with the Mayo Proponent and HTM to address any documented findings and remediation plans.

The timeline to complete the Medical/Research Device Risk Assessment is dependent on the following:

* **Timeliness** of Vendor to complete a manual security assessment of the system as well as all artifacts requested in the Vendor Packet for Medical/Research Device Risk Assessment.
* **Completeness** of the provided Vendor Packet for Medical/Research Device Risk Assessment. This allows Mayo assessment teams to review materials without delays due to inaccurate or incomplete information; missing items or information may result in additional meetings or discussions.
* **Responsiveness** of the Vendor to follow this process. Please be aware, all assessment requests will be reviewed for patient safety, device security, and network harm.

# Conclusion

In conclusion, after the device has been categorized and if an assessment was completed, the device will be on-boarded and the SPAD process is complete.

# Contact Information

## For questions or concerns on this process, please communicate with the HTM contact identified in the purchase process.

## Appendix – Table A

**Table A** outlines the required Vendor artifacts to initiate the Medical/Research Device Risk Assessment. The artifacts MUST match the EXACT system version being purchased for Mayo Clinic. **NOTE: Please complete the Mayo Clinic Medical and Research Device Vendor Workbook FIRST to determine if the remaining artifacts are required.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Deliverable** | **Description** | **Task** | **Resource** |
| 1. Mayo Clinic Medical and Research Device Vendor Workbook | Outlines the capabilities required for systems within the Mayo Clinic environment. | Respond to the provided spreadsheet for each device included in the purchase for system alignment with Mayo Clinic Medical and Research Device Standards.  **\*Follow instructions within the Device Information tab to determine if other tabs need to be completed. Macros have been removed.** |  |
| 1. Manufacturer’s Disclosure Statement for Medical Device Security (MDS2) | Industry standard document describing the security and risk management of a system. | Provide most current MDS2 for the device or system. Simply download the complimentary MDS2 form NH-2019 located at link.  Note: Mayo will require the 2019 version sometime in 2020. | <http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx> |
| 1. Medical/Research Device Architecture Diagram | Provides an outline of the system interaction within the Mayo Clinic environment. | Provide an architecture diagram of the system, its components, and network connectivity.  Provided is an example template as a Visio diagram and a pdf for reference. |  |
| 1. System information:  * List of Accounts * List of Network Ports * List of firewall rules (if applicable) * Documentation of Security Capabilities/Configurations for System Hardening * Scanning Requirements * Third Party Software Bill of Materials Template | Provides more granular information as to how the system is setup and managed within the Mayo Clinic environment. | Complete the system information provided within the Word template and the 3rd party software bill of materials within the provided Excel template. |  |
| 1. Manual Security Assessment, including:  * Testing Results * Remediation Tracking | Provides an in-depth manual security assessment, outstanding vulnerabilities and appropriate remediation plans and timelines to resolve the issues. This provides Mayo Clinic with appropriate information on risks that may be introduced into the patient care environment and allows for collaborative mitigation strategies to be detailed. | Complete a Manual Security Assessment as detailed in the Manual Security Assessment Book.  Once testing is finished, document findings and remediation plans in a report (Example Manual Security Assessment Template report provided). |  |
| 1. Mayo Clinic Information Security Schedule | **Provides advanced copy** of Mayo Clinic’s Information Security Schedule that Supply Chain Management will negotiate as part of the purchase contract or Vendor agreements. | 1. Ensure appropriate Vendor internal staff receives Mayo’s Information Security Schedule for review. 2. Perform review and prepare any proposed redline items. 3. Provide a Vendor contact to the Mayo proponent for the redlined ISS negotiation. |  |