DHHS POLICIES AND PROCEDURES

Section:	**VIII - Privacy and Security Office**
Title:	**NC DHHS – Medical Device Management Policy**
Current Effective Date:	**April 22, 2026,**
Revision History:	
Original Effective Date:	**April 22, 2026,**

Purpose

The purpose of this policy is to establish risk-based safeguards to ensure the protection, confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) and Individually Identified Health Information (IIHI) collected, stored, processed, or transmitted by medical devices, in accordance with federal and state regulatory requirements. This policy pertains to any item, instrument, apparatus, or machine that contains software/firmware used to diagnose, treat, prevent, mitigate or monitor health conditions that stores, transmits, or receives ePHI or IIHI, other medical devices*, or what the U.S. Food and Drug Administration (FDA) would identify as a " device" under Section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 USC §§ 301 et seq., (collectively referred to as a "Medical Device" or "Medical Devices").

The intended outcome of this policy is to:

- Prevent unauthorized access to sensitive data such as ePHI.
- Reduce the likelihood of data compromise involving any sensitive and confidential patient information and/or other state information.
- Ensure compliance with applicable Federal, and North Carolina information security and privacy requirements.

Policy

This policy is implemented pursuant to Federal and State risk management requirements such as but not limited to the HIPAA Privacy Rule and HIPAA Security Rule (45 CFR Part 164, Subparts E and C), and the Substance Abuse and Mental Health Services Administration (SAMHSA), NIST SP 800-53 (IA-3, SA-22, SI-2, SI-3, PM-5). These authorities collectively require risk-based safeguards to protect systems containing sensitive and confidential information included but not limited to PHI, IIHI, PII etc. If the vendor will have access to HIPAA-covered data or other data protected by law, the vendor must sign the NC DHHS Business Associate Agreement and/or Data Use Agreement as determined by NC DHHS.

1. Procurement of Medical Devices

All Divisions and Offices that own or utilize Medical Devices shall establish a policy and/or procedures ensuring all Medical Device purchases, renewals, leases, and connected services

undergo a documented privacy, security, and operational risk review by the Division, Office or Facility ISO prior to approval.

As part of any contract, lease, or purchase, the business or device owner must gather any FDA required documentation per the FDA risk classification process. This includes FDA device certification documents and individual device security artifacts. A full list of these documents is beyond the scope of this policy, but examples include:

- Appropriate pre-market documentation (510(k), PMA, or De Novo).
- FDA registration and listing confirmation.
- Labeling/packaging compliance evidence.
- Software Bill of Materials (SBOM): a complete inventory of software components
- Vulnerability management plan
- Security risk assessments and threat models
- Incident response documentation, including patch cycles and vulnerability disclosure procedures
- security labeling and integration guides, highlighting interfaces, user authentication, and secure configurations

The specific requirements for each review will be determined by the ISO based on the device's intended use, data classification, functions, features and FDA requirements in accordance with the device risk classification described below.

As part of the review process, all Medical Devices are required to go through the standard IT Project PTA process. Additionally, the review must determine whether the Medical Device will store DHHS data in a non–State-hosted environment. Any device that stores DHHS data outside of a State-managed environment will require a more rigorous security review and must proceed through the standard IT project procurement security review process to ensure all required security and privacy obligations are fully addressed and agreed upon by the vendor. If the security review determines that the vendor will have access to HIPAA-covered data, the vendor must sign the NC DHHS Business Associate Agreement.

A Medical Device may not be deployed until all identified risks have been documented and remediated in accordance with NC DHHS risk management processes, this policy, and applicable state and federal requirements.

2. Risk Classification

Each Division or Office that utilizes Medical Devices shall develop a set of procedures to classify each device based on a risk classification of the device and its data. Minimally the classification shall consider patient-safety impacts, connectivity, exposure to external networks, remote support, unsupported software, patch management, volume or sensitivity of confidential information and whether the device or system is 42 CFR Part 2-sensitive.

All Medical Device data risk classifications shall incorporate and align with applicable North Carolina Department of Information Technology (NCDIT) Statewide Data Classification and

Handling Policy to ensure the sensitivity of data processed, stored, or transmitted by the device is appropriately considered in the overall risk determination.

3. Device Inventory

All Divisions and Offices that own or utilize Medical Devices shall create a centralized inventory process to track their devices. All devices shall be entered into the inventory prior to production deployment and shall be maintained in the inventory until an approved decommissioning is complete. Minimally the inventory shall include the following records:

- Device name
- Device owner
- Device location
- Vendor
- Model number
- Serial number
- Operating system and/or firmware version
- SBOM
- MDS2
- UDI
- FDA Assigned Risk Classification

If applicable the following device information should be documented as well

- Network status
- Network interfaces
- ePHI is created, stored, or maintained
- Subject to 42 CFR Part 2
- Vendor support terms
- Remote Access Status
- Support/End Of Life status
- Recall Status
- Patch Management schedule

4. Implementation

Medical Devices must be implemented using secure deployment practices to reduce operational and security risks. All normal procedures should be followed when deploying a Medical Device. This includes but is not limited to device authentication, configuring manufacturer-recommended security settings, and placement of the device on appropriately segmented networks. Where applicable, each device must be configured to receive security updates, default passwords and insecure settings must be removed before use, and logging or monitoring should be enabled to detect abnormal activity.

5. Ongoing Monitoring

All devices shall be subject to ongoing monitoring appropriate to their risk classification throughout the lifecycle of the device. Divisions and Offices who utilize Medical Devices shall develop procedures to ensure that appropriate monitoring of their devices is occurring. This shall include as applicable:

- audit-log review
- access-report review
- security-incident monitoring
- vulnerability and advisory review
- patch and firmware status review
- network-communication review
- remote-access review
- unsupported / end of life status review
- review of devices operating under an approved exception or compensating controls.

6. Maintenance and Remote Support

Access to Medical Devices shall be limited to authorized personnel and authorized software processes. Privileged access, service accounts, and remote access pathways shall be controlled, reviewed according to standard Department and Statewide processes, and promptly removed or disabled when no longer needed. All vendor maintenance and remote support activities must comply with all applicable Federal requirements, as well as the NC DHHS Security Manual and NC DIT Statewide Security Policies. This included requiring the vendor to sign a non-disclosure agreement prior to performing any work on a DHHS owned Medical Device.

If a device must be sent offsite to a vendor for support, updates or maintenance, IT staff must ensure any locally stored data remains protected throughout the process. This includes verifying that the vendor is authorized to access the data and ensuring the data is encrypted prior to transport. If adequate data protection is not feasible, all locally stored data must be securely deleted in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 and 800-66, Guidelines for Media Sanitization before the device is delivered to the vendor. If this is not possible or appropriate, an exception and mitigating controls must be identified, documented, and approved before the device leaves DHHS control.

7. Vulnerability and Patch Management

Medical Devices shall be subject to vulnerability and patch management processes consistent with applicable federal and state requirements and NC DHHS security standards. Divisions and Offices are required to follow the established remediation timeframes identified in the NC DHHS Security Manual and NC Statewide System and Information Integrity Polices. Security patches, firmware updates, service packs, hotfixes, and other manufacturer-approved remediations shall be reviewed, risk-assessed, documented, tested where appropriate, and implemented within required remediation timelines. Remediation decisions shall consider device criticality, patient safety, cybersecurity risk, operational necessity, and regulatory obligations, including applicable FDA requirements, HIPAA, HITECH, and where applicable, 42 CFR Part 2

requirements. When remediation cannot be completed within the required timeframe due to vendor dependency, technical constraints, unsupported systems, or operational limitations, Divisions and Offices shall implement documented compensating controls and obtain an approved exception in accordance with the NC DHHS Form C Exception process. See Appendix A for additional information.

8. Security Incident / Breach

Any breach or suspected breach must be reported to the PSO using the NC DHHS Privacy and Security Office Incident Reporting Form. All reports must be performed in accordance with the NC DHHS Privacy Manual Section 6.1.2 Reporting HIPAA Incidents and Complaints. Reportable events includes any suspected compromise, malware / ransomware events, unauthorized access, unexpected transmission, lost or stolen device, inappropriate disclosure, or other security or privacy event(s).

9. Device Decommissioning

All Medical Devices shall be disposed of, transferred, returned, or retired through a documented process that protects patient data and reduces operational, privacy, and security risk. Before a device leaves DHHS control, all local storage and associated media must be disposed of in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization. The Division or Office shall disable associated access, update inventory records, and retain documentation of final disposition, sanitization, chain of custody, and vendor certificates where applicable. Any Medical Device disposal shall include a Certificate of Sanitization form. See Appendix G of the NIST 800-88 Guidelines for a sample form.

10. Privacy Rule Controls

As required under the NC DHHS Privacy Manual, any confidential data utilized by a medical-device workflow shall be configured and monitored to support minimum necessary disclosure, handling, and access standards and to detect inappropriate access, use, disclosure, printing, export, or redisclosure of protected health information. Divisions and Offices that utilize Medical Devices shall preserve sufficient records to support requests for an accounting of disclosures where required.

11. 42 CFR Part 2 Controls

Medical Devices, other devices, and connected systems used by substance use disorder programs or other lawful holders of Part 2 records shall receive enhanced privacy and security monitoring. Formal safeguards should be maintained to protect Part 2 patients identifying information against unauthorized use or disclosure and against reasonably anticipated threats or hazards. The organization shall also preserve sufficient disclosure information to support accounting obligations under 42 CFR Part 2.

12. Documentation and Retention

The Division or Office shall maintain written or electronic records necessary to demonstrate compliance with the policy and the corresponding procedure, including inventories, risk classifications, review logs, findings remediation records, exceptions, incident records, and evidence of closure. Required documentation shall be retained for at least six years unless a longer period is required by laws, retention schedule, or litigation hold.

13. Other

The Division or Office shall comply with all applicable state and federal laws, regulations, and governmental requirements, in addition to adhering to all internal policies established by the organization. Where conflicts arise between this policy and any legal requirement, the organization will follow the applicable law or regulation. When in doubt, the Division or Office should consult with their identified NC DHHS legal counsel.

Roles and Accountability

Business Owner/Device Owner: The Business Owner/Device Owner is the individual or business unit responsible for the overall procurement, development, integration, modification, operation and maintenance of the information system/Medical Device. The information systems owner develops and maintains the system security plan in coordination with the information owners, the system administrator, the information system security officer, functional "end users," third parties, and other covered personnel.

Information Security Official (ISO): The Division or Office ISO is responsible for ensuring that security risks are managed in compliance with State and Departmental requirements by collaborating with organizational entities. Liaisons are responsible for ensuring that the appropriate controls are in effect for agency information systems.

End user: An end user is an approved State employee, contractor, or a visitor who is authorized to use the IT system/Medical Device to conduct the business of the State.

Covered Personnel: Covered personnel include officers, employees, any other NCDHHS staff members, volunteers, and trainees, as well as any individual retained under contract or other arrangement who performs functions like those of an officer, employee, or other staff member. Covered personnel are required to understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of an IT system/Medical Device.

Third Parties: Third party service providers must ensure that all IT systems and applications developed for the State conform to this and other applicable information technology policies, standards and procedures.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in adverse contractual and financial consequences, disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Authority and Governing Requirements

This policy supports compliance with 45 CFR Part 164, including the HIPAA Security Rule and HIPAA Privacy Rule, HITECH breach-related obligations, and 42 CFR Part 2 requirements for substance use disorder patient records. The organization also uses NIST SP 800-30, NIST SO 800-53, and NIST SP 800-66 Rev. 2 as recognized implementation guidance, along with relevant FDA, OCR, and CISA Medical Device security guidance.

Definitions

A. *Medical Device

- A Medical Device is any instrument, apparatus, machine, implant, software, in vitro reagent, or related article that collects, stores, processes, or transmits data associated with an individual's identity and/or connects to a network or communication platform(e.g., USB, Wi-Fi, cellular, Bluetooth, NFC, GPS, cloud systems, remote monitoring systems, APIs, or other digital interfaces) and/or performs diagnostic, monitoring, therapeutic, or life sustaining functions. Medical devices may include hardware-only systems, software as a medical device (SaMD), embedded systems, wearable technologies, and cloud-connected medical platforms.

B. Software Bill of Materials (SBOM)

- An SBOM is a detailed, machine-readable inventory of all software components, libraries, and dependencies within a Medical Device. It includes information such as component name, version, supplier, unique identifiers, and licensing.

C. Manufacturer Disclosure Statement for Medical Device Security MDS2

- The MDS2 is a standardized document provided by medical device manufacturers to communicate the security features, capabilities, and risks associated with their products. The MDS2 enables healthcare organizations to assess device security controls, evaluate potential vulnerabilities, and determine compliance with internal security requirements and regulatory expectations. This document supports informed decision-making throughout the procurement, risk-assessment, and lifecycle-management processes for medical devices connected to the organization's network

D. Unique Device Identifier (UDI)

- A UDI is a globally standardized product identification system designed to enhance medical device traceability, safety, and regulatory compliance.

Appendix A – Form C Exception Document

Exceptions may be granted for a defined period not to exceed one year, after which reevaluation is required. Facilities/divisions, together with the ISO and the Facility Director's signature, must complete Form C Exception request and submit it to the Privacy and Security Office.

References

- 45 CFR PART 164, including HIPAA Privacy Rule and HIPAA Security Rule administrative, physical, technical and documentation safeguards.
- HITECH breach-related obligations for unsecured protected health information.
- 42 CFR Part 2, including formal safeguard and disclosure-accounting requirements for substance use disorder patient records.
- NIST SP 800-30, Guide for Conducting Risk Assessments.
- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.
- NIST SP 800-66 Rev. 2, Implementing the Health Insurance Portability and Accountability Act Security Rule.
- FDA, Post-market Management of security in Medical Device: Guidance for Industry and Food and Drug Administration Staff.
- FDA, Classify Your Medical Device
- U.S. Department of Health and Himan Services, Office for Civil Rights (OCR), Guidance on Risk Analysis.

For questions or clarification on any of the information contained in this policy, please contact the policy owner or designated contact point: ***NC DHHS PSO Policy Coordinator.***