The Future of Secure Work:
How to Enable the Secure Workforce of the Future Through Secure Mobility

White Paper Annex 5
How to Enable the Secure Workforce of the Future through Electronic Medical Devices

ATARC The Future of Secure Working Group

July 2024

ATARC

Advanced Technology Academic Research Center

Table of Contents

***Disclaimer**: This white paper was prepared by the ATARC The Future of Secure Work Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated. This white paper is intended to be a helpful guidance relating to current quantum technological capabilities.*

Breaking the "NO" culture…managing risk while enabling wearable healthcare devices

Who Benefits from this Paper:

- Employees – will understand the EMD approval landscape
- Approving Authorities – will know the existing guidance
- Security Managers – will have guidelines that clarify risk and approvals for EMDs
- Organizations – will benefit by having an experienced, enabled, diverse and satisfied workforce

The 21st century brought significant demand for wireless technology into the federal, Department of Defense (DoD) and Intelligence Community workforces and facilities. Organizations commonly banned Electronic Medical Devices (EMDs, also known as "MedPeds" or wearable healthcare devices) from secure spaces. However, separating employees from their physician-prescribed embedded and or wearable EMDs presents health risks, undesirable work conditions, performance barriers and even legal liability. Many surgeries result in embedded EMDs, and military veterans in the workforce also introduced a substantial increase in hearing aids to the workplace. Banning EMDs also prevents the most seasoned employees from being full, valued members who contribute the breadth of their experience to mission accomplishment. This makes it vital that organizations fully recognize the value and growing dependance of employees on wearable medical devices and adapt to the introduction of EMDs in secure and Secure Compartmented Information Facilities (SCIFs).

Although a wide range of US Government (USG) guidance on health, EMDs, and compliance of the American Disability Act exists, navigating the guidance to properly care for employees while respecting security is often a challenge for Chief Information Officers (CIOs), Security Approving Officials and supervisors alike.

This document will help Approving Officials and supervisors understand the risks and find the way to a "Yes" approval for the workforce's wireless medical personal devices in secure areas and SCIFs. The approach, guidance and example references should provide a path for identifying risk and approving acceptable use for employees across agencies and organizations.

The Situation: As EMDs increase in sophistication and reliability, they are rapidly becoming the standard for patient care for certain medical conditions. The FDA's Medical Device Product Classification database lists over 6,000 types of EMDs regulated by FDA's Center for Medical Devices and Radiological Health (CDRH). From simple devices such as hearing aids to complex hybrid closed-loop systems for managing Type-1 Diabetes (T1D), the range of technical needs varies widely, as does the associated risk. As these solutions continue to evolve, the related threats and mitigations evolve as well.

A 2020 Virginia Tech study of potential risks from EMDs correctly stated, "The IC cannot meet security requirements simply by refusing to employ people who rely on [implanted medical devices.]."[1] Figure 1 from the same study shows an estimated number of cleared USG employees using IMDs as of 2020.

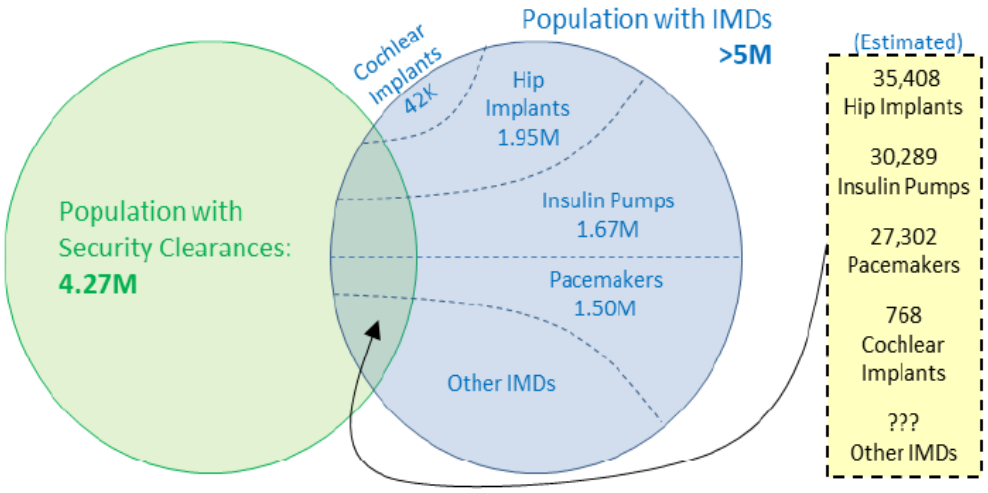

Figure1: Estimated number of cleared USG employees with Implanted Medical Devices[2]

Currently, US Government agencies, including Intelligence Community (IC) organizations, are developing use policies for EMDs. Section 723 of the FY2022 NDAA requires the DOD to develop a digital health strategy to include wearable devices. The July 2023 DoD Report, "Use of Fitness Wearables to Measure and Promote Readiness," observed that the "DoD has led multiple analytical efforts to include pilot programs to collect and use data from health and fitness trackers to measure individual and troop readiness." The report listed over 20 studies and pilot programs across the DoD intended to understand and develop methods for using wearable medical technology. The report acknowledged the complexities of operational security for EMDs.

Most significantly, Intelligence Community Directive (ICD) 124, Electronic Medical Devices published on April 26, 2024, establishes IC policy for maximum accessibility for people using EMDs. Significant provisions in ICD 124 include:[3]

- Consistency and transparency in EMD use.

[1] Whitepaper: "An Invisible Insider Threat: The Risks of Implanted Medical Devices in Secure Spaces," Virginia Tech Hume Center for Security and Technology, August 2020, p. 3.

[2] Ibid..

[3] ICD 124, Wearable Medical Devices, Office of the Director of National Intelligence, 26 April 2024, p.4.

- Assured informed and safe access to all IC Secure Compartmented Information Facilities (SCIFs), including the need to protect classified information.
- The IC need to attract, maintain, and support a world-class, diverse workforce.
- Broad provisions for entry-on-duty and visitors to SCIFs.
- Outlines risk-based parameters for requesting EMD use in SCIFs, with considerations for approvals or denials.
- Reciprocity across IC agencies.
- Protection of wearer Personally Identifiable Information (PII).
- Roles and responsibilities within the IC for governance and implementation.

While the provisions of ICD 124 and results from related programs proliferate, we recommend two paths towards applying EMDs in current secure spaces: Continuing to permit use through agency Reasonable Accommodation policies and procedures, and an eventual standardization of allowable EMD use and thorough implementation of ICD 124.

> *"Consumer privacy, protections, and information security are additional flashpoints, or challenges, to full commercial adoption and trust/acceptance of wearable technologies . . .."*
>
> ATRC White Paper, "Data From Wearables: Emerging Technology and Emerging Challenges," March 2023

Goal: Enable secure workforces to operate in an environment that enhances their health, efficiency, productivity, satisfaction, security and privacy. Implement policies and procedures that allow employees to use their wearable health devices in secure spaces.

Resources:

- Access to Wireless Intrusion Devices (WIDS)
- When tethering to mobile devices is authorized, consider employing anti-surveillance hardware mitigations to mobile device to protect data in vicinity and track user compliance.
- References:
  - ICD 124, Office of the Director of National Intelligence, April 26, 2024.
  - NCIC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705, v1.5, March 13 2020.
  - NIST Special Publication 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements, November 2021.
  - NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, May 2020.
  - See the "Frequently Asked Questions" section for additional references.

Step-by-Step Considerations:

Step 1: Review organization policies that apply to EMDs. Has your agency implemented ICD 124, or is there a Reasonable Accommodation policy that permits security review of wearable medical devices?

"Approval for medical devices will comply with all applicable laws and oversight policies, including the Rehabilitation Act, and the latest IC medical device approval process. As a minimum, the medical device must be reviewed to determine any technical security issues introduced by the device. Based on the security/technical review, medical devices may be approved by the AO for introduction and use within a SCIF."[4] NCIC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705

The following is a sampling of agencies that have Reasonable Accommodation Policies and Procedures:

- **Office of the Director of National Intelligence (ODNI):** https://www.dni.gov/files/documents/EEOD/PAS_procedures_-_External_Website.pdf
- **National Security Agency:** https://www.nsa.gov/Culture/Diversity-Equity-Inclusion-Accessibility/Accommodations-Accessibility/
- **Defense Intelligence Agency:** https://www.dia.mil/Portals/110/Documents/Careers/DIA_Instruction_1020.002_Reasonable_Accommodation.pdf
- **Department of Defense:** https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/ai/a114p.pdf?ver=2019-02-14-151537-973#:~:text=It%20is%20DoD%20policy%20according%20to%20DoD%20Directive,hardship%20to%20the%20Department%2C%20consistent%20with%20Reference%20%28b%29.
- **Federal Bureau of Investigation:** https://fbijobs.gov/sites/default/files/oeeoa_fast_facts_-_reasonable_accommodations_-apply.fbijobs.gov_.pdf

Step 2: Employees should submit for or register EMD use in their facility following the procedures in the organization Reasonable Accommodation policy. While ICD 124 is implemented, per ICD/ICS 705, heads of IC elements shall establish risk mitigation programs if high- or medium-risk EMDs are allowed into SCIFs. Figure 2 shows a range of risks in Internet of Things devices and how they intersect from the National Institute of Standards and

[4] NCIC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec – for ICD/ICS 705, p. 75.

Technology (NIST Interagency Report 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.

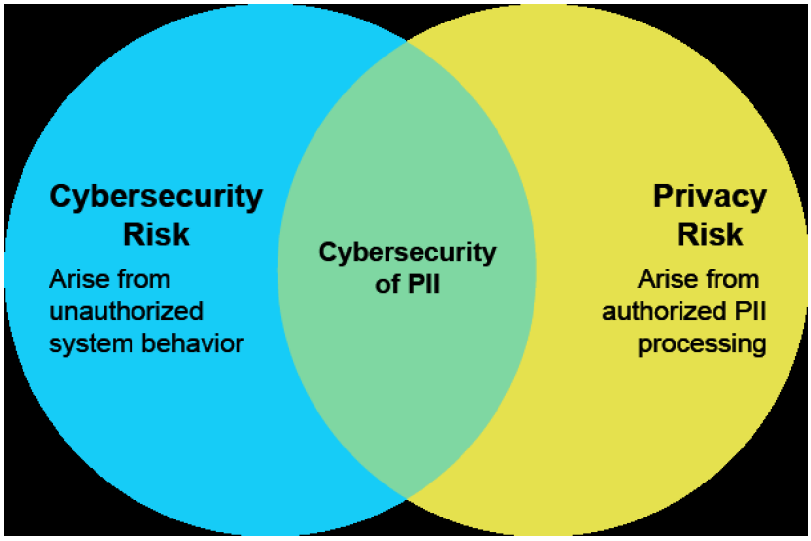

Figure 2: Relationship Between Cybersecurity and Privacy Risks[5]

Per ICD 705, risk mitigation programs for EMDs shall contain the following elements:

- Formal approval process for PEDs.
- Initial and annual refresher training for those individuals with approval to bring PEDs into a SCIF.
- Device mitigation compliance documents listing the specific PEDs, their permitted use, required mitigations, and residual risk after mitigation.
- A user agreement that specifies the following:
    - The USG or a designated representative may seize the PED for physical and forensic examination at the government's discretion.
    - The USG and the designated representative are not responsible for any damage or loss to a device or information stored on personally-owned PEDs resulting from physical or forensic examination.

Risk mitigation programs may include the following elements:

- Registration of PED serial numbers.
- PED security training program.
- Reporting procedures for loss or suspected tampering.
- Labeling approved PEDs for easy identification.

[5] National Institute of Standards and Technology (NIST) Interagency Report 8228, Considerations for Managing
Internet of Things (IoT) Cybersecurity and Privacy Risks, June 2019, p. 5.

- Electronic detection equipment to detect transmitters/cell phones.

Enhanced monitoring considerations
Agencies should consider working with cybersecurity teams to include monitoring for EMD devices when allowed by policy and when feasible. For example, Wireless Intrusion Detection Systems can be used to detect EMD transmitters, compare against a whitelist and report exceptions to a SIEM system.

Governance, Risk Management and Compliance (GRC)
Additional cybersecurity considerations may include updating GRC documentation.

Mobile Device Tethering
Tethering EMDs to employee-owned mobile devices is a common practice. Organizations should implement security monitoring and risk mitigations in secure spaces. For more information on enabling mobile devices in secure spaces see the ATARC Future of Secure Work White Paper How to Enable the Secure Workforce of the Future Through Secure Mobility and Annex 3: How to Enable Secure Mobility for Fixed Location Workplaces.

Step 3: Consider requesting an update to organization policy. In May 2020, the National Institute of Standards and Technology (NIST) issued NISTIR 8259A with standards for organizations used in identifying device cybersecurity capabilities for new IOT devices that may integrate into existing architectures. Reviews of EMDs under ICD 124 or other policies that thoroughly addresses EMD security should address these potential risks and mitigations:

Potential EMD risks in secure spaces:

- EMDs with microphones, cameras, and other sensors not required for medical information present higher risk.
- Some level of risk of EMD hacking will remain, so organizations should focus on:
  - Can the device be used to illicitly gather national security info in the secure space?
  - If yes, how can that be mitigated?
  - If no, is there any way to detect or prevent data exfiltration?
  - Can a bad actor leverage the introduction of new technologies for malicious intent? (such as introduce a BLE implant)

Potential EMD mitigations:[6]

- **Independent EMD security testing:** Independent testing would verify the true risk, or lack of risk, by transmissions.

[6] White Paper, Hidden Insider Threat, pp. 4-5; Securing Consumer Mobile Healthcare Devices, Department of Homeland Security, 2021, p.7.

- **Wireless Intrusion Devices (WIDS):** Use of WIDS could allow Security Managers to identify if unauthorized EMD are used in the secure area. This would augment the self-reporting requirements in ICD 124.
- **Whitelisting:** A pre-approved list of tested and verified EMDs would enable Security Manager approval and the approval process under ICD 124.
- **Device configuration management:** to disable device camera, microphone, Wi-Fi, to address potential risk, privacy, or usability.
- **Random Inspections:** Random inspections would identify unauthorized devices.
- **Data protection:** The ability to install cryptographic modifiers to render data inaccessible from unauthorized parties.
- **Logical access interfaces:** Disabling unnecessary access or restricting access.
- **Use of Bluetooth Low Energy:** lowers the risk of unauthorized transmission of sensitive information.
- **Enforcing high level information protection on backend services**: require medical device vendors to comply with information protection regimes for their backend, cloud, or other auxiliary services.

Step 4: Continually measure compliance. Adjust and revise security practices based on lessons learned.

Conclusions

By following the considerations and steps in this paper, forward-thinking approving officials can advance the accomplishment of national security missions and enhance the workforce. Emerging national policy is clarifying how to identify and address risk from EMDs. The proliferation of EMDs in medicine is improving their security. Seasoned employees and veterans are vital workforce members with invaluable, if not irreplaceable, skills and experience. This combination means that introducing EMDs in secure spaces with thorough security is not only inevitable, but also crucial to enabling organizations to accomplish their respective missions. The US faces multiple adversaries that enjoy massive workforces. Allowing EMDs in secure spaces is one step towards a counterweight to that imbalance through what the US does best: bringing our best people and technology to outweigh adversarial brute force. The US has no shortage of people who have dedicated their lives to national security and want to continue doing so through meaningful secure work. We need not wait any longer to employ this force to their fullest capabilities.

Frequently Asked Questions:

Question: What are some additional references that apply to EMDs?

Answer: See below for some examples of additional references

ODNI

ICD-124-Electronic_Medical_Devices.pdf (dni.gov)

NSA

Agency, Audiologist Solve Hearing Aid Security Concern, Get Needed Devices in NSA Spaces > National Security Agency/Central Security Service > Article

USAID

ADS Chapter 568 - National Security Information Program (usaid.gov)

568.3.8.4 Medical Devices Effective Date: 01/19/2021 Exceptions may be made for medical devices. Members of the workforce requesting an exception or reasonable accommodation due to the use of a medical device must submit a request to the Office of Civil Rights and Diversity (OCRD). OCRD will coordinate with SEC and the Bureau for Management, Office of the Chief Information Officer, Information Assurance Division (M/CIO/IA) and provide only the information necessary to process the request. Specific documentation from a medical professional may be required. SEC, M/CIO/IA, and OCRD will provide written approval for any approved medical device. OCRD, SEC, and SCIF Accreditation Officials must approve reasonable accommodations for medical devices in a SCIF.

NNSA Advanced Change Directive (ACD) 470.6

ACD4706FAQ-1.pdf (sandia.gov)

Medical devices themselves are not restricted by the policy. Nothing in the directive alters or supersedes legal or policy requirements regarding accommodation of employees' medical needs, which continues to follow the Essential Job Function process. However, many medical devices pair with peripheral devices which could meet the definition of a mobile device. Nothing in the requirement makes exception paired, mobile devices, and therefore they are not permitted in Secure Space.

GAO FEDERAL REAL PROPERTY Improved Data and Access Needed for Employees with Disabilities Using Secure Facilities

https://www.usaid.gov/sites/default/files/2023-07/568.pdf

US Navy

mynavyhr.navy.mil/Portals/55/Messages/NAVADMIN/NAV2023/NAV23169.txt?ver=RrNvYeQEj6qse9qHzfw31Q%3D%3D

Electronic medical devices, including but not limited to implanted medical devices (e.g. pacemakers, electronic nerve stimulators), hearing aids, insulin pumps, blood glucose monitors, and supporting equipment may be permitted in a DON SCIF with approval from their Navy RSSO. Requests for wear or use of electronic medical devices will be considered upon receipt of orders from a physician.