DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

DAFGM2024-16-01

24 April 2024

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FLDCOMs/FOAs/DRUs

FROM: HAF/A2/6
1700 AF Pentagon
Washington, DC 20330-1700

SUBJECT: Department of the Air Force Guidance Memorandum Establishing *Security Guidance for the Use of Electronic Medical Devices and Portable Wearable Fitness Devices in Secure Spaces*

By Order of the Secretary of the Air Force, this Department of the Air Force Guidance Memorandum implements guidance in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance.* It provides guidance addressing consolidated security guidance for the use of Electronic Medical Device and Portable Wearable Fitness Devices within secure spaces. This Guidance Memorandum updates the expired original 2022 Guidance Memorandum that established consolidated security guidance for the use of Electronic Medical Device and Portable Wearable Fitness Devices within secure spaces. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Department of the Air Force/Air Force/Space Force publications, the information herein prevails, in accordance with Department of the Air Force Instruction (DAFI) 90-160, *Publications and Forms Management* and Department of the Air Force Manual (DAFMAN) 90- 161, *Publishing Processes and Procedures*. This guidance is applicable to all uniformed members of the Regular Air Force, the United States Space Force, the Air Force Reserve, the Air National Guard, the Civil Air Patrol, when conducting missions as the official Air Force Auxiliary, all DAF civilian employees, and those personnel with a contractual obligation to abide by the terms of DAF issuances.

The Intelligence Community (IC) and the Department of Defense (DoD), and their partners throughout government and industry, are in the process of updating policy and guidance on portable electronic devices (PED). Specifically, for electronic medical devices (EMD) and their reciprocity throughout the IC and DoD sensitive compartmented information facilities (SCIF), special access program facilities (SAPF), and secure rooms. At the same time, several government-wide force health initiatives are being implemented that will utilize portable wearable fitness devices (PWFD) with data recording capabilities and other embedded technologies. Airmen and Guardians require updated guidance on the use and introduction of EMDs and PWFDs to enable greater reciprocity within (DAF) secure spaces.

Adherence to the guidance in this Memorandum is necessary to protect classified information and enable reciprocity for personnel requiring EMDs, and to maximize the effectiveness of force health initiatives utilizing PWFDs. This guidance has been developed in coordination with all required DAF security policy authorities. Addressing request to meet "reasonable accommodation(s)" will be consistent with law (e.g., Americans with Disabilities Act) and policy. No tier waiver statement or tier numbering is provided, as the reciprocity compliance requirements of this guidance memorandum are not waivable. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command.

This Guidance Memorandum requires the collection and or maintenance of information protected by the Privacy Act of 1974, as implemented by DoD 5400.11-R, *DoD Privacy Program.* The applicable System of Records Notice can be found at https://dpcld.defense.gov/Privacy/SORNs/.

Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, Records Management and Information Governance Program, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon publishing of a new Instruction/Manual permanently establishing this guidance, whichever is earlier**.**

LEAH G. LAUDERBACK, Lt Gen, USAF
Deputy Chief of Staff for Intelligence, Surveillance,
Reconnaissance and Cyber Effects Operations

Attachment
1. DAF Form 110, DAF Electronic Medical Device (EMD) Request form & Approval Card
2. DAF Form 111, DAF Personal Wearable Fitness Device (PWFD) Request Form & Approval Card

DAFGM2024-16-01

Minimum Security Requirements and General Guidance

1. Introduction. The Department of the Air Force (DAF) periodically requires the utilization of portable electronic devices (PED) within secure spaces in order to support operations, or to monitor the health of personnel, especially when fielding new assets, systems, or other technologies. Additionally, there has been a significant increase in the use of sophisticated electronic medical devices (EMDs) and personal wearable fitness devices (PWFD) to treat medical issues or disabilities, support force health initiatives, and for personal health use. The DAF requires a cohesive approach and guidance for the fielding of these devices, in order to provide maximum support to our personnel, while mitigating the risk to classified information associated with the introduction PEDs with rapidly advancing capabilities and embedded technologies.

2. Definitions

2.1. Secure Space: refers to any space designated or accredited for the storage, discussion, or processing of classified information in government owned or leased facilities and contractor-owned or -leased facilities which are under the security cognizance of the DAF.

2.2. Security Official: DAF personnel formally assigned duties for the protection of classified information, including but not limited to: security manager/assistant working in (or supporting) an information protection office, special security officer (SSO), special security representative (SSR), program security officer (PSO), government special access program security officer (GSSO), information systems security manager (ISSM), and information systems security officer (ISSO).

2.3. Security Cognizance: The formal assignment of security responsibilities for the protection, oversight, and operation of DAF secure spaces and classified national security information, by law, regulation, or policy.

3. Applicability and Scope

3.1. All uniformed members of the Regular Air Force, the United States Space Force, the Air Force Reserve, the Air National Guard, the Civil Air Patrol, when conducting missions as the official Air Force Auxiliary, all DAF civilian employees, and those personnel with a contractual obligation to abide by the terms of DAF issuances, (hereby referred to as "DAF personnel").

3.2. All DAF secure spaces located within the Continental United States (CONUS), Alaska and Hawaii, and Overseas locations. Security officials must remain aware of specific limitations in overseas locations that may be imposed by Accrediting and Authorizing Officials per the references.

3.2.1. For devices in overseas locations, nothing in this memorandum shall be construed to supersede or circumvent the requirements of references (a) and (g), which may require additional evaluation, mitigation, and approval prior to the introduction into a secure space.

3.3. All EMDs and PWFDs, regardless of reason for use.

3.4. The goal of this memorandum is to enhance reciprocity across the DAF. Nothing in this memorandum shall limit or prevent security officials from exercising their authorities, in accordance with the references, for the introduction of PEDs into secure spaces under their cognizance.

3.5. Nothing in this memorandum shall prevent commanders/directors from making risk-based decisions and applying more stringent rules for PEDs, based on mission or operational security requirements.

4. EMD Guidance

4.1. EMDs are any PED which is prescribed, recommended, or issued by a medical professional that is required to treat or safeguard the health of DAF personnel, or to meet a "reasonable accommodation" request due to a medical issue or disability, and which may possess any of the following: Bluetooth, Wi-Fi, microphone, or user-modifiable storage (list is not all-inclusive).

4.2. EMD Request Process

4.2.1. DAF personnel, requiring the use of an EMD within a secure space, shall initiate the request process with their servicing security official, by utilizing DAF From 110 "DAF EMD Request Form & Approval Card," in Attachment (2).

4.2.2. EMD Approval

4.2.2.1.Servicing security officials shall evaluate all requests, in accordance with the references.

4.2.2.2.Servicing security officials shall approve all requests unless there is an articulable risk to classified information, operations, or an exception exists as detailed in paragraph 6.

4.2.2.3.Servicing security officials shall provide training to the requestors on the use of approved EMDs within secure spaces and provide the requester an EMD Approval Card. Training shall include, at a minimum, responsibilities and requirements for utilizing the EMD within secure spaces, annual reauthorization requirement, foreign travel considerations, and any specific limitations for the utilization of the approved device.

4.2.2.4.When an EMD is requested, which is listed as "permitted" on the National Security Agency (NSA) Office of Security & Counterintelligence (S&CI) PED listing, then it shall be assumed that all the technical vetting requirements of references (a) and (b) have been met, and those devices may be utilized without further evaluation or coordination, unless an exception exists as detailed in paragraph 6. If a device is listed as "not permitted," than it will be assumed to have failed the vetting requirements of references (a) and (b) and poses a risk to

classified information without additional coordination, mitigation, and approval with the appropriate security officials.

4.2.2.5.EMD approvals shall be valid for one year (e.g., the one-year anniversary from the date of issuance). After one year, requestors shall resubmit the EMD for reauthorization. Upon review of the request, a new EMD Approval Card shall be issued.

4.2.2.6.Servicing security officials shall forward a copy of all EMD approvals to their cognizant security official, who shall maintain a consolidated list of all approvals and make it available to other security officials, as needed. Information gathered through the request process, shall be protected in accordance with references (h) and (i).

4.2.3. EMD Disapproval

4.2.3.1.Servicing security officials shall only disapprove requests when there is an articulable risk to classified information or operations, or if prohibited by directive, regulation, or security standard.

4.2.3.2.Servicing security officials shall provide an unclassified reason for the disapproval to the requester. When it is not possible to provide an unclassified reason, due to the sensitivity of a secure space or operation, servicing security officials shall provide an appropriately classified reason to DAF personnel if they are cleared to receive such information.

4.2.3.3.Servicing security officials shall forward a copy of all EMD disapprovals to their cognizant security officials, who shall maintain a consolidated list of all disapprovals and make it available to other security officials, as needed.

4.3. Reciprocity

4.3.1. An EMD Approval Card, for a device recorded on the NSA S&CI PED listing, signed by an SSO and a PSO, shall be accepted by all security officials within all DAF secure spaces, unless a specific exception exists, as detailed in paragraph 6. SSO and PSO can delegate to SSR and GSSO approval authority on their behalf. Delegation must be done in writing and maintained by the SSO and or PSO with security cognizant over the facility.

4.3.2. An EMD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by an SSO or the delegated SSR shall be accepted by all security officials in all secure spaces, except in areas accredited or approved for the protection of special access program (SAP), or when a specific exception exists, as detailed in paragraph 6.

4.3.3. An EMD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by a PSO or the delegated GSSO shall be accepted by all security officials within all secure spaces, except in areas accredited for the protection of sensitive compartmented information (SCI), or when a specific exception exists, as detailed in paragraph 6.

4.3.4. An EMD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by a security manager or designated representative, shall be accepted by all security officials within all secure spaces, except in areas accredited or approved for the protection of SCI or SAP, or when a specific exception exists, as detailed in paragraph 6.

4.3.5. DAF personnel will have their EMD Approval Card in their possession, and present it upon demand by DAF security officials, while utilizing an approved device within a secure space.

5. PWFD Guidance

5.1. PWFDs are any PED which is approved, recommended, or issued as part of a DAF force health initiative or which is being utilized in a personal capacity by DAF personnel for physical fitness and which may possess any of the following: Bluetooth, Wi-Fi, camera, cellular, microphone, or user-modifiable storage (list is not all-inclusive).

5.2. Request Process

5.2.1. DAF personnel, requesting the use of a PWFD within a secure space, shall initiate the request process with their servicing security official utilizing DAF Form 111 "DAF PWFD Request Form & Approval Card," in Attachment (2).

5.2.2. PWFD Approval

5.2.2.1.Servicing security officials shall approve all PWFD requests unless there is an articulable risk to classified information, operations, or an exception exists as detailed in paragraph 6.

5.2.2.2.Servicing Security Officials shall provide training on the use of approved PWFDs within secure spaces and provide the requester a PWFD Approval Card. Training shall include, at a minimum, responsibilities, and requirements for utilizing the PWFD within secure spaces, annual reauthorization, foreign travel considerations, and any specific limitations for the utilization of the approved device.

5.2.2.3.When a PWFD is requested, which is listed as "permitted" on the NSA S&CI PED listing, then it shall be assumed that all the technical vetting requirements of references (a) and (b) have been met, and those devices may be utilized without further evaluation or coordination, unless an exception exists as detailed in paragraph 6. If a device is listed as "not permitted," than it will be assumed to have failed the vetting requirements of references (a) and (b) and poses a risk to classified information without additional coordination, mitigation, and approval with the appropriate security officials.

5.2.2.4.PWFD approvals shall be valid for one year (e.g., the one-year anniversary from the date of issuance). After one year, requestors shall resubmit the PWFD for reauthorization. Upon review of the request, a new PWFD Approval Card shall be issued.

5.2.2.5.Servicing security officials shall forward a copy of all PWFD approvals to their cognizant security officials, who shall maintain a consolidated list of all approvals and make it available to other security officials as needed. Information gathered through the request process, shall be protected in accordance with references (h) and (i).

5.2.3. PWFD Disapproval

5.2.3.1. Servicing security officials shall only disapprove requests when there is an articulable risk to classified information or operations, or if prohibited by directive, regulation, or security standard.

5.2.3.2. Servicing security officials shall provide an unclassified reason for the disapproval to the requester. When it is not possible to provide an unclassified reason, due to the sensitivity of a secure space or operation, servicing security officials shall provide an appropriately classified reason to DAF personnel if they are cleared to receive such information.

5.2.3.3. Servicing security officials shall forward a copy of PWFD disapprovals to their cognizant security officials, who shall maintain a consolidated list of all disapprovals and make it available to other security officials, as needed.

5.3. Reciprocity

5.3.1. A PWFD Approval Card, for a device recorded on the NSA S&CI PED listing, signed by an SSO and a PSO, shall be accepted by all security officials within all DAF secure spaces, unless a specific exception exists, as detailed in paragraph 6. SSO and PSO can delegate to SSR and GSSO approval authority on their behalf. Delegation must be done in writing and maintained by the SSO and or PSO with security cognizant over the facility.

5.3.2. An PWFD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by an SSO or the delegated SSR shall be accepted by all security officials in all secure spaces, except in areas accredited or approved for the protection of special access program (SAP), or when a specific exception exists, as detailed in paragraph 6.

5.3.3. An PWFD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by a PSO or the delegated GSSO shall be accepted by all security officials within all secure spaces, except in areas accredited for the protection of sensitive compartmented information (SCI), or when a specific exception exists, as detailed in paragraph 6.

5.3.4. A PWFD Approval Card, for a device recorded on the NSA S&CI PED listing, signed only by a security manager, shall be accepted by all security officials within all secure spaces, except in areas accredited or approved for the protection of SCI or SAP, or when a specific exception exists as detailed in paragraph 6.

5.3.5. DAF personnel will have their PWFD Approval Card in their possession, and present it upon demand by DAF security officials, while utilizing an approved device within a secure space.

6. Exceptions

6.1. Due to the extremely sensitive nature of some activities and operations, EMDs and PWFDs cannot be approved for entry into some secure spaces, or areas within them. Security officials with cognizance over secure spaces where EMDs and PWFDs must be prohibited, shall maintain a list of all such areas and provide that information to other security officials, upon request, to the greatest extent possible. Security officials will post signage at the entryways or provide other appropriate notice to all personnel prior to entry into those areas.

6.2. An EMD or PWFD Approval Card, for a device not recorded on the NSA S&CI PED listing, shall be accepted by a requestor's servicing security official for the secure spaces under their cognizance, after all mitigations and approvals have been completed in accordance with the references.

7. Coordinating Instructions

7.1. Personnel regularly requiring access to support secure spaces, that are not cleared for unescorted or unrestricted access (e.g., information systems installation, maintenance personnel, alarm system technicians, etc.), may request and be issued a DAF EMD Approval Card by the cognizant security officials, if the device is recorded on the NSA S&CI PED listing. Devices not on the NSA S&CI PED listing, may be approved by the DAF cognizant security officials for the secure spaces under their cognizance, and only after all mitigations and approvals have been completed per the requirements of the references and this memorandum (or section 6).

7.2. The most current version of the NSA S&CI PED listing may be requested from the servicing SSO or PSO. Devices may be added or removed, as the listing is periodically updated. Security officials will review updates to the listing and will notify DAF personnel when their devices are no longer supported. At a minimum, servicing security officials will validate all devices during the annual reauthorization.

7.3. Nothing in this memorandum shall obligate the United States Government in any currently executed contract or contract negotiation. Industry partners shall continue to execute under the guidance and references stipulated under current contracts. DAF officials will update security guidance to include this memorandum, when issuing new contracts or during regular updates to existing contracts, if required.

Attachment 1
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

(a) Defense Intelligence Agency Instruction 8460.002, *Portable Electronic Devices*, 01 May 2014

(b) Office of the National Counterintelligence Executive, *Technical Specifications for the Construction and Management of Sensitive Compartmented Information Facilities*, Version 1.5.1," 26 July 2021

(c) Department of Defense, *Intelligence Information System (DoDIIS) – Joint Security Implementation Guide (DJSIG)*, June 2011

(d) Department of Defense, *Joint Special Access Program (SAP) Implementation Guide (JSIG)*, 11 April 2016

(e) DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 12 April 2022

(f) DoDM 5205.07-V3, *DoD Special Access Program (SAP) Security Manual: Physical Security*, 08 December 2020

(g) Defense Intelligence Agency U-15-0001/CIO-3, *Policy Clarification, Portable Electronic Devices, Introduction and Use of Personal Wearable Fitness Devices and Personal Headphones*, 26 January 2015

(h) Department of Defense Chief Information Officer Memorandum, *Introduction and Use of Wearable Fitness Devices and Headphones within DoD Accredited Spaces and Facilities*, 21 April 2016

(i) Air Force Instruction 33-322, *Records Management and Information Governance Program*, 23 March 2020

(j) Air Force Instruction 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

Prescribed Forms

DAF Form 110, *DAF EMD Request Form & Approval Card*

DAF Form 111, *DAF PWFD Request Form & Approval Card*