INTELLIGENCE COMMUNITY DIRECTIVE 124

TECHNICAL AMENDMENT

Electronic Medical Devices

A. PURPOSE

1. Pursuant to Intelligence Community Directive (ICD) 101, Section G.1.b.(3), technical amendments are hereby made to Intelligence Community Directive 124, *Electronic Medical Devices*, signed 26 April 2024.

2. This Directive, as amended, reflects the signature of Executive Order (EO) 14148, *Initial Recissions of Harmful Executive Orders and Actions*, and EO 14151, *Ending Radical and Wasteful Government DEI Programs and Preferencing*, both issued 20 January 2025. EO 14148 repeals EO 14035, *Diversity, Equity, Inclusion and Accessibility in the Federal Workforce*. This technical amendment also reflects the current structure of the Office of the Director of National Intelligence.

B. EFFECTIVE DATE: This technical amendment becomes effective on the date of signature.

Assistant Director
for Policy and Strategy

March 14, 2025
Date

INTELLIGENCE COMMUNITY DIRECTIVE 124

Electronic Medical Devices

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12333, as amended; the Rehabilitation Act of 1973, as amended; the Privacy Act of 1974, as amended; and other applicable provisions of law.

B. PURPOSE:

1. This Intelligence Community Directive (ICD) establishes policy advancing the Intelligence Community's (IC) commitment to adopting the principle of maximum accessibility for individuals using electronic medical devices (EMD). A consistent and transparent approach to the management and governance of EMDs will:

a. Advance accessibility to attract, maintain, and support a world class workforce; and

b. Assure informed, safe access to Sensitive Compartmented Information Facilities (SCIFs) for individuals with EMDs.

2. This Directive also:

a. Recognizes the need to protect classified information and sensitive operations in accordance with applicable legal and policy requirements; and

b. Rescinds the "Medical Devices" section of E/S 2017-00043, *Wireless Technology in the Intelligence Community*, dated January 19, 2017.

C. APPLICABILITY

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

2. This Directive applies to all SCIFs located in or sponsored by the executive, judicial, and legislative branches of the U.S. Government.

3. This Directive leverages the Food, Drug, and Cosmetic Act, as amended, (see Appendix) to define "electronic medical devices" as those:

a. Available by prescription or over-the-counter;

b. Cleared or approved by the Food and Drug Administration (FDA); and

c. Capable of acquiring, transmitting, receiving, or storing data.

4. For the purposes of this Directive, technology enabled health products (e.g., wearable hydration sensor, personal fitness device, etc.) are not considered EMDs. However, an IC element may approve an individual's use of such devices consistent with accessibility and reasonable accommodation (RA) processes, or when recommended in writing by a licensed medical provider. Reciprocity is not presumed for such devices and may be subject to review by other IC elements.

5. Nothing in this Directive alters or supersedes IC elements' authorities or responsibilities regarding accessibility, RA, and equal employment opportunity (EEO) for individuals with disabilities in accordance with applicable law and policy.

D. POLICY

1. To attract, maintain, and support a world-class workforce, the IC shall make every reasonable effort to permit the use of EMDs within SCIFs.

2. The IC shall take a consistent approach to the management of EMDs to promote workforce mobility and accessibility and to maximize career growth opportunities for EMD users in the IC, to the greatest extent possible.

3. IC elements shall promote accessibility through risk acceptance and risk mitigation to the maximum extent practical.

4. IC elements shall adopt the principle of maximum accessibility for their in-person meetings, conferences, and other such gatherings by first identifying and utilizing their SCIFs approved for widely used and approved EMDs and, in addition, provide virtual options or other arrangements to the greatest extent practical.

5. The Assistant Director of National Intelligence for Human Capital (ADNI/HC) is the Accountable Official for this policy and shall issue IC Standards (ICS) in accordance with ICPG 101.2, *Intelligence Community Standards*, and in coordination with the Director, National Counterintelligence and Security Center (D/NCSC), as necessary, to implement this Directive.

6. The D/NCSC shall coordinate with the ADNI/HC when issuing ICS, in accordance with ICPG 101.2, on counterintelligence, security matters, and the protection of classified information affecting accessibility for individuals with EMDs.

7. All ICS and other IC guidance on matters affecting accessibility for individuals with EMDs shall be issued under this ICD and coordinated with the IC Electronic Medical Device Governance Board and other governance boards as determined by the Accountable Official.

8. *Confidentiality*. The IC shall protect Personally Identifiable Information (PII) including medical information obtained during the EMD review or appeals process, and information that an individual voluntarily discloses, in accordance with applicable laws and policies on confidentiality and privacy. Medical information shall be shared only with those with a need to know and the information disclosed shall be no more than necessary to either process the request or to monitor the presence of the EMD within the SCIF.

9. *Communication.* IC elements shall provide robust communication and current information to the IC workforce, including prior to entry-on-duty, and visitors to SCIFs on the use of EMDs in their SCIFs including but not limited to:

a. Making such information easily discoverable on classified and unclassified websites for employees and visitors including, at a minimum, requirements to self-report EMD use in SCIFs, procedures for requesting EMD approvals and accessing SCIFs, information on rights of appeal, response timeframes, points of contact, and any other relevant informational materials. Classified websites shall also provide, at a minimum, the IC element's policy, including rights of appeal, and other relevant governing documents. IC elements shall also make available a list of approved and denied EMDs to the extent practical; and

b. Advising EMD users of areas which may interfere with the operation and effectiveness of an EMD and clearly mark these areas to avoid accidental entry.

10. The D/NCSC shall advise the ADNI/HC on counterintelligence and security matters related to the use of EMDs including threat streams and risk mitigations in a timely manner.

11. Connecting EMDs to IC information technology systems is prohibited, unless approved in writing by an IC element's Authorizing Official, consistent with ICD 503, *Intelligence Community Information Environment Risk Management.*

E. ELECTRONIC MEDICAL DEVICE REVIEWS

1. *Submitting EMD Requests*

a. EMD users are not permitted to bring EMDs into SCIFs without prior review and approval. EMD users must submit requests and receive approvals for:

(1) New EMDs;

(2) Any change in capabilities of an approved EMD; or

(3) Expiration of prior approval.

b. IC elements shall generally not require a licensed medical provider's note for FDA approved or cleared over-the-counter EMDs as part of the request process.

c. IC elements shall review and approve an EMD request prior to the first-time entry of an EMD into a SCIF.

d. IC elements must clearly communicate procedures for requesting use of an EMD consistent with Section D.9.

2. *Reviewing EMD Requests*

a. IC elements shall review and respond to requests whether submitted through classified or unclassified channels.

b. Reviewing Officials

(1) Requests for EMDs shall be reviewed by no less than two officials at the IC element, to include a representative from security (e.g., Cognizant Security Authority,

Accrediting Official, insider threat program manager, etc.) and at least one workforce representative knowledgeable in accessibility matters (e.g., human resources, EEO, RA, medical services, etc.).

(2) An information technology representative (e.g., Authorizing Official, Chief Information Security Officer, Information System Security Manager, etc.) may also review the request, as appropriate.

(3) In accordance with Section D.8, medical information shall be shared only with those with a need to know and the information disclosed shall be no more than necessary to either process the request or to monitor the presence of the EMD within the SCIF.

c. Review Timeline

(1) The review of and response to EMD requests shall be transparent, timely, and interactive between the EMD user and the IC element.

(2) IC elements shall respond to requests as soon as possible, but no later than 30 calendar days after submission.

(3) IC elements shall expedite urgent or time-sensitive requests (e.g., surgery related, medical testing, etc.).

(4) IC elements should strive to provide arrangements to assist the user until a determination is made.

d. Review Criteria

(1) When reviewing a request for an EMD, IC elements shall consider:

(a) Impact to the user;

(b) Impact to the mission;

(c) Physical and technical capabilities of the EMD;

(d) Physical and technical security mitigations of the SCIF;

(e) Other IC element approvals of the EMD and associated mitigation measures; and

(f) Potential mitigations the IC element could implement to allow the EMD.

3. *Communicating EMD Determinations*

a. EMD Approval

(1) IC elements shall make every effort to approve the EMD first requested by the EMD user.

(a) IC elements may provide the user an EMD that meets security requirements when practical and in accordance with applicable legal and policy requirements.

(2) EMDs shall be approved for the maximum duration possible, but no less than one year, except when EMDs are intended for short-term or temporary use. In such cases, those EMDs shall be approved for the duration requested by the EMD user.

(3) The IC element shall provide a written statement of approval to the user including:

(a) SCIFs for which the EMD is approved (may be consolidated by floor(s), facility, etc., as appropriate);

(b) Duration of the approval;

(c) Any restrictions or risks associated with using the EMD, including areas presenting a potential medical hazard;

(d) Information on the overall security risks posed by EMDs; and

(e) Any other information required to promote workforce mobility, security, and user safety.

(4) The IC element head or designee may accept, in writing, the risk of the EMD entering a SCIF.

(a) For co-use (or joint-use) SCIFs, the host IC element head or designee shall promptly notify co-use tenants of such acceptance, in writing.

(b) If the co-use tenant of the SCIF is a non-IC element, then the host IC element head or designee shall promptly notify the SCIF site security officer, in writing.

(5) The Cognizant Security Authority and the Accrediting Official shall be informed, in writing, of EMD request approvals for their respective SCIFs.

(6) As determined by the IC element, if the threat level, security risk, or areas of approval/restriction change for a previously approved EMD, the IC element shall notify the requestor and re-evaluate the approval of the EMD.

b. EMD Denial

(1) If the risks posed by the EMD's capabilities cannot be sufficiently mitigated or are not accepted, the EMD request will be denied.

(2) The IC element shall provide the user a written statement of denial including information on the risks posed by the EMD and the criteria used to review the EMD.

(a) The written statement of denial shall also include a rationale for the denial that provides sufficient detail and is written such that a reasonable person without related subject-matter expertise will understand the determination.

(b) The statement shall also include unclassified information that the user may share with their medical provider or refer to as needed.

(3) Any denial shall be accompanied by all information needed to initiate an appeal and, if applicable, the IC element's policy and procedures for requesting a RA.

4. *EMD Reciprocity*

a. IC element heads or designees shall reciprocally accept a user's EMD approval from other IC elements to the greatest extent practical.

b. To promote workforce mobility and reciprocity, EMDs shall be approved for as many of the IC element's SCIFs within a geographic region, to the greatest extent practical.

(1) At a minimum, IC elements should strive to approve an EMD for use at all of their SCIFs within the Washington D.C. Metropolitan Area (WMA) to promote ease of workforce mobility across IC element headquarters. For the purposes of this ICD, the WMA includes the District of Columbia, the cities of Alexandria, Falls Church, and Fairfax, Virginia; the counties of Arlington, Fairfax, Loudoun, Prince William, Fauquier, and Culpeper, Virginia; and the counties of Baltimore, Anne Arundel, Montgomery, Howard, Frederick, and Prince George's, Maryland.

F. APPEALS

1. IC elements shall establish a process for users to appeal a denied request.

a. Any EMD user may request an appeal.

b. A user may only appeal a denied request once.

c. IC elements shall review and respond to appeal requests whether submitted through classified or unclassified channels.

2. Appeal Review and Decision

a. The appeal shall be reviewed by the IC element head or designee. The designee shall be from an office not involved in the initial EMD review and determination; be authorized to make an element-level determination; and have oversight over the various stakeholders, such as the Chief of Staff or Chief Operating Officer.

b. IC elements shall notify the requestor within 15 calendar days after submission. IC elements shall expedite urgent or time-sensitive requests.

3. If there is a change in the capabilities of the EMD or a change in the SCIF's security measures, a new request for review should be submitted in accordance with Section E.

4. If applicable, EMD users may also engage in the RA process referenced in Section C.5.

G. IC ELECTRONIC MEDICAL DEVICE GOVERNANCE BOARD

1. The IC EMD Governance Board (IC EMDGB) will serve as the primary IC forum for the oversight and governance of EMDs. The IC EMDGB will:

a. Develop strategies to address emerging EMD technology;

b. Promote strategic communications and awareness of EMD policies and procedures;

c. Encourage consistent processes;

d. Advance workforce mobility; and

e. Ensure secure use of EMDs.

2. To promote reciprocity, reduce duplicative efforts, and expedite the review process, the IC EMDGB shall also serve as the primary IC forum for information sharing, including best practices and, to the maximum extent practical:

a. All information on EMD capabilities, testing and evaluation plans, and methods used to determine those capabilities;

b. All information on threat streams relating to the use of EMDs;

c. Best practices for accommodating EMDs, information on emerging technology, and methods and approaches for mitigating the associated physical and technical security risks; and

d. Each IC element's list of approved and denied EMDs.

3. The Board will periodically review and evaluate all IC elements' lists of approved and denied EMDs to promote consistency and reciprocity across the IC.

4. The IC EMDGB shall be co-chaired by the ADNI/HC and the D/NCSC or their designees.

a. The co-chairs shall:

(1) Be responsible for overseeing, governing, and improving the IC state of practice for the use of EMDs;

(2) Keep IC element heads apprised of such state of practice; and

(3) Develop and maintain an IC Charter in accordance with E/S 2021-01996, *IC Charters*.

b. The Chief, Civil Liberties, Privacy, and Transparency (CLPT) or designee shall attend as an advisor on civil liberties, privacy, and transparency matters related to the use of EMDs.

c. IC elements shall designate a senior executive-level official to serve as an IC EMDGB member who is authorized to make decisions on behalf of the IC element and will represent their element's collective equities and expertise such as medical, security, facilities, information technology, RA, EEO, human resources, civil liberties, and privacy and transparency.

H. ROLES AND RESPONSIBILITIES

1. The ADNI/HC shall:

a. Serve as the Accountable Official for this Directive and develop and promulgate ICS, in accordance with ICPG 101.2, and other guidance as necessary, to implement this Directive. All ICS shall be coordinated by the IC EMDGB;

b. Co-chair the IC EMDGB with the D/NCSC as described in Section G; and

c. Provide a report to the DNI, in consultation with the D/NCSC, at least annually on the overall state of practice for the use of EMDs in the IC, including supporting metrics, current threat and security information, implementation efforts including their impact on the workforce, and other information as directed by the DNI or PDDNI.

2. The D/NCSC shall:

a. Coordinate with the ADNI/HC when issuing ICS, in accordance with ICPG 101.2, on counterintelligence, security matters, and the protection of classified information affecting accessibility for individuals with EMDs;

b. Co-chair the IC EMDGB with the ADNI/HC as described in Section G;

c. Advise the ADNI/HC on counterintelligence and security matters related to the use of EMDs including threat streams and risk mitigations in a timely manner; and

d. Advise the ADNI/HC on, and provide counterintelligence and security related information for incorporation into, the annual report to the DNI.

3. The Chief, CLPT shall:

a. Advise the ADNI/HC and the D/NCSC on civil liberties, privacy, and transparency matters related to the use of EMDs; and

b. Designate a senior representative to serve as an advisor to the IC EMDGB on civil liberties, privacy, and transparency matters related to the use of EMDs.

4. IC elements shall:

a. Establish or revise internal policies and processes to implement and be consistent with this Directive and promote reciprocity;

b. Protect PII including medical information in accordance with applicable laws and policies on confidentiality and privacy;

c. Process EMD requests and conduct EMD reviews in accordance with Section E;

d. Establish a process for appeals in accordance with Section F;

e. Conduct in-person meetings, conferences, and other such gatherings in their SCIFs established as safe for widely used and approved EMDs and provide virtual options or other arrangements to the greatest extent practical;

f. Provide robust communication and current information on the use of EMDs in accordance with Section D.9;

g. Share information on EMDs and best practices with other IC elements and the IC EMDGB;

h. Establish processes to collect and provide metrics to support the annual report to the DNI. Metrics shall be internally reviewed to identify trends to inform and ensure internal policies and processes reflect current best practices; and

i. Designate a senior executive-level representative to serve on the IC EMDGB in accordance with Section G.4.c.

I. EFFECTIVE DATE: This Directive becomes effective on the date of signature.

//SIGNED// Avril D. Haines
Director of National Intelligence

April 26, 2024
Date

Appendix - Definition

For the purposes of this ICD, the following terms are defined in accordance with The Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. Sections 321-399i.

Per 21 U.S.C. 321(h)

(1) A medical device is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component, part, or accessory which is:

(A) Recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;

(B) Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or

(C) Intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to 21 U.S.C. Section 360j(o).

Per 21 U.S.C. 360j(o)

(1) The term device, as defined in 21 U.S.C. Section 321(h) shall not include a software function that is intended:

(A) for administrative support of a health care facility, including the processing and maintenance of financial records, claims or billing information, appointment schedules, business analytics, information about patient populations, admissions, practice and inventory management, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, and laboratory workflow;

(B) for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition;

(C) to serve as electronic patient records, including patient-provided information, to the extent that such records are intended to transfer, store, convert formats, or display the equivalent of a paper medical chart, so long as:

(i) such records were created, stored, transferred, or reviewed by health care professionals, or by individuals working under supervision of such professionals;

(ii) such records are part of health information technology that is certified under section 300jj-11(c)(5) of Title 42; and

(iii) such function is not intended to interpret or analyze patient records, including medical image data, for the purpose of the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition;

(D) for transferring, storing, converting formats, or displaying clinical laboratory test or other device data and results, findings by a health care professional with respect to such data and results, general information about such findings, and general background information about such laboratory test or other device, unless such function is intended to interpret or analyze clinical laboratory test or other device data, results, and findings; or

(E) Unless the function is intended to acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or a signal from a signal acquisition system, for the purposes of:

(i) Displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

(ii) Supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and

(iii) Enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any such recommendations to make a clinical diagnosis or treatment decisions regarding an individual patient.

(2) In the case of a product with multiple functions that contains:

(A) At least one software function that meets the criteria under paragraph (1) or that otherwise does not meet the definition of device undersection 21 U.S.C. Section 321(h); and

(B) At least one function that does not meet the criteria under paragraph (1) and that otherwise meets the definition of a device undersection 21 U.S.C. Section 321(h), the Secretary of Health and Human Services shall not regulate the software function of a such a product described in subparagraph (A) as a device. Notwithstanding the preceding sentence, when assessing the safety and effectiveness of the device function or functions of such product described in subparagraph (B), the Secretary of Health and Human Services may assess the impact that the software function or functions described in subparagraph (A) have on such a device function or functions.

(3) (A) Notwithstanding paragraph (1), a software function described in subparagraph (C), (D), (E) or paragraph (1) shall not be excluded from the definition of device under 21 U.S.C. Section 321(h) if:

(i) The Secretary of Health and Human Services makes a finding that use of such software functions would be reasonably likely to have serious adverse health consequences; and

(ii) The Software function has been identified in a final order issued by the Secretary of Health and Human Services under subparagraph (B)

(B) Subparagraph (A) shall only apply if the Secretary of Health and Human Services:

(i) Publishes a notification and proposed order in the Federal Registrar;

(ii) Includes in such notification the Secretary of Health and Human Services' finding, including the rationale and identification of the evidence on which such finding was based, as described in subparagraph (A)(i); and

(iii) Provides for a period of not less than 30 calendar days for public comment before issuing a final order or withdrawing such proposed order.

(C) In making a finding under subparagraph (A)(i) with respect to a software function, the Secretary of Health and Human Services shall consider:

(i) The likelihood and severity of patient harm if the software function were not to perform as intended;

(ii) The extent to which the software function is intended to support the clinical judgment of a health care professional;

(iii) Whether there is a reasonable opportunity for a health care professional to review the basis of the information or treatment recommendation provided by the software function; and

(iv) The intended user and user environment, such as whether a health care professional will use a software function of a type described in subparagraph (E) of paragraph (1)

(4) Nothing in this subsection shall be construed as limiting the authority of the Secretary of Health and Human Services to:

(A) Exercise enforcement discretion as to any device subject to regulation under this chapter;

(B) Regulate software used in the manufacture and transfusion of blood and blood components to assist in the prevention of disease in humans; or

(C) Regulate software as a device under this chapter is such software meets the criteria under 21 U.S.C. Section 360c(a)(1)(C).