MACH COALITION DATA PRIVACY AND BREACH RESPONSE POLICY

Military Aviator Coalition for Health

16 JUL 26

Effective Upon Receipt Until Superseded

1. Purpose

This Data Privacy and Breach Response Policy ("Policy") establishes how the Military Aviator Coalition for Health ("MACH" or "the Coalition") safeguards personal and health information in its custody, and how MACH responds to, investigates, and provides notification of a security incident involving that information. This Policy implements, and should be read together with, the data protection provisions of the MACH Records Retention Policy.

2. Policy Statement

MACH is committed to protecting the personal and health information entrusted to it by donors, volunteers, veterans, aviators, and their families, and to responding promptly and lawfully in the event that information is lost, stolen, or accessed without authorization. This Policy is intended to satisfy MACH's obligations under applicable Virginia law, including the Commonwealth's breach notification statutes, and to reflect sound practice for a small, all-volunteer nonprofit organization. The Virginia Consumer Data Protection Act, Va. Code §§ 59.1-575 through 59.1-584, does not apply to MACH. That statute exempts nonprofit organizations at the entity level, regardless of the volume of personal data an organization processes, consistent with Va. Code § 59.1-576(B). MACH volunteers and officers should understand that this Policy's obligations arise from Virginia's breach notification statutes described in Section 7, not from the Virginia Consumer Data Protection Act.

3. Applicability

This Policy applies to all Personal Information and Protected Health Information created, received, or maintained by MACH in connection with its activities, regardless of physical or

electronic format, and to all individuals serving MACH in a volunteer capacity, including but not limited to Board members, officers, committee members, and general volunteers. MACH's Board of Directors recognizes that Section 4.15 of the MACH bylaws contemplates the possibility of compensated Board member or staff positions in the future. In the event MACH establishes any compensated position, this Policy shall apply equally to that position. This is a living document and as such is eligible for and subject to change when directed by the MACH Board.

4. Definitions

A. "*Personal Information*" has the meaning given to that term in Va. Code Ann. § 18.2-186.6, and generally means a person's first name or first initial and last name in combination with a data element such as a Social Security number, driver's license or state identification number, financial account or payment card number in combination with any required access code, passport number, or military identification number, where neither the name nor the data element is encrypted or redacted.

B. "*Protected Health Information*" means information regarding an individual's medical history, mental or physical condition, or treatment, of the kind addressed by Va. Code Ann. § 32.1-127.1:05, including case narratives and personal health information described in the MACH Records Retention Policy.

C. "*Security Incident*" means any suspected or confirmed unauthorized access to, acquisition of, loss of, or disclosure of a Record containing Personal Information or Protected Health Information, whether the Record is in paper or electronic form.

D. "*Breach of the Security of the System*" has the meaning given to that term in Va. Code Ann. § 18.2-186.6 and generally means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of Personal Information and that causes, or that MACH reasonably believes has caused or will cause, identity theft or other fraud to a resident of the Commonwealth.

E. "*Record*" has the meaning given to that term in the MACH Records Retention Policy.

5. Data Protection Practices

MACH shall take reasonable steps to protect Records containing Personal Information or Protected Health Information from unauthorized access, consistent with Section 7 of the MACH Records Retention Policy. Where a Record containing Personal Information or Protected Health Information is created or stored on a third-party platform or service used on MACH's behalf, MACH shall take reasonable steps to confirm that the platform or service maintains reasonable safeguards for that information. Access to Records containing Protected Health Information (PHI) shall be limited to individuals with a legitimate need to access that information in connection with MACH's mission and advocacy activities.

6. Incident Response Procedure

A. A volunteer, officer, or Board member who discovers or reasonably suspects a Security Incident shall promptly report it to the Director.

B. Upon becoming aware of a Security Incident, the Director shall promptly notify the Board and *take reasonable steps to contain the incident*, assess its scope, and determine what Personal Information or Protected Health Information may have been affected.

C. The Director, in consultation with the Board, shall determine whether the Security Incident constitutes a Breach of the Security of the System requiring notification under Section 7 of this Policy. Where there is uncertainty, MACH shall consult legal counsel.

D. Nothing in this Section shall be construed to delay reasonable, immediate steps to prevent further unauthorized access, including disabling compromised credentials, systems, or accounts.

7. Notification Requirements

A. **General Personal Information**. Where a Security Incident constitutes a Breach of the Security of the System involving Personal Information, MACH shall notify the Office of the Attorney General of Virginia and each affected Virginia resident without unreasonable delay, consistent with Va. Code Ann. § 18.2-186.6. Notice may be reasonably delayed to determine the scope of the breach, restore the reasonable integrity of the affected system, or at the request of a law-enforcement agency.

B. **Protected Health Information**. Where a Security Incident involves Protected Health Information, MACH shall provide notification to the subject of that information and, where the affected individual is a different person, to any affected Virginia resident, consistent with Va. Code Ann. § 32.1-127.1:05.

C. **Consumer Reporting Agencies**. If MACH provides notification to more than 1,000 persons at one time under this Section, MACH shall also notify, without unreasonable delay, all nationwide consumer reporting agencies, consistent with Va. Code Ann. § 18.2-186.6.

D. Nothing in this Section shall be construed to require notification where MACH reasonably believes, after a good-faith investigation, that *a Security Incident has not caused* and will not cause identity theft or other fraud to any affected individual.

8. Notice Content and Method

Notice provided under Section 7 shall include, to the extent known: a general description of the incident; the *type of Personal Information or Protected Health Information involved*; the general steps MACH has taken to protect the information from further unauthorized access; a telephone number the recipient may call for further information, if one exists; and advice directing the recipient to remain vigilant by reviewing account statements and monitoring credit reports. Notice may be provided in writing to the recipient's last known address, by telephone, by electronic notice, or, where permitted by applicable law, by substitute notice.

9. Recordkeeping

MACH shall maintain a written record of each Security Incident, including the date of discovery, a description of the incident, the Director's assessment under Section 6, and any notification provided under Section 7. Records of a Security Incident shall be retained consistent with the MACH Records Retention Policy, and shall not be destroyed while a Legal Hold applies to that Security Incident under the MACH Records Retention Policy.

10. Responsible Parties

A. The Director is responsible for overall administration of this Policy, for leading MACH's response to a Security Incident, and for determining whether notification is required under Section 7.

B. The Secretary is responsible for screening Board and committee meeting minutes for personal information consistent with Section 6.7(b)(i) of the MACH bylaws, and for promptly notifying the Director where that screening reveals a suspected Security Incident.

C. The Board is responsible for reviewing the Director's assessment of a Security Incident and for approving any notification provided under Section 7.

D. Each Board member, officer, and volunteer is responsible for promptly reporting a suspected Security Incident consistent with Section 6(A) of this Policy.

11. Relationship to Other MACH Policies

This Policy works together with, and does not replace, the confidentiality provisions of Section 6 of the MACH Whistleblower Protection Policy and the data protection provisions of Section 7 of the MACH Records Retention Policy. Where this Policy and another MACH policy address the same subject matter, the more protective provision shall control.

12. Administration and Review

This Policy is administered by the MACH Board of Directors and may be amended by the Board as future circumstances warrant. This Policy will be reviewed annually and will remain in effect until superseded or modified by any other MACH document. In addition to the Board's annual review, MACH shall periodically consult legal counsel to confirm that this Policy remains consistent with applicable law. This Policy will be publicly visible on the MACH website, www.milaviator.org. Where this Policy is amended, the provisions in effect at the time of a given Security Incident shall govern MACH's response to that Security Incident. An amended version of this Policy shall apply only to a Security Incident discovered after that amended version is in full force and effect, as measured from the date of Board enactment stated at the end of this Policy.

13. Acknowledgment

Each individual serving as a MACH Board member or officer shall read this Policy and sign Attachment A, Attestation of Review. The Director shall receive and file all attestations executed under this Section. If such an individual reports that he/she has not reviewed this Policy, that

individual will be suspended pending a documented review of this Policy, after which that individual may be reinstated by the Board to resume such duties.

Enacted by the MACH Board on: _____

Attachment A: Attestation of Review

MACH Coalition Data Privacy and Breach Response Policy

I, the undersigned, attest that I have received, read, and reviewed the MACH Coalition Data Privacy and Breach Response Policy, and that I understand and agree to comply with the responsibilities it assigns to my role with MACH.

Printed Name: _____

MACH Role: _____

Signature: _____

Date: _____