DEPARTMENT OF DEFENSE
United States Military Entrance Processing Command

INSTRUCTION

Personally Identifiable Information (PII) and Protected Health Information (PHI) Incident Reporting and Breach Notification Procedures

Human Resources Directorate
Programs Division (J-1/MEHR-PR)

USMEPCOM INST 25-52-1
February 24, 2017

PURPOSE. This Instruction provides USMEPCOM policy on how to properly report any loss, theft, or compromise (actual or suspected) of PII/PHI. The USMEPCOM Privacy Act Officer is responsible for all PII and PHI related reporting.

REFERENCES. Army Regulation (AR) 25-22, *The Army Privacy Program*; Department of Defense Directive (DoDD) 5400.11, *DoD Privacy Program;* Department of Defense Instruction *(*DoDI) 6025.18, *Privacy of Individually Identifiable Health Information in DoD Health Care Programs*; U.S. Department of Health and Human Services, *Health Information Privacy*; Records Management and Declassification Agency (RMDA)

APPLICABILITY. This instruction applies to every level of hierarchy (e.g., section, branch, division, group, etc.) within Military Entrance Processing Stations (MEPS), Battalions, Sectors, Headquarters Special Staff Offices and Directorates.

MANAGERS' INTERNAL CONTROL PROGRAM. Not applicable.

RELEASABILITY – UNLIMITED. This instruction is approved for internal use only.

SUPPLEMENTATION. Supplementation of this instruction is prohibited without prior approval from HQ USMEPCOM, ATTN: J-1/MEHR-PR, 2834 Green Bay Road, North Chicago, IL 60064-3091.

POLICY RESOURCE PAGE. https://spear/Headquarters/J-1%20MEHR/ProgramsDiv/SitePages/CONG.aspx

EFFECTIVE DATE. February 24, 2017.

STEPRO.JOSEPH.RICHARD.JR.1152853030
Digitally signed by STEPRO.JOSEPH.RICHARD.JR.1152853030
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=STEPRO.JOSEPH.RICHARD.JR.1152853030
Date: 2017.03.27 13:19:50 -05'00'

Joseph R. Stepro, Jr.
Director, J-1/Human Resources

TABLE OF CONTENTS

CHAPTER 1

POLICY

1.1. POLICY. It is USMEPCOM policy that:

1.1.1. PII/PHI breaches will be reported immediately as instructed in Chapter 2 of this Instruction.

1.1.2. PII/PHI maintained within USMEPCOM as a result of USMEPCOM operations will be safeguarded to the maximum extent possible.

1.1.2.1. Safeguarding refers to protecting PII/PHI from loss, theft, or misuse while simultaneously supporting USMEPCOM's mission.

1.1.2.2. Safeguards are protective measures USMEPCOM takes to prevent unauthorized access to or disclosure of PII/PHI.

1.1.2.3. Safeguards are used to protect USMEPCOM from "reasonably anticipated threats."

1.2. PII DEFINITION.

1.2.1. PII is information that identifies, links, relates, is unique to, or describes an individual.

1.2.2. PII is not anchored to any single category of information or technology. Non-PII can become PII when information is publicly available and when combined could identify an individual.

1.2.3. Examples of PII Data:

1.2.3.1. Name, such as full name, maiden name, mother's maiden name, or alias.

1.2.3.2. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account or credit card number, and Department of Defense Identification (ID) number.

1.2.3.3. Address information, such as street address or email address.

1.2.3.4. Telephone numbers, including mobile, business, and personal numbers.

1.2.3.5. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry).

1.2.3.6. Information identifying personally owned property, such as vehicle registration number or title number and related information.

1.2.3.7. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, age, place of birth, race, religion, weight, activities, geographical indicators, demographic information, employment information, security clearance information, medical information, education information, financial information, drug test results, criminal history, marital status, and family information).

1.3. PHI DEFINITION.

1.3.1. PHI is individually identifiable health information that is maintained or transmitted by electronic or any other form or medium.

1.3.2. Individually identifiable health information is a subset of health information, including demographic information collected from an individual, and:

1.3.2.1 Relates to the past, present, or future physical or mental health or condition of an individual;

1.3.2.2. That identifies the individual; or

1.3.2.3. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

1.4. PII TRAINING. For further information regarding PII breaches, procedures, and training please visit the RMDA website: www.rmda.army.mil (click on the Privacy Tab).

1.5. PHI TRAINING. For further information regarding PHI breaches, procedures, and training please visit the Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/breach-notification/.

CHAPTER 2

REPORTING PROCEDURES

2.1. REPORTING PROCEDURES (FOR HQ, SECTORS, BATTALIONS, MEPS).

2.1.1. Report any loss, theft, or compromise of PII/PHI (actual or suspected) to the USMEPCOM FOIA/Privacy Act Officer within one hour of being identified. USMEPCOM organizations (MEPS, BNs, Sectors, Directorates, SSOs) are to thoroughly document the circumstances of all breaches of PII/PHI.

2.1.2. Submit a STARNET Report identifying the loss, theft, or compromise of PII/PHI (actual or suspected).

2.1.2.1. Ensure the STARNET does not contain any PII/PHI.

2.1.3. ***Do not delay reporting in order to provide details (i.e., root cause, vulnerabilities exploited, or mitigation actions) as this may result in an increased risk to the individuals concerned or enterprise system.***

2.1.4. Complete DD 2959, *Breach of Personally Identifiable Information Report* to report the loss, theft, or compromise of PII/PHI (actual or suspected). Reports will be submitted electronically to the USMEPCOM FOIA/Privacy Act Officer at: osd.north-chicago.usmepcom.list.hq-j1-mehr-foia-info@mail.mil.

2.1.5. Provide the USMEPCOM FOIA/Privacy Act Officer a detailed list via Excel Spreadsheet of the affected persons, via encrypted email. Include the following information:

2.1.5.1. Full name of affected individual(s)

2.1.5.2. Social Security Number

2.1.5.3. Gender

2.1.5.4. Complete mailing address

2.1.5.5. Telephone number

2.1.5.6. If individual is under 18 years of age, include contact information of parent or guardian (name, address, and telephone number)

2.2. REPORTING PROCEDURES (FOR FOIA/PRIVACY ACT OFFICER).

2.2.1. The USMEPCOM FOIA/Privacy Act Officer will notify the United States Computer Emergency Readiness Team (US-CERT) using the US-CERT Incident Reporting System. Notification will be made within one hour of discovery of a loss, theft, or compromise of PII/PHI (actual or suspected).

2.2.2. The USMEPCOM FOIA/Privacy Act Officer will notify HQDA Privacy Office and Army G-6 via email to usarmy.belvoir.hqda-oaa-ahs-mbx.rmda-foia-privacy-alert.mil@mail.mil as well as via the Privacy Act Tracking System (PATS) within 24 hours of notification of a loss, theft, or compromise of PII/PHI (actual or suspected).

2.2.3. The USMEPCOM FOIA/Privacy Act Officer will notify affected individuals of compromised PII by U.S. mail within 10 days of compromise if deemed appropriate based on the risk assessment.

2.2.4. The USMEPCOM FOIA/Privacy Act Officer will notify Defense Health Agency within 24 hours of notification of loss, theft, or compromise of PHI (actual or suspected).

2.2.4.1. Additional information regarding HIPAA Breach Notification policy can be found at the following hyperlink: http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

2.2.5. The USMEPCOM FOIA/Privacy Act Officer will interact with all necessary parties within USMEPCOM when alerted of a potential or actual breach. This includes, but is not limited to: the Staff Judge Advocate, Public Affairs, J-6, J-7, and the Designated Command Representative (defined by USMEPCOM as either the Deputy Commander/Chief of Staff or the Commander) that will be the decision maker regarding the actions to take by USMEPCOM. Coordination between the FOIA/Privacy Act Officer and these Special Staff Offices and Directorates will continue throughout the entire reporting and notification process.

CHAPTER 3

PII/PHI BREACH REPORTING TEMPLATE, UPDATES, NOTIFICATION, REMEDIAL ACTIONS, AND RISK ANALYSIS

3.1. TEMPLATE

3.1.1. USMEPCOM personnel will use the DD 2959, *Breach of Personally Identifiable Information Report* to report every PII/PHI breach in accordance with paragraph 2.1.4.

3.2. REPORT UPDATES

3.2.1. Report updates will be made by the affected unit or organization (i.e., MEPS, Directorate, SSO, etc.) to the USMEPCOM Privacy Officer who in turn will report updates to the U. S. Army Privacy Office.

3.2.2. Personnel will complete report updates to initial PII/PHI breach reports to ensure a complete report is filed. For example, complete a reporting update and include:

3.2.2.1. The number of individuals affected by the breach now known (it was reported as unknown on the initial report).

3.3. NOTIFICATION PROCEDURES

3.3.1. Notification procedures to affected individuals deemed at **high risk** of identity theft.

3.3.1.1. The USMEPCOM Privacy Officer must notify affected individuals deemed at high risk of identity theft. The affected individuals must be notified as soon as possible, but no later than 10 days after the loss or compromise (or potential loss/compromise) of PII/PHI is discovered. USMEPCOM must continue its efforts to promote a culture to continuously "think privacy" and act swiftly to develop and implement effective breach mitigation plans. Our challenge is that no two breaches of PII involve the exact same circumstances, personnel, systems, or information. A case-by-case analysis combined with the use of best judgment is required for effective breach management. The determination whether to notify individuals of a breach is based on an assessment of the likelihood that the individual will be harmed as a result of the breach and its impact. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional distress and loss of self-esteem. See paragraph 3.5 for the five factors that must be weighed to assess the likely risk of harm.

3.3.1.2. A formal decision regarding whether to make notification cannot be made until after each factor has been assessed. The decision to notify should not be based on one factor alone. For example, a breach may involve SSNs making that factor a high risk. However, SSNs may be stored on an encrypted, Common Access Card-enabled laptop to mitigate potential compromise which could lead to harm. Therefore, although one factor (in this example data elements) rates as a high likelihood of harm, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place. Generally, absent other factors, USMEPCOM should not notify personnel of breaches that have a low overall likelihood of harm. USMEPCOM should remain cognizant of the effect that unnecessary notification may have on the public. Notification when there is little or no risk of harm might create unnecessary concern and confusion. Additionally, overzealous notifications resulting from notification criteria which are too strict could render all such notifications less effective because consumers could become numb to them and fail to act when risks are truly significant.

3.3.1.3. The USMEPCOM Privacy Officer will coordinate with the USMEPCOM Office of the Staff Judge Advocate prior to sending the notification letter. At a minimum, the notification letter will advise the individuals of the following: specific data involved; circumstances surrounding the loss, theft, or compromise; a statement as to whether the information was protected; for example, encrypted; and protective actions the individual can take to minimize their risk.

3.3.1.4. When the organization or unit where the incident occurred is unknown, by default the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notification should be made by an individual at a senior level (such as, Commanders, Directors, Special Staff Officers) to reinforce to impacted individuals the seriousness of the incident.

3.4. REMEDIAL ACTIONS

3.4.1. Commanders, Directors, Special Staff Officers and Supervisors will ensure the appropriate remedial action(s) are taken when PII/PHI is lost or compromised or suspected to be lost or compromised. At a minimum, if PII/PHI is lost as a result of negligence or failure to follow established procedures, the individual(s) responsible will receive counseling and additional training reminding them of the importance of safeguarding PII/PHI. Additional remedial actions may include prompt removal of authority to access information or systems from individuals who demonstrate a pattern of error in safeguarding PII/PHI, as well as other administrative or disciplinary actions as determined appropriate by the Commander, Director, Special Staff Officer or Supervisor.

3.5. IDENTITY THEFT RISK ANALYSIS

3.5.1. USMEPCOM will consider the five factors identified below when assessing the likelihood of risk and/or harm. It is difficult to characterize data elements as creating low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

3.5.1.1. **Nature of the data elements breached**. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names in conjunction with SSNs, and/or dates of birth may pose a high level of risk or harm, while a theft of a database containing only names of individuals may pose a lower risk, depending on its context.

3.5.1.2. **Number of individuals affected**. The magnitude of the number of affected individuals may dictate the method you choose for providing notification, but not be the only determining factor for whether an agency should provide notification.

3.5.1.3. **Likelihood the information is accessible and usable**. Upon learning of a breach, agencies should assess the likelihood that PII/PHI will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the decision to notify the affected individual.

3.5.1.3.1. Depending on the number of physical, technological, and procedural safeguards employed by the agency, the fact that information has been lost or stolen does not necessarily mean it has been accessed by unauthorized individuals. If the information is properly protected by encryption, for

example, the risk of compromise may be low to nonexistent. In this context, proper protection means encryption has been validated by the National Institute of Standards and Technology (NIST).

3.5.1.3.2. Agencies will first need to assess whether the breach involving PII/PHI is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual of group of individuals. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individuals will know the value of the information and either use or sell the information to others.

3.5.1.4. **Likelihood the breach may lead to harm.**

3.5.1.4.1. Broad reach of potential harm. The Privacy Act requires agencies to protect against an anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Additionally, agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential of blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

3.5.1.4.2. Likelihood harm will occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. SSNs and account information are useful for committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other PII, the loss may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease.

3.5.1.5. **Ability of the agency to mitigate risk of harm.** Within an automated information system, the risk of harm will depend on how USMEPCOM is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of personal information and patterns of suspicious behavior should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

3.5.2. All breaches of PII/PHI, whether actual or suspected, require the USMEPCOM Privacy Officer to make notification to US-CERT. Low and moderate risk/harm determinations and the decision whether notification to the individual(s) is made, rest with the head of the organization (USMEPCOM Commander) where the breach occurred. All determinations of high risk/harm require notification by the USMEPCOM Commander.