Revised August 2018

Guidelines for Reporting Breaches

Purpose:

Protecting the privacy and security of personally identifiable information (PII) and protected health information (PHI) is the responsibility of all Defense Health Agency (DHA) workforce members. All of DHA must adhere to the reporting and notification requirements set forth in the DHA Administrative Instruction #71, "Incident Response Team and Breach Response Requirements," September 15, 2015, or its successor issuance; Department of Defense (DoD) 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, or its successor issuance; and DoD 6025.18-R, "Department of Defense Health Information Privacy Regulation," January 24, 2003, or its successor issuance. Please visit https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI for more information.

Definition:

DoD Directive 5400.11, "Department of Defense Privacy Program," October 29, 2014, defines a breach as follows:

"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic."

The DHA Privacy and Civil Liberties Office will determine whether a breach meets the requirements of reporting to the Department of Health and Human Services (HHS).

Guidance:

This document outlines the DoD Reporting and Notification Requirements for breaches:

1. Notify your Supervisor/Director (immediately, upon discovery)
2. *Notify the United States Computer Emergency Readiness Team (within 1 hour for potential and confirmed cyber-security related breaches, e.g., not a paper breach)*
3. Notify the DHA Privacy and Civil Liberties Office within 1 hour at DHA.PrivacyOfficer@mail.mil or (703) 275-6363*
    - Report using the DoD breach reporting form (DD Form 2959), which is available on the DHA Privacy and Civil Liberties Office website referenced above
    - Report to the Contracting Officer within 24 hours
4. Notify the Defense Privacy, Civil Liberties, and Transparency Division and Component Head (within 48 hours) (completed by the DHA Privacy Office)
5. Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if required by the DHA Privacy Office
6. Notify law enforcement authorities, if necessary
7. Notify issuing banks if government issued credit cards are involved

If PHI is involved, please refer to DHA Privacy and Civil Liberties Office guidance for additional breach reporting and notification actions as required by the HHS Final Omnibus Rule and Title 45, CFR, Parts 160 and 164.

Breaches often occur when PII or PHI is mishandled. Examples of these types of breaches may include, but are not limited to:

- Misdirected fax documents that reach anyone other than the intended recipient
- Failing to properly secure documents when mailing or transporting
- Lost or stolen removable media devices (e.g., laptops, thumb drives, compact discs)
- Transmission of unsecured e-mails and unencrypted files
- Unauthorized access to computer systems
- Inappropriate disposal of documents
- Inadvertent posting on the internet

*If email is down, please call (703)-275-6363 to report the breach and follow up with the DD Form 2959 when email becomes available.