DEPARTMENT OF THE ARMY
OFFICE OF THE ADMINISTRATIVE ASSISTANT TO THE SECRETARY
105 ARMY PENTAGON
WASHINGTON DC 20310-0105

AAHS-ZA (25-22g)

23 May 2022

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Preventing Personally Identifiable Information Breaches

1. Reference Department of Defense (DoD) Instruction 5400.11 (DoD Privacy and Civil Liberties Programs), 29 January 2019, incorporating change 1, effective 8 December 2020.

2. DoD Instruction 5400.11 requires Department of the Army Privacy and Civil Liberties Officers (PCLOs) to implement formal breach management policies and to provide adequate training and awareness for employees and contractors on reporting and responding to breaches of PII.

3. The enclosed PII Breach Fact Sheet provides examples of PII, clarifies what constitutes a breach and the common causes of breaches, and offers breach prevention strategies. I ask that all Army PCLOs encourage the use of this fact sheet throughout all Army commands, Army service component commands, and direct reporting units.

4. The point of contact is Ms. Joyce M. Luton, at joyce.luton2.civ@army.mil.

SMITH.CHRISTIE.P.1117722860
Digitally signed by SMITH.CHRISTIE.P.1117722860
Date: 2022.05.23 21:01:14 -04'00'

CHRISTIE P. SMITH
Acting Senior Component Official
for Privacy

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
U.S. Army Europe and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
(CONT)
DISTRIBUTION: (CONT)
U.S. Army Special Operations Command

Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Human Resources Command
Superintendent, U.S. Military Academy
Director, U.S. Army Acquisition Support Center
Superintendent, Arlington National Cemetery
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency

CF:
Director of Business Transformation
Commander, Eighth Army

ARMY PRIVACY OFFICE: Personally Identifiable Information (PII) Breach Fact Sheet

What is a PII breach? The actual or possible loss of control, unauthorized disclosure, or unauthorized access of personally identifiable information (PII) where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.

Examples of PII:

- Social Security Number (Standalone–full or in ANY form)
- date of birth
- home/cell phone number
- financial information
- DoD ID
- protected health information (PHI)
- Inmate Registration Number

What can you do to prevent a PII breach?

As a Department of Army employee, you are entrusted with safeguarding PII contained in any command documents and system of records. **You have a responsibility to**—

- Encrypt the email message and ensure the email recipients have a "need to know." (Forward emails with PII only to email recipients who have a need to know.)
- Lock your computer before walking away AND secure any PII on your desk before leaving for the end of the day.
- Before printing a document containing PII, verify the printer location and select secure print mode.
- If a breach of PII occurs, notify your supervisor and contact your privacy office immediately.
- Report the PII breach within 24 hours to the Army Privacy Office using the Privacy Act Tracking System (PATS): https://www.privacy.army.mil/PATS/login.aspx.
- When teleworking in an area of your home, ensure it is free from individuals who do not have a "need to know."
- Secure and protect Army mobile electronic devices, such as government laptops and government cellphones.
- Ensure laptops and mobile electronic devices have Data at Rest (DAR) encryption and are Common Access Card/Public Key Infrastructure (CAC/PKI) enabled. See your information technology (IT) support team for assistance.
- Complete annual PII training.

What are common causes of PII breaches?

Most PII breaches are due to human error. Army personnel who mishandle PII are required to take remedial training. It is your responsibility to prevent human errors:

- Do not send unencrypted emails containing PII or send unencrypted or encrypted emails containing PII to recipients who DO NOT have a "need to know."
- Do not post PII on shared network drives, Microsoft Teams or SharePoint sites without restricted access for only those with a need to know. See your IT support team for assistance.
- Do not post personal documents on a network shared drive.
- Do not discuss PII/PHI with others that do not have a need to know.
- Do not leave PII unsecured, such as on a desk or at a network printer.
- Do not post or discuss work-/health-related information on any social media platforms.
- Do not leave your government-issued devices unattended in an unlocked vehicle or trunk.
- Do not Report IT-related PII breaches to the U.S. Computer Emergency Readiness Team (US-CERT).