The most commonly reported Personally Identifiable Information breach in the Department of the Air Force is also one of the easiest breaches to prevent: failure to encrypt an email message containing PII. As a result of the rising reported amount of PII breaches, The under secretary of the Air Force has mandated the immediate blocking of all unencrypted messages with PII or PII-like information from transiting Air Force networks via email.

Frequently Asked Questions

WHAT IS PII?

The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

WHAT IS A BREACH?

A breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

AM I REQUIRED TO ENCRYPT EMAILS THAT CONTAIN PII?

Yes. Air Force policy requires that all email containing sensitive information, including PII, must be digitally signed and encrypted.

Email containing PII and email subject to the Privacy Act should be digitally signed and encrypted using Department of Defense approved certificates.

Double check that you have the correct email addresses and all recipients have a “need to know” before sending.

Double check your attachment to make sure you have selected the right document.

WHY WAS MY EMAIL BLOCKED?

Chances are your email was tagged as having PII or PII-like material and was sent unencrypted. The Air Force has deployed multiple technologies to block all unencrypted emails containing PII or PII-like information.

WHAT DO I DO IF MY EMAIL WAS TAGGED BUT DOES NOT CONTAIN PII?

Best business practice is to ensure you encrypt the message. This is easiest and simplest method. Encrypted traffic will not be blocked.

If you believe your e-mail was inaccurately tagged for PII, please contact your local Communications Focal Point to submit a Remedy Ticket (https://eitsm2.us.af.mil/). These tickets will be used to improve the accuracy of the PII filter to avoid future identification of non-PII

data. However, if the non-PII material is time sensitive please use either email encryption or AMRDEC SAFE (https://safe.amrdec.army.mil/safe/Welcome.aspx) to transmit your data.

WHAT IF I CANNOT ENCRYPT THE EMAIL?

Either refer the recipient to the authoritative database for the information they require or use AMRDEC SAFE (https://safe.amrdec.army.mil/safe/Welcome.aspx) to send.

CAN I BYPASS THE BLOCKS AND SEND MY EMAIL UNENCRYPTED BECAUSE IT'S EITHER NON-PII OR OPERATIONALLY IMPORTANT AND IT HAS TO GO NOW?

No, that is a breach and you have put your fellow Airmen at risk! Either encrypt the email, refer the recipient to the authoritative database for the information they require or use AMRDEC SAFE (https://safe.amrdec.army.mil/safe/Welcome.aspx) to send.

CAN I TRANSMIT PII OUTSIDE OF THE AIR FORCE NETWORKS?

Via email, no! Via AMRDEC SAFE, yes. AMRDEC SAFE provides a secure transmittal capability to send PII to authorized users with a need to know inside and outside the Air Force networks. However, it is on you to ensure the recipient is an authorized user!