

PLEASE READ THIS EMAIL IN ITS ENTIRETY!

Dear NAVMED Accessions Program Participants,

As you know, AMRDEC Safe has been down and will continue to be down for an indefinite period of time. Until AMRDEC is back up and running OR until we develop an alternative way to send documents containing Personally Identifiable Information, we wanted to provide alternative options to send documents to our office. These will hopefully provide some convenient and safe options to continue receiving your documents.

Following are some points to consider:

If you are sending a document that DOES NOT contain PII, you DO NOT have to send it encrypted or through a secure site. You can directly attach documents without PII to an email and send it to the OH inbox.

***Please do not include the last 4 of your SSN on ANY documents even if there is a field requesting it. We can obtain your SSN from the data base if we need it.

***You can STILL use FEDEX to send any documents, if you prefer.

ATTN: ***insert appropriate department here***
NAVMED Accessions
8955 Wood Road, Building 1/13th floor (Room 13130)
Bethesda, MD 20889-5628

Specific NAVMED Accession Document Submissions:

- Academic Year Statements (AYS) and Reimbursement Claims can be sent as direct attachments unencrypted. Please leave the last 4 of SSN and home address fields BLANK (eliminates PII).
- Travel Claims: Encrypt the PDF. Consider scanning your travel claim as ONE PDF. That way there is ONE document to encrypt (versus multiple) and one document to unlock and open on this end.
- Contact Information Sheet (CIS): Encrypt the PDF using the steps and Pass Word (PW) rule described below (last name, 2 digit month, ! example: peterson11!)
- Medical Records: Encrypt PDF or for more secure sending, FEDEX.
- Personal statements, other documents that do not contain PII send directly attached to emails.

*** The default action if you have ANY concerns about the information in your document is to encrypt your PDF:

STEPS TO ENCRYPT ADT PDF (see attached “How to Guide”:

1. Open the pdf and go to “Tool” top of tool bar.
2. Go to “Protect” (Shield symbol), click on it.
3. Right in the center of document you will see “encrypt with lock symbol” pop up.

4. On the encrypt document drop down menu pick “encrypt with password” (option 2).
5. Another box will open. Check “require a password to open the document”.
6. Now enter the password to protect the document.

When you encrypt a PDF, you will need to create a password. To make it easy and efficient, please use the following rule when creating the PW for your documents. The password rule is: Your last name, 2 digit month, ONE exclamation point (!). So your password should ALWAYS look like the examples below (except with YOUR last name):

1. peterson11! (if I am sending/encrypting a document in November)
2. peterson12! (if I am sending/encrypting a document in December)
3. peterson01! (if I am sending/encrypting a document in January)

By constructing your PW via this rule, we eliminate the need for a second email to “share” the PWs on the encrypted documents. Utilizing this PDF encryption process allows us to continue to send documents via email versus FEDEX.