

# 10 Tips

## To Protect Personally Identifiable Information (PII)

**A. Be cautious of companies claiming to contact you** - Whether on behalf of Department of Veterans Affairs (VA) or presenting themselves as having special affiliation with VA.



**B. Never give out PII via text** - VA will never text to confirm or request PII for benefits or federal payments.



**C. Do not provide a copy of a driver's license, passport, VA ID, or any other type of picture identification card** - Whether via text, fax, or email correspondence.



**F. Maintain healthy cyber habits** - Utilize multi-factor authentication, strong passwords, change passwords frequently, set security software to update automatically and encrypt devices.



**E. Be cautious of suspicious or unfamiliar hyperlinks** - Do not open emails, attachments or click on links from unknown sources.



**D. Do not share PII such as date of birth, military entrance/ discharge information, branch of service, banking or credit card information etc.** - Whether contacted via text or by someone claiming affiliation with VA.



**H. Do not share your VA National Call Center personal pin with anyone** - That includes family, friends, or any entity who makes contact via mobile communication.



**G. Verify your identity** - Obtain a VA Security Personal Identification Number (PIN). A PIN is an additional way to secure direct deposit accounts from theft and protect PII.



**I. Back up important files** - Files include military/medical records, discharge papers and copies of VA claims to ensure proof of identity.



**J. Report suspicious activity** - If you miss a VA benefits payment, identify a discrepancy in payments, or find suspicious activity with your direct deposit account, contact the VA immediately at 1-800-827-1000.

