

United States Senate

WASHINGTON, DC 20510

October 26, 2015

The Honorable Robert McDonald
Secretary of Veterans Affairs
810 Vermont Avenue
Washington, DC 20420

Dear Secretary McDonald:

We are writing to request information on the process by which the Department of Veterans Affairs (VA) shares information with non-VA personnel for purposes of assisting veterans with their claims for service-connection of disabilities. It has come to our attention that gaps in VA's current process resulted in veterans' personally identifiable information (PII) being disclosed to an unintended recipient in Wisconsin. As such, we would appreciate information on how veterans' PII is safeguarded from inappropriate or accidental disclosure from the Department to a third-party, such as a state department of veterans affairs, or from the third-party to another individual. Unintended disclosure of PII puts veterans at risk for fraud and identity theft, regardless of whether credit monitoring is offered to mitigate the effects of the disclosure. We must assure veterans that the Department is doing everything possible to protect their PII.

We understand that VA utilizes several tools to protect veterans' PII from unintended disclosure. In detail, please describe these tools and how they work to safeguard veterans' information. In particular, do these tools: flag for the sender (VA employee) that PII is contained in the communication being sent, require a sender to encrypt such information before it is sent, and oblige the recipient (non-VA employee such as a state employee who is the intended recipient) to enter a password before opening a message with such information? Do any Department partners use these VA tools? What are the Department's instructions to its partners who are intended recipients of veterans' PII on how to prevent unintended disclosure? Does the Department require—as a condition of the information sharing partnership—its non-VA partners to have certain information security standards specific to the protection of PII, including, but not limited to: software, network systems, and employee protocols and training? Who is liable when a third-party inappropriately or accidentally discloses a veteran's PII that was provided to the third-party by VA?

Further, how are VA personnel trained on the importance of safeguarding PII when transmitting information via email or other means? How often does the Department offer this training and with what frequency are employees provided "refresher" training? Does the Department monitor whether tools meant to safeguard a veteran's PII are being utilized by employees – if yes, by what means?


The Honorable Robert McDonald

October 26, 2015

Page 2

We look forward to your response and thank you for all you continue to do on behalf of our Nation's veterans.

Sincerely,


Tammy Baldwin
U.S. Senator


Richard Blumenthal
U.S. Senator