VCU Work Incentives Planning and Assistance
National Training and Data Center
VIRGINIA COMMONWEALTH UNIVERSITY

Email, PII, and Encryption Guidance

July 2016

WIPA projects must collect and report beneficiary data as required by Social Security. This includes, but isn't limited to, Social Security Number (SSN), the name, address, and work activity for the beneficiary, as well as other highly sensitive information. All beneficiary information provided to a CWIC must be kept strictly confidential at all times. Maintaining the confidentiality and privacy of the beneficiary is of utmost importance. CWICs are required to follow Social Security's Privacy and Confidentiality policies for maintaining records of individuals, as well as provide specific safeguards surrounding beneficiary information sharing, paper, computer records, data, and other issues potentially arising from providing work incentives planning and assistance services to Social Security disability beneficiaries.

This document will specifically address guidance related to personally identifiable information (PII), email, and encryption. For more information on Social Security's Privacy and Confidentiality policies, refer to Attachment B in your WIPA Terms & Conditions, and to Unit 1, Module 7 in the CWIC Initial Training manual.

What is Personally Identifiable Information (PII)?

"Personally Identifiable Information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth,mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." *(Excerpted from Attachment B – WIPA Terms and Conditions)*

PII, Email, and Encryption

WIPA projects have been encouraged to utilize more distance service methods and rely less on face-to-face services. In this technological age, email, social media, and text messaging are becoming the primary modes of communication. Using such methods of communication with beneficiaries is acceptable, as long as precautions are taken to protect PII.

Frequently Asked Questions:

- Are we permitted to use our agency's web-based email system on the secure laptop to send emails that include personal identifying information, or emails that include attachments with PII?

  Answer: **Email should NEVER contain any PII in the subject line or body of the email; even if it is being accessed on the secure WIPA laptop. If there is a need to send PII, it MUST be in an encrypted attachment. Passwords for encrypted attachments must be sent in a separate email, they may not be sent in the email containing the secure attachment.**

- If an email exchange with a beneficiary occurs, as long as any PII is removed (such as the beneficiary noting their name at the bottom of their message) and the CWIC doesn't add any PII, then is there still a need to encrypt?

  Answer: **It is best practice to encrypt all emails between you and a beneficiary.**

- If the beneficiary's email address includes their first and last name, would the email need to be encrypted (since that PII can't be removed)?

  Answer: **Absolutely.**

- What about the auto-emails that we get via ETO notifying us of a new referral? They contain a beneficiary's full name, and sometimes I need to reply or forward that email, is that okay since they came securely through ETO?

  Answer: **If you need to respond to, or forward, an automatic email generated by ETO, you must delete all but the first initial of the beneficiary's last name before you reply or forward the email. For example, the auto-email will contain the full name of the referred beneficiary – Joe Participant. When you hit 'reply', or 'forward', you must scroll down to the original email and delete the last name so that it would now show only as – Joe P.**

Please remember that you must always protect beneficiary information. That means encrypting any email containing a beneficiary name, address, telephone number, or other information that would or could identify the individual. For best practice, you should encrypt any email to and from a beneficiary that might contain beneficiary information. Be sure to tell the beneficiary in advance how to open the email and access what you are sending.