West Virginia Executive Branch
Privacy Tip

Emailing Personally Identifiable Information (PII)



Using email is the norm for most members of the workforce when communicating with business partners and co-workers. However, from a security standpoint, email communications may not be fully secured. Especially if you are using an unencrypted network. The potential for messages to be intercepted "in transit" is a very real and potential danger. Email is also prone to human error…you didn't really mean to put your client's social security number in the subject line of your email and unintentionally send it to the wrong email address did you?

When using email, think privacy to ensure any personally identifiable information (PII) is not compromised. PII is defined as information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes protected health information (PHI). Examples of PII include social security numbers, driver's license numbers or financial account numbers (credit/debit).

There are several steps to consider when using email to minimize the risk of unintentional breaches of PII:

- ✓ Do not put PII in the subject line of an email. Your internal email network may be encrypted; however, the subject line is not protected. Hackers have been known to scan the subject lines of email communications looking for user names, passwords, and other PII.
- ✓ Be aware of your Department's privacy and security protocols for using email.
- ✓ Follow established encryption procedures.
- ✓ Is disclosing PII in an email necessary?

Before you hit "send", check and re-check the email address! Many problems can be avoided if you're sure your sending an email to Michael E. Smith, not Michael S. Smith. Your Outlook address book is handy, but make absolutely sure you're sending to the correct person in the correct department.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.