Securing the University’s digital information, including information communicated through email, is a priority for the Division of Information Technology. This document is intended to help you understand the importance of encryption and how to encrypt your emails that contain sensitive and personally identifiable information (PII).

Learn to Encrypt your Email Messages:

1.

Why do you need to encrypt email

With very little information, an attacker can create false accounts, steal identities, and perform other malicious acts using personally identifiable information (PII). Personally Identifiable Information is data that could be used to identify a specific individual. Any two or more pieces of identifying data communicated together are also considered PII. Examples of PII that incorporate sensitive data include but are not limited to the following:

- Full name
- Birthdate
- Birthplace
- Social Security Number or Driver's license
- Student/employee identification number, or any other personal ID number
- Financial account number or credit card number
- Regulated Information: Medical Information (HIPAA dataWtf-1.71(,)1.1 ( )E (I)-1.5 a (c)3.7

How to encrypt email

Encrypted emails must be sent and received through YSU Office 365 Web Client.

To enable the Do Not Forward function only without encryption:

1. Within the encryption banner, click the Change Permissions link > Select Do Not Forward from the dropdown menu > Click OK.

A banner will appear that reads *Do Not Forward:*