

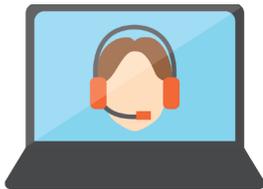
GUIDELINES FOR SECURELY SENDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

EVALUATE RISKS



How sensitive is the information?

- More sensitive information requires more security.
- Some information is **always** sensitive, e.g., SSNs, disability status.
- Some information is sensitive if **combined** with other information.
- Some seemingly harmless information may become sensitive depending on **circumstances**, e.g., custody or foster care issues.



Does it have to be Emailed?

- Would it be safer to deliver **in person**, over the **phone**, or by **postal mail**?



Does it all have to be sent?

- Avoid sending more information than the receiver legitimately needs.



Have you checked local policies/technology?

- Is there a local policy regarding what PII can be sent by Email?
- If sending directory information, have any of the students been opted out?



Can I use a shared drive?

- For internal communication, your organization may have a secured shared drive. There may even be a way to ensure that only specific users in the organization can access the document/information.

CAN I ENCRYPT?*

Can I use my regular work Email?

- Depending on the security certificates, your current work Email may already be end-to-end encrypted.

**Consult your IT security or local policies regarding what types of encryption are available and when to use them.*

Is there a separate, free, encrypted Email service I can use?

- There are several services such as ProtonMail, CounterMail, or Hushmail.
- They each have their own pros and cons.



Is there a paid encryption service I can use?

- You may already have access to paid services which can be separate from your Email (such as MOVEit) or integrated (Zix, Virtru).

Does the recipient have encryption?

- Vendors may already have their own SFTP or other encryption. You can always ask to send them data using their service.

Can I use a password-protected attachment?

- Microsoft Office products, Adobe PDFs, Google docs, Apple Pages, and many other files can be password protected.
- The recipient would get the password to unlock it outside of the Email (in person, over the phone, or even in a separate Email).