North Carolina Infant-Toddler Program

Procedural Guidance

Reference: Confidentiality

Emails That Contain Protected Health Information and Personally Identifying Information

Introduction

1. Do not include Personally Identifiable Information (PII) or Protected Health Information (PHI) in the subject-line or in the body of an email. This includes any combination of: name, initials, date of birth, ID number, SSN number, or any other information that could be combined to identify the child.

2. All emails containing PII/PHI must be encrypted using ZixMail for State CDSA staff. Staff at Contract CDSAs should use the encryption software approved for their use by their local management.

   Instructions for State CDSA employees to ensure ZixMail appears as an option for their emails can be found at the end of this document. State CDSA employees may also ensure their emails are encrypted with ZixMail by including dhhsencrypt in the subject line of the email.

3. All email containing PII/PHI must include "Confidential Information" in the subject line of the email to protect against any accidental disclosure from a Freedom of Information Act (FOIA) request of staff emails.

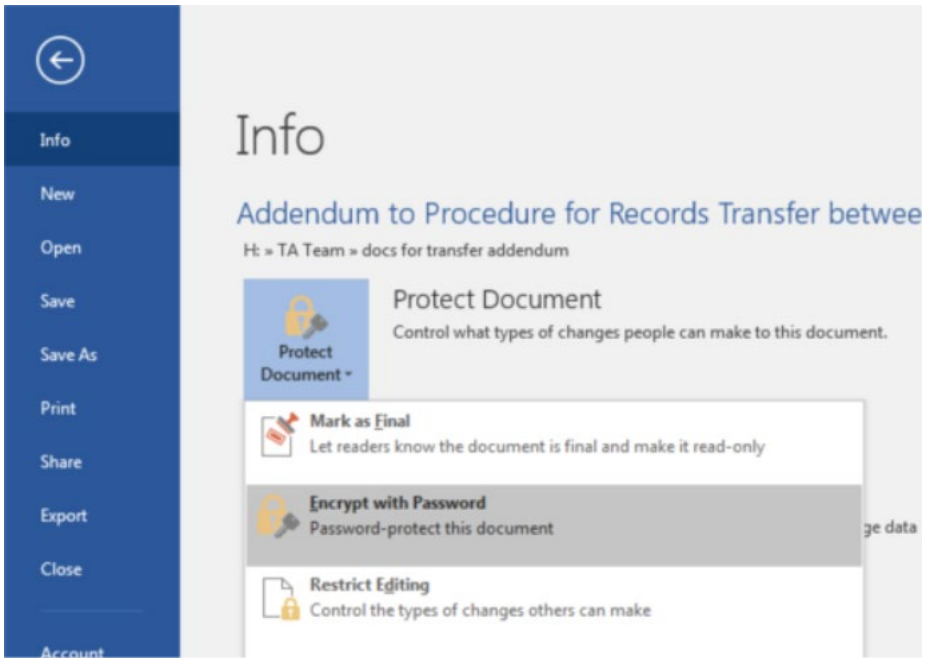
4. Transmit PII/PHI only in a password-protected attachment.

   - For emails between CDSAs and between CDSA staff and EI Branch Office staff, ITP-wide passwords and timeframes in which they should be used have been established and made available to the CDSAs. (This includes both State and Contract CDSAs.)
   - For emails going outside of the Infant-Toddler Program (i.e. to families, other State agencies), staff should generate a new password for the document. The password must conform to DHHS' password requirements:
     - must be at least 8 characters long
     - must contain a capital letter
     - must contain a lower-case letter
     - must contain a number
     - must contain a special character

     a. Staff should use an online password generator to generate passwords that comply with the requirements above. Examples of password generators include:
        - https://1password.com/
        - https://www.lastpass.com/features/password-generator
        - https://us.norton.com/feature/password-generator

b. **Do not** send attachment passwords via email. Call the recipient to provide the password.

c. To apply password protection in Microsoft Office applications such as Word or Excel, select *File*, *Info, Protect Document, Encrypt With Password*.



Enter the password when prompted and click on Save so that the password is applied.

d. For documents of other file types (such as .pdf or .jpg files), these documents must be encrypted using an encryption program such as AxCrypt or WinZip. If you are unsure whether a file needs to be encrypted in this way or if the program you are using for encryption is acceptable, please contact the EI Branch Central Office at 919-707-5520 and a member of the data team will assist you.

Instructions for Adding ZixMail to Emails in Microsoft Outlook

1. In Outlook, click on File in the toolbar.
2. Scroll down to Slow and Disabled COM Add-ins and click on Manage COM Add-ins.
3. ZixSelect for Outlook should appear in the pop-up.
4. Click on Options and Select “Do not monitor this add-in for the next 30 days”.
5. Click Apply then Close.
6. The ZixMail “Encrypt and Send” button should now appear in the toolbar for any new emails you create.