Subject: E-mail Data Security Requirements for Child Care Information Services (CCIS)

Date: 05/07/2013
Category: Informational
Priority: Medium
Action Required: No
Response Required: No

Purpose:
To share information with the CCISs regarding email encryption, why email encryption is important, and when encryption must be used for sending email.

Discussion:
Secure e-mail provides a number of key benefits, including protecting and encrypting all outbound e-mails where the e-mail contents contain sensitive information, enabling agencies to comply with federal mandates requiring secure e-mail transmissions and ensuring that sensitive communications and exchange of information originating from the organization will not be compromised.

Examples of sensitive data where email encryption must be used include any correspondence that contains client personal information (name, address, Social Security numbers, etc.), personal health information (PHI), credit card numbers, financial account numbers, and other information protected by the Health Insurance Portability and Accountability Act (HIPAA) and other laws and regulations.

Electronic PHI data as defined in HIPAA includes individually identifiable information that relates to a person’s health, mental or physical health treatment, or payment for healthcare services. Examples of PHI include any combination of personal identifiers (such as patient name, account number or other identifying information) and healthcare treatment information such as an ICD-9 diagnosis code, an American Medical Association treatment code, or the names of diseases or other health conditions.

Requirements:
- CCIS workers are not permitted to forward encrypted e-mails to personal e-mail accounts.

Next Steps:
1. Share this information with appropriate staff.
2. Direct questions or technical difficulties to RA-oodelwebadmin@pa.gov.
3. Direct any other questions to your Subsidy Coordinator.