SAN BERNARDINO COUNTY | Human Services

HS Privacy and Security

Contractor Encryption Requirements

Encryption Requirements:

Contracted providers must:

- Utilize encryption when transmitting client confidential/Personally Identifiable Information (PII) via email
- Encrypt all workstations and mobile devices (laptops, USB, SD, smart phones, tablets, etc.) and other systems that process and/or store County PII with Federal Information Processing Standards (FIPS) 140-2 Certified Algorithm at 128 bit or higher, whole/full disk

Approval Process:

Prior to providing services, send an encrypted test email to the County's Information Technology & Support Division (ITSD) for review and approval (allow 72 hours for a response):

EncryptionCheck@hss.sbcounty.gov

To access all privacy and security requirements, refer to the HS Privacy and Security contractor's website at: **hss.sbcounty.gov/privacy**

Frequently Asked Questions

When should I submit a test email?	*As soon as you have been notified of a contract award. Only one test email is required per agency if all staff use the same encryption solution.*
My agency has a current contract with the County, do we need to resubmit an encrypted email for approval?	*Yes, a test email is required for all agencies with newly-awarded contracts.*
What type of email encryption should my agency use?	*The County does not endorse any particular product. To meet email encryption requirements, your agency must select a solution that:* • *Stores the email on a secure/encrypted server, and* • *Requires the user to either register by creating a username and password or enter a one-time passcode*
Does a password-protected document meet encryption requirements?	*No, the encryption solution must require the user to enter a username and password in order to access the email.*

FLYER #20-323 (09/20) MP:JR:ap