PRIVACY & SECURITY INFORMATION NOTICE

RAISING AWARENESS ABOUT THE IMPORTANCE OF PROTECTING THE PRIVACY & SECURITY OF SENSITIVE INFORMATION

September 2010

Email Encryption Guidelines

The County now has email encryption available using Iron Port CRES/PXE encryption software. Email encryption ensures the protection and privacy of County email containing confidential or sensitive information to be sent outside our County Network. Encryption ciphers or encodes data so that it cannot be read by anyone who is not the intended recipient to decode it while electronically transmitted. **In order for email encryption to work, an IMAR must be submitted to install it.** Agency staff who do not have email encryption installed must continue to follow the procedures indicated in the Agency Email Policy (see next page for the Policy link). Email sent within the County (i.e. sending email from one County employee to another) will not encrypt.

Email (whether sent or received) is not secure unless it is encrypted. All outgoing (sending or forwarding) email outside the County's Network that contains confidential or sensitive information (e.g. an individual's personal information whether or not it includes Medical/Health information) must be encrypted and delivered to the recipients email address via IronPort CRES/PXE.

Examples of email content that must be encrypted are:

- Person's name (Patient or Client Name)
- Home Address (Patient or Client Address)
- Date of birth
- Social Security Number
- Medical/Health information (treatment, diagnosis, medication, health services)
- Medical record number
- Health plan beneficiary number
- Bank account number
- Email address (Patient or Client email address)
- Certificate/license number
- Any vehicle or device serial number that can locate an individual

An external sender (e.g. patient or client) who sends email to the County cannot be obligated to use encryption. Also, the Agency has no control of what information they include in their email. However, Agency staff can provide the sender with guidance to send any further email containing confidential or sensitive information through secure email. The Agency staff person would then send the first secure email to the sender that includes the Web link to register for an email encryption account to begin communicating securely with the County.

In regards to contractors (or their subcontractors) or other entities doing business with the County, any exchange of confidential or sensitive information transmitted outside the County Network must be encrypted. HHSA ITD is to be contacted for transmitting a higher volume of information in a secure manner with contractors or other entities (e.g. SSLVPN, SSH, SSL, SFTP).

In any circumstance, when sending or forwarding an email message, exercise caution to avoid sending it to the wrong recipient or sending it to an individual who has no business need to receive it. The wrong recipient can still register for an email encryption account and retrieve the email containing the confidential or sensitive information.

Email encryption can be installed on Agency staff email accounts.
It cannot be installed on Agency generic email accounts at this time.

Pilar.Miranda@sdcounty.ca.gov

HHSA Information Technology Division

PRIVACY & SECURITY INFORMATION NOTICE

RAISING AWARENESS ABOUT THE IMPORTANCE OF PROTECTING THE PRIVACY & SECURITY OF SENSITIVE INFORMATION

E-mail Encryption Guidelines

Email Encryption Features: (See 'Email Encryption – End-User Instructions' below)

For Agency staff with email encryption, you can:

- Send encrypted e-mail to external recipients. The recipient will receive an email notice in their inbox informing them that they have been sent an encrypted e-mail from the County and instruct them to click on the Web link provided. There they can register for an account (userID and password) to retrieve and reply securely to encrypted messages through this secure web site. It is free of any cost to external recipients. (Attachments are also encrypted).
- Set up requests for 'Read' and/or 'Delivery' receipts.
- Lock or otherwise prevent a message from being read by a recipient after the message has been sent.
- Set up an expiration date after which encrypted messages you have sent cannot be opened.

Additionally:

- An external recipient with a registered encryption account can reset their own password in case they forget what it is. There is no need to call a Help Desk.
- The IronPort Outlook plug-in software makes an '*Encrypt*' button available to simply 'click it' to encrypt a message.

How to request Email Encryption:

Submit an IMAR (not a CSRF) and provide the following: (includes a monthly charge)

- Employee Name
- Email Address
- Desktop or Laptop Asset #
- Request to install the IronPort Outlook plug-In for the '*Encrypt*' button to be displayed

References: (Click on the title of the reference below to view the document)

1. Privacy and Security Information Notice (Unauthorized disclosure of Identifier Information to be reported)
2. Agency Policy: Security of Client Data and Portable Devices
3. Agency Policy: Acceptable Use of County Email
4. Email Encryption - End-User Instructions

IF YOU HAVE ANY QUESTIONS PLEASE CONTACT:

Pilar Miranda, HHSA Information Security Manager
(619) 338-2806
Pilar.Miranda@sdcounty.ca.gov

HHSA Information Technology Division