INTERIM INSTRUCTION NOTICE #11-002

June 30, 2011

SUBJECT:	**Email Encryption**

DISTRIBUTION:	**All Department of Behavioral Health (DBH) Staff, Contract Providers, and Email Recipients Outside the County Network**	**OBSOLETE:**	**Upon completion of related policy and/or procedure**

Effective Date   **June 30, 2011**

From   Office of Information Technology

Introduction   The Department of Behavioral Health's (DBH) Office of Information Technology (IT), in partnership with the County's Information Services Department (ISD), has implemented email encryption technology for all email messages originating from the County of San Bernardino communications network.

Background   Email encryption is now recognized as a best practice for organizations responsible for protected health information (PHI) privacy and security. The Health Insurance Portability and Accountability Act (HIPAA) requirement that PHI sent via email must be encrypted for the email to be considered secure is the catalyst of this email policy change for DBH.

This Interim Instruction Notice (IIN) outlines changes from previous email services and provides instruction for transition to the Cisco Registered Envelope Service (CRES) to securely send and receive encrypted email.

CRES Overview   CRES helps companies secure email communications that allows businesses to send encrypted messages via registered envelopes. The registered envelope is an encrypted email which may also be password protected. Password protected email can only be opened by authorized recipients who authenticate themselves. First-time recipients receiving a password protected secure envelope are asked to register with CRES to set the password which will be used for authentication.

No changes are required by DBH staff to encrypt emails addressed to recipients outside the County network. Email generated from DBH staff exiting the County communications network is automatically encrypted through CRES, by converting the email message into a secure attachment.


Continued on next page.

CRES Overview
(continued)

DBH staff and anyone outside the County network must register their email addresses with CRES to view encrypted email by completing the New User Registration process. Registration is completed one time only for each email address. The only requirement to read secure email after staff have been registered and verified as the recipient, will be to enter the password assigned to that email address.

Secure Workflow Process
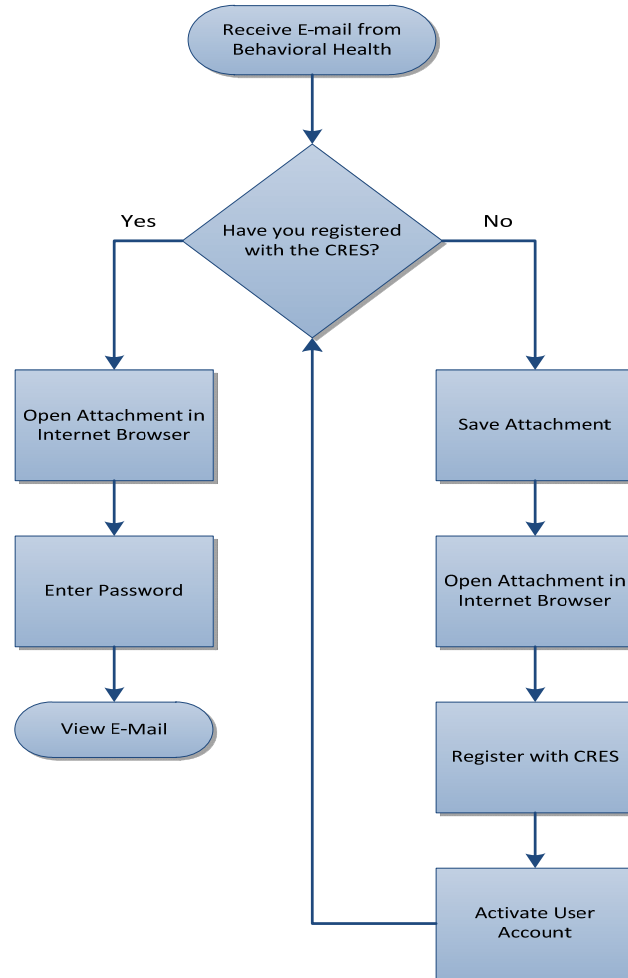
Procedure to Open DBH Generated Email

To open DBH-generated email sent outside the County network:

Step	Action
1	Open the email. **Displayed Response:** A box labeled "You have received a secure message" will be shown in the place where the email message is usually displayed.
2	Open the attachment. **Displayed Response**: A window will be displayed asking if you want to unblock the message.

Continue on next page.

Procedure to Open DBH Generated Email (continued)	Step	Action
	3	Click on "yes."
		Displayed Response: A window will be displayed which offers a choice between opening and saving the document.
	4	Choose to save the document for best results.
		Displayed Response: The "My Documents" window will open.
	5	Select or create an appropriate folder in which to save the attachment in "My Documents" and save it as usually completed.
		Displayed Response: A window will be displayed advising the download is complete. Close that window as directed.
	6	Go to "My Documents" and click on the folder to open the attachment.
		Displayed Response: A window will open which displays a graphic envelope. This is the Registered Envelope.
	7	Either open the document or register for a password as follows:

If the user:	Then:
Previously registered a password for the email address,	The document (attachment/original email) opens.
Is opening a Registered Envelope for the first time,	An electronic form entitled "NEW USER REGISTRATION" will open. **See First Time User Registration** below to create a password.

	Step	Action
	8	Click on the "Reply" button (displayed in the upper and lower right side corners of the message) to send a response.

First Time User Registration

Follow the steps below to register with CRES and establish a password for the email address from which the document has been opened and subsequently open the Registered Envelope.

Step	Action
1	Complete the information in the electronic "NEW USER REGISTRATION" form to establish a password, then click on the "Register" button at the bottom of the form.
	Displayed Response: Displayed on the screen will be "FINAL STEP: ACCOUNT ACTIVATION."
2	Follow the displayed instructions for account activation, which requires returning to the email site to open a CRES-generated registration confirmation email.
3	Open the registration confirmation email and click on the line, "Click here to activate this account."
	Displayed Response: Displayed on the screen will be "EMAIL ADDRESS CONFIRMED."

First Time User	**Step**	**Action**
Registration	4	Close the registration confirmation email.
(continued)	5	Return to the Registered Envelope and: • Enter the newly established password • Click on the "continue" button to open the attachment. **Displayed Response:** The attachment (or original email) will open.

CRES Assistance

Password

Click the "Forgot Password" link on a Registered Envelope to reset a password when a password has been forgotten or it does not seem to work. CRES will send a "New Password" message to the email address associated with your account.

Important Note: DBH, IT and the ISD Helpdesk *do not* have access to reset a CRES user password.

CRES Questions

Click the following link to obtain additional assistance from the Cisco Registered Envelope Service:

Cisco Registered Envelope Service FAQ

Other Questions

Other questions regarding this Interim Instruction Notice should be directed to the DBH Office of Information Technology (IT) by contacting the ISD Helpdesk at (909) 884-4884.

Standard Practice Manual

Upon implementation of this IIN, DBH staff may send PHI via email, as long as it complies in all other respects with current DBH Standard Practice Manual (SPM) policy and procedure language addressing electronic PHI transmission. Appropriate revisions to the SPM are forthcoming.

References

Code of Federal Regulations, 45 CFR, Section 164 et seq.: Health Information Portability and Accountability Act.
County of San Bernardino Policy
• No. 16-02: Protection of Individually Identifiable Health Information
• No. 16-02SP Protection of Individually Identifiable Health Information
DBH Standard Practice Manual
• COM0905: Confidentiality of Protected Health Information (PHI)
• COM0909: Electronic Transfer of Client Protected Health Information-Internet and Intranet Policy
• COM0944: Privacy or Security Breach Policy
• IT5005: Electronic Mail Policy