



SANTA BARBARA COUNTY  
DEPARTMENT OF  
**Behavioral Wellness**  
A System of Care and Recovery

# Departmental Policy and Procedure

**Section** Information Technology (IT)

**Effective:** 12/9/2015

**Sub-section**

**Version:** 1.1

**Policy** Email Encryption

**Last**

**Policy #** 14.004

**Revised:** 9/12/2018

**Director's Approval**

  
\_\_\_\_\_  
Alice Gleghorn, PhD

**Date** 10/1/18

**Division Chief's  
Approval**

  
\_\_\_\_\_  
Marshall Ramsey

**Date** 10/2/18

**Supersedes:** COMP-11.xxx Email Encryption rev. 12/9/2015

**Audit**

**Date:** 9/12/2021

## 1. PURPOSE/SCOPE

- 1.1. To ensure the proper use of the Santa Barbara County Department of Behavioral Wellness (hereafter "the Department") e-mail system and make users aware of what the Department deems as acceptable and unacceptable use of its e-mail system. This policy outlines the minimum requirements when sending sensitive Protected Health Information (PHI), Personal Information (PI), and Personally Identifiable Information (PII) via e-mail in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations.
- 1.2. This policy applies to all employees, contractors on payroll, locum tenens, and other agents operating on behalf of the Department that include any PHI, PI, and/or PII sent via e-mail from a Department computer to any e-mail address or account outside the County's e-mail system. This policy does not apply to contractors using non-Department computers. Contractors are responsible for obtaining and implementing their own email encryption solutions for the purposes of communicating PHI, PI and/PII information electronically with the Department and other relevant agencies.

## 2. DEFINITIONS

The following terms are limited to the purposes of this policy:

- 2.1. **Protected Health Information (PHI)** – refers to any Protected Health Information (PHI) that is covered under the HIPAA Security regulations, including PHI produced, saved, transferred or received in an electronic form. For example, the combination of past, current or future information related to health, provision of care or payment, **together with** any identifying information that is reasonably likely to identify the client constitutes PHI as defined by the [HIPAA Privacy Rule's 18 Identifiers](#) related to the PHI definition ([see Attachment A](#)).

- 2.2. **Personal Information (PI)** – any information that is maintained by an agency, including Personal Information (PI) produced, saved, transferred or received in an electronic format, that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. [California Civil Code §1798.3(a)]
- 2.3. **Personally Identifiable Information (PII)** – any information, including Personally Identifiable Information (PII) produced, saved, transferred or received in an electronic format, which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- 2.4. **Secure E-mail Message** – an e-mail whose content has been encrypted.
- 2.5. **Encryption** – the process of encoding the message so that it is unreadable to all but the intended recipient. Please refer to Attachment B for a step-by-step instruction on how the secure email process works.
- 2.6. **Proofpoint Encryption Plug-in (hereafter “Proofpoint”)** – the network service that allows the Department to send encrypted messages to any e-mail address or account outside the County’s e-mail system.
- 2.7. **Outside E-mail Address or Account** – any e-mail address or account outside of the Department.
- 2.8. **County of Santa Barbara Outlook Web Access (OWA)** – a web-based version of the County of Santa Barbara’s E-mail System available from any outside electronic device.

### 3. **POLICY**

- 3.1. All use of e-mail must be consistent with the Department’s policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- 3.2. All emails containing PHI, PI, and/or PII, either within the body of the e-mail message or as an attachment, that are sent to an outside e-mail address or account must be encrypted in accordance with this policy.
- 3.3. The e-mail encryption process is not intended to circumvent the Request for Information (ROI) process.

#### **4. PROCEDURE**

- 4.1. Any email sent to an outside email address or account containing PHI, PII and/or PI must be encrypted by including brackets and the word “[secure]” in the Outlook subject line ([see Attachment B](#)).
  1. The subject line is not encrypted. No PHI, PII and/or PI may be written in the subject line of the email.
  2. Omission of the brackets or substituting the brackets will render the email unencrypted.
  3. Alternatively, users with access to the Proofpoint plug-in within Microsoft Outlook can automatically send encrypted e-mails to outside e-mail addresses or accounts.
- 4.2. First-time recipients need to register and create a user account with Proofpoint ([see Attachment B](#)).
- 4.3. Senders must notify a first-time recipient about the e-mail encryption process prior to sending an encrypted e-mail, therefore ensuring that the encrypted e-mail can be deciphered.
- 4.4. After the e-mail recipient successfully creates, logs in, and authenticates an account, the e-mail message will appear in a browser window.

#### **ASSISTANCE**

HIPAA Sub-committee

#### **ATTACHMENTS**

[Attachment A – Individual Identifiers of PHI \(18\)](#)

[Attachment B – How The Secure E-mail Process Works](#)

#### **REFERENCE**

Code of Federal Regulations – Public Welfare  
*Title 45, Section 164.514 – De-identified Information*  
*Title 45, Section 164.312(e)(1) – Transmission Security*

California Civil Code  
*Section §1798.3(a)*

**RELATED POLICIES**[Release and Access: Outpatient Medical Records](#)[County of Santa Barbara – Acceptable Use Policy](#)[County of Santa Barbara/ICT Adopted Policies – E-mail Policy](#)**REVISION RECORD**

DATE	VERSION	REVISION DESCRIPTION

***Culturally and Linguistically Competent Policies***

*The Department of Behavioral Wellness is committed to the tenets of cultural competency and understands that culturally and linguistically appropriate services are respectful of and responsive to the health beliefs, practices and needs of diverse individuals. All policies and procedures are intended to reflect the integration of diversity and cultural literacy throughout the Department. To the fullest extent possible, information, services and treatments will be provided (in verbal and/or written form) in the individual's preferred language or mode of communication (i.e. assistive devices for blind/deaf).*