

## **VENDOR GUIDELINES FOR EMAIL SECURITY AND INTEGRITY**

It is the responsibility of each regional center to protect the right of privacy for people with developmental disabilities. This can be accomplished by adopting practices consistent with the recommended Best Practices Guidelines included in the Department of Developmental Services (DDS), Community Operations Division (COD) Program Advisory COD 08-01, issued August 2008. That Advisory reminds regional centers that vendors/business partners of the regional center also need to be aware of the requirement to safeguard confidential information.

Every employee of each organization – regional centers and vendors – plays a role in the protection of personal and confidential information. Information is a valuable asset and needs to be protected from loss and unauthorized disclosure.

Failure to take the steps to protect confidential information can place people in jeopardy in a variety of ways, including identity theft, damage to reputation, breach of privacy, and possible physical injury.

### **AWARENESS -- THE FIRST STEP**

First of all, regional center and vendor email users need to be aware of what constitutes confidential, sensitive, and/or personal information. For the purposes of this guideline, the term “confidential” information will be used to include sensitive and personal information, as defined in various codes, such as Civil Code section 1798.3.

**Any communication** that includes individual identifiers or personal information, such as the person’s name, home address, home phone number, birth date, social security number, Medi-Cal number, physical description, education, financial matters, and employment history, and personal health information, such as medical and psychiatric diagnoses or medical history, is considered confidential, sensitive and personal information.

Welfare and Institutions Code 4514 states that “all information and records obtained in the course of providing intake, assessment, and services ... to persons with developmental disabilities shall be confidential.”

That means that emails with the regional center containing assessments, progress reports and other routine communications must comply with the steps to safeguarding the exchange of confidential information, as noted below.

## **STEPS TO SAFEGUARD EXCHANGE OF CONFIDENTIAL INFORMATION**

First of all, be sure that you are authorized to send out confidential information and the intended recipient is authorized to receive that confidential information before you send it.

Send a person's information to others only when it is necessary for them to know that information to do their jobs and only to the extent necessary to do that job. In other words, do not include any more information than necessary, regardless of the form of communication. There needs to be a legitimate business "need to know" before releasing any confidential information.

**Never send confidential information in the body of an email message, without taking the steps indicated below to protect that information.**

**Never include confidential information in the subject line of an email message.**

As a first choice, confidential information may be sent in the body of the email message **if the information is encrypted.**

If encryption is not available, the email user may communicate confidential information **only** if that information is contained within a **password protected attachment**, and if the **password is sent in a separate communication**, such as a phone call, fax or email. (See Attachment A below.)

For password protected documents, use "hard-to-crack" passwords, which are more like "vanity plates" (like If33lgr8! for I feel great!) than regular words found in the dictionary.

These passwords are a minimum of eight (8) characters and include at least one of each of the following:

Uppercase letters (A-Z)

Lowercase letters (a-z)

Numbers (0-9)

Punctuation marks (!@#\$\$%^&\* ( ) \_ - + =)

Store all passwords separately and in a secure place.

761 Corporate Center Drive, Pomona, California 91768  
(909) 620-7722

Program of San Gabriel/Pomona Valleys Developmental Services, Inc.

As an alternative, communication of confidential information shall be sent via fax, after double checking the fax number prior to sending information out and confirming that the intended recipient received the fax.

If secure email and fax options are not available, confidential information should be sent by mail. Of course, confidential documents can be hand-delivered to the SG/PRC reception area, if the envelope is sealed and the intended recipient is clearly identified.

It is considered acceptable to use a client's initials (initials **only** for both the first and last names) along with the Unique Client Identification Number (UCI#), as that information is considered secure within the body of the email message. However, it is still preferable that this sort of information not be included in the subject line of the email.

If you have questions regarding these guidelines, which are supplemental to the HIPPA agreements that you have already reviewed and submitted to the regional center, please feel free to contact Carol L. Tomblin, Director of Community Services, San Gabriel/Pomona Regional Center. The email address is [ctomblin@sgprc.org](mailto:ctomblin@sgprc.org) and the phone number is (909) 868-7521 (where you can always leave a message at any time).

---

## **Attachment A**

### **Password Protecting a Document**

**(taken directly from the "HELP" menu on the Microsoft Word software)**

1. Open the file.
2. On the **Tools** menu, click **Options**, and then click **Security**.
3. Do one of the following – (a) create a password to open,  
or (b) create a password to modify.
  - (a) 1 – In the **Password to open** box, type a password, and then click **OK**.
  - 2 – In the **Reenter password to open** box, type the password again and then click **OK**.

**Or you may create password to modify.**

- (b) 1 – In the **Password to modify** box, type a password, and then click **OK**.
- 2 – In the **Reenter password to modify** box, type the password again, and then click **OK**.