CALSTRS
HOW WILL YOU SPEND YOUR FUTURE?

Employer Information Circular

Volume 21; Issue 1 **January 7, 2005**

Information Security Tips for Transmitting Confidential Information

The California State Teachers' Retirement System (CalSTRS) appreciates your continued assistance regarding information security by providing the essential protections necessary to properly care for member information. This is critical to CalSTRS' on-going efforts to decrease risks to confidential information.

Due to the growing number of identity theft cases, now is a good time to review and be prudent with your methods for sharing and transmitting confidential CalSTRS member information. This information circular contains some ***Information Security Tips*** to assist you in this regard and may help you ensure information is used for its intended business purpose. Confidential information includes, but is not limited to, Social Security numbers, birth dates, and beneficiary information. Below are tips to follow for the most common transmission methods used.

United States Postal Service

The United States Postal Service (USPS) provides federally-recognized protection for confidential data. However, the USPS is also concerned with the rise of mail theft and identity fraud. Precautions include ensuring the area where you place items for mail pick up and drop off is restricted to authorized personnel. When sending items

- clearly identify the name and address of the intended recipient;
- include the name and return address of the sender;
- add a confidentiality statement to documents containing confidential data.
  Example: *"CONFIDENTIAL - UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED";*
- ensure that confidential data cannot be read through the envelope or envelope window;
- use a secure mail depository; and
- do not include complete Social Security numbers on correspondence.

(Continued . . .)

Facsimile (faxes)

With precautions, sending confidential information via fax provides a reasonable level of protection. Precautions include checking your fax machine "receipts" to ensure the transmission was successfully sent to the number for which it was intended.

Fax cover sheets should clearly identify:

- Name of intended recipient;
- Total number of pages;
- Name of sender;
- Telephone number of sender; and
- Confidentiality statement (see example below).

> "This facsimile is intended only for the addressee shown above. It may contain information that is privileged, confidential, or otherwise protected from disclosure. Any review, dissemination, or use of this transmission or its contents by persons other then the addressee is strictly prohibited. If you have received this transmission in error, please notify the sender immediately and follow their instructions regarding the disposition of this facsimile."

Telephone

With precautions, sharing confidential information on the telephone can provide a very good level of security. There are some precautions to take when using the phone, including discussing confidential information where and when only authorized persons can hear it, and using speaker phone capability with caution to avoid disclosure of sensitive information. Also, it is important you verify you are speaking to a person authorized to discuss the information. You may be able to achieve this by having the person identify a combination of unique identifiers like an employee identification number, Social Security number and date of birth.

E-mail

Typically, e-mail does not provide appropriate security protection and is not recommended for sending confidential data. There are special scrambling options, called encryption, that help secure sending confidential information however this feature is normally not 'built in' as a standard to most e-mail programs.

We hope these ***Information Security Tips*** are useful, and thank you for taking the time to ensure confidential information is acquired, used, maintained and shared in a secure manner. We value your assistance in ensuring CalSTRS' continuing efforts to provide quality service to our members, business partners and stakeholders.

Please share this information with appropriate parties at your place of business.