

Date: September 9, 2010

Code: TECHNICAL LETTER  
HR/Benefits 2010-05  
Supplement #1

To: Human Resources Directors  
Benefits Officers

Reference: HR/Benefits 2008-10

From: Evelyn Nazario   
Assistant Vice Chancellor  
Human Resources Management

Subject: Implementation Update: Delta Dental Benefits Interface

Overview

**Audience:** Human Resources Directors, Benefits Officers, and/or campus designee(s) responsible for benefits and leave of absence administration

**Action Item:** Submit the Delta Dental Benefits Interface file on a monthly basis to Delta Dental beginning in September, 2010

**Affected Employees:** N/A

Summary

This Technical Letter provides additional information regarding the Delta Dental Benefits Interface and its pending implementation. This interface enables campuses to electronically submit benefits enrollment data of active employees and their eligible dependents to the dental carrier on a monthly basis. The implementation in each campus' production environment is scheduled for September 2010, using August 2010 (pay period) data.

Campus designees responsible for benefits administration should read this Technical Letter in its entirety.

As previously announced in HR/Benefits 2010-05, Systemwide Human Resources Management (HRM) partnered with Common Management Systems (CMS) and the dental carrier, Delta Dental Plan of California (comprised of Delta Dental and DeltaCare USA), to provide the ability for campuses to electronically transmit benefits enrollment data of active employees and their dependents via the Delta Dental Benefits Interface (Oracle/PeopleSoft HIPAA EDI 834<sup>1</sup>).

As a result of successful testing activities please note the following "go-live" information in preparation for campuses to send the first Delta Dental Benefits Interface file from production databases. The file must be sent no later than September 15, 2010.

<sup>1</sup> Oracle/PeopleSoft delivered industry benefits enrollment and maintenance standard file HIPAA (Health Insurance Portability & Accountability Act) 834 EDI (Electronic Data Interchange).

**Distribution:**

CSU Presidents  
Vice Chancellor, Human Resources  
Vice President, Administration

Payroll Managers  
Delta Dental Plan of California  
State Controller's Office

### The Process

Beginning in September, each campus must upload a valid encrypted Delta Dental Benefits Interface file on Delta Dental's secure FTP server no later than the 15<sup>th</sup> of each month by 3:00 pm. In the ongoing months, campuses are encouraged to submit files earlier. The file, which is generated from Oracle/PeopleSoft's HIPAA EDI 834 process, will capture employee and dependent data from the previous business month. For example, the file sent to Delta Dental in September will contain August data.

Delta Dental's system is configured to automatically validate the file fields of each campus' file and send an e-mail to campus-identified contacts (designated in a Human Resources Management (HRM) Benefits Survey) with confirmation that a valid file was received. If errors are found, the designated contacts will receive a secure e-mail from Delta Dental that contains file validation errors. These errors must be corrected in Oracle/PeopleSoft and a newly generated file must be resent to Delta Dental no later than 3:00 pm prior to the 20<sup>th</sup> of the month in which the errors were reported. To assist campuses with file validation errors, a Delta Dental Enrollment Analyst will be assigned to the CSU. Contact information for the Enrollment Analyst will be sent to the campuses in a separate communication.

Once all 23 campuses, including the Chancellor's Office has completed the upload process and passed the initial file validation process, the files will be merged on the 20<sup>th</sup> of each month and discrepancies will be forwarded to HRM. **It is critical that each campus ensure a valid file is submitted with no errors as the entire CSU will be impacted if there are delays in campus file transmittals. The system will process the merged CSU file and any missed campus records will result in a termination of benefits for the employee and their dependents.**

Internally, Delta Dental will audit dependent data against the monthly file of deductions provided by the State Controller's Office (SCO). Please note, however, Delta Dental Benefits Interface does not replace the current process in place at the SCO for dental enrollments. **Campuses must continue to submit the Std. 692 Dental Enrollment form to the SCO in order for dental enrollments and deductions to be processed.**

### Use of Home Address Type in Oracle/PeopleSoft

The information provided to Delta Dental on the Delta Dental Benefits Interface must include a valid home address acceptable to the United States Post Office (USPS), which includes street, city, state and zip code. Therefore, each employee must have a valid home address designated in Oracle/PeopleSoft.

Please note: It is anticipated that a similar process (use of the Oracle/PeopleSoft HIPAA EDI 834 file) will also be used to transmit employee and dependent data to the CSU vision carrier (VSP) by campuses in the future. Therefore, it is important that the fields are properly populated to avoid potential errors.

### CSU Security Protocols

Due to the nature of the sensitive data extracted from Oracle/PeopleSoft to populate the Delta Dental Benefits Interface file, HRM partnered with the Systemwide Information Security Office to develop stringent protocols for securing the data while at rest and in transmission. In addition to the security requirements listed in this section, campuses are expected to follow CSU Systemwide Information Security Policies (<http://calstate.edu/icsuam/sections/8000/>) and comply with applicable regulations regarding the use, access, and management of sensitive data. Campuses can obtain the CSU Data Classification Standard from their campus Information Security Officer (ISO).

- **User ID and Password for Designated Individuals**

During the testing phases, Delta Dental provided each campus with a "testing" User ID and password. However, each campus-identified designated individual will be provided a unique User ID and password in preparation for "go-live." The assigned User ID and password must not be shared under any circumstances. **Campuses must contact HRM in the event of any of the following circumstances:**

- Issuance of new User ID and password;
- Update or a new assignment of designated individual;
- Revoke current access due to employee separation or new designated assignment;
- Lost/forgotten User ID and password; and/or
- Compromised User ID and/or password.

- **Security Incident Response**  
Campuses must contact HRM and their respective campus Information Security Officer if any one of the following events occurs:
  - A User ID and/or password are compromised;
  - An unauthorized access to sensitive data; and/or
  - Any suspicious activity of a breach or disclosure of sensitive data.
  
- **Security Auditing**  
User activities and access to Delta Dental are monitored, logged, and kept for auditing purposes. HRM will perform an annual review of access granted to validate whether continuing access is necessary and appropriate.
  
- **File Encryption Requirements**  
Campuses are required to encrypt the file prior to uploading it onto Delta Dental's secure FTP server. Files that are not encrypted correctly will be rejected.  
  
PGP Desktop Software has been identified as an acceptable solution that meets the CSU security standards to allow campuses to successfully encrypt the file. Please note: a Systemwide encryption software solution is being explored.  
  
A Delta Dental PGP Public Key was provided to each campus-identified contact in a secure e-mail, and must be used when encrypting the file sent to Delta Dental.
  
- **Sensitive Data Storage and Disposition**
  - Users must not store any sensitive data on their workstations, laptops, and/or any portable media devices such as external drives, USB flash drives, portable digital assistants (PDAs), etc. unless there is a business need to store such data.
  - An approved method of file encryption must be used to protect the data.
  - Devices (i.e., workstations, laptops, and/or any portable media devices such as external drives, USB flash drives, portable digital assistants (PDAs)) containing sensitive data must be sanitized prior to disposal to remove information from media such that data recovery is not possible.
  - Non-electronic media must be cross-cut shredded.
  - The encrypted Delta Dental Benefits Interface file must be electronically "shredded" within 60 days of file creation.

### **Business Process Guide**

A new Business Process Guide (BPG) was created that details the set-up, extraction and file generation process of the Delta Dental Benefits Interface file, including how to upload the file to Delta Dental along with encryption instructions. The BPG will be available on the CMS website.

### **Common Management Systems (CMS) Processing Instructions**

A new interface has been developed for the purposes of the Delta Dental Benefits Interface and is included in CMS Baseline along with required updates, e.g. configuration, objects, etc.

Questions regarding this Technical Letter may be directed to Human Resources Management at (562) 951-4411. This document is also available on the Human Resources Management Web site at: <http://www.calstate.edu/HRAdm/memos.shtml>.

EN/mh