



TOBY DOUGLAS
DIRECTOR

State of California—Health and Human Services Agency
Department of Health Care Services
LEA Medi-Cal Billing Option Program
Frequently Asked Questions (FAQs)



EDMUND G. BROWN JR
GOVERNOR

[DHCS PHI Security Requirements](#)

****PLEASE REVIEW THE LEA MEDI-CAL BILLING OPTION PROVIDER MANUAL FOR COMPLETE LEA PROGRAM AND POLICY INFORMATION****

- Q1. On attachment C, the first page says it is security controls. Does this pertain to SELPAs? If so, how can I determine if my SELPA is certified? If not, who does the certification? Should all the districts in our SELPA be certified as well?**
- A. The Security Controls apply to LEA signatories and any employees or agents who will access the eligibility match data. If the SELPAs or their employees will handle the data, the Security Controls apply to them. These employees must sign a certification indicating they received training in privacy and security protocol. Current employee training programs may suffice if they incorporate privacy and security protocol for handling sensitive data. A certificate containing the name of the employee and date of training is sufficient certification.
- Q2. Can the custodian comply with the DUA rules on behalf of the district if that LEA never directly participates in the "creation, receipt, maintenance, transmittal (or) disclosure of data from DHCS containing PHI or PI" (for example, when only the Custodian receives, maintains, etc. this data)?**
- A. Yes. The custodian named in an LEA's DUA should have the power to act on behalf of the LEA in matters regarding the data. These individuals are responsible for implementing the DUA's provisions, including privacy and security controls. The custodian should have a formal written agreement with the LEA.
- Q3. The Data Use Agreement mentions that only Department of Defense acceptable software can be used to destroy electronic files. Could you please identify this software further, or type of software acceptable so that we can determine which one to purchase? Is PGP software adequate for "shredding?"**
- A. The Security Controls specify that electronic files shall be destroyed using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. There are several types of software, which meet these standards, and DHCS does not require that any specific one be used. The [DHCS Information Security Office \(ISO\)](#) will respond to inquiries as to whether a specific software meets these standards. If a method of destruction other than one specified in the Security Controls is to be used, the prior written permission of the DHCS ISO is needed.

Q4. Will DHCS continue to utilize PGP software for transferring confidential student info for Medi-Cal matching purposes? If not, what will be the accepted software in the future?

- A. The PGP software is acceptable as long as it is using the AES256 encryption method. Additional questions on PGP software, and other questions regarding specific software, can be sent to the [DHCS ISO](#) and DHCS will provide direction and feedback.

Q5. On Attachment E, ‘Department of Health Care Services Certificate of Destruction of Confidential Data,’ what if the name of the custodian holding the files is not employed by the name of the user? For instance, if the County Office of Education is holder of the records (copies that districts send to us) but is not employed by the district, we are the vendor to the district. What information would I use on Attachment E?

- A. In Attachment E, the name of the custodian listed in Paragraphs 3 and 21 should be the point person/custodian who will receive the data files and be responsible for their safekeeping, even if that person is employed by a vendor. The listing can include the name of the person, his/her organization’s name and address, and the notation that the organization is the vendor of the LEA. In Paragraph 1, the “Name of User” should be the LEA.

Q6. Page 5 #14 refers to training. I assume that the training is in-house or arranged by the LEA, correct? What is the scope of this training? Are there required components?

- A. The training should cover privacy and security protocol for handling confidential Personal Information (PI) and Protected Health Information (PHI). LEAs responsible for providing training and are given flexibility to use a format and method of training tailored to their own policies and operations. DHCS does not dictate a format or curriculum for the training. It should cover privacy and security protocol in a manner sufficient to ensure that PI and PHI will be handled according to the requirements contained in the DUA and Attachments. A pre-existing training that fits this description may suffice. At the end of the training, the LEAs should issue a certificate to each participant containing the name of the employee and the date of the training.

Q7. SSA Agreement with DHCS- Table 1- Seems to indicate that the agreement applies to more than Medicaid. Page 2 indicates MSP and Medicare Outreach (1144). We would like clarification that this agreement applies only to the LEA Medi-Cal Billing Option Program.

- A. It is correct that this Agreement applies only to the LEA Medi-Cal Billing Option Program. Under DHCS’ SSA Agreement, we are required to attach a copy of our SSA Agreement to all DUAs with other entities where SSA-owned data is exchanged. The SSA Agreement lists MSP and Medicare Outreach on page 2 because these are federally funded programs that DHCS administers and for which DHCS receives data from SSA. This section is not relevant to the LEAs, as this Agreement applies only to the LEA program, which is covered under Medicaid. Section 11 of the DUA lists the specific sections of the SSA Agreement that apply to the LEAs.

Q8. Regarding DUA requirements: Does the [Freeraser software](#) meet the DOD requirements?

- A. The tool needs to be able to do a complete wipe of a disk, including the free space. Use of the [Gutmann Method](#) wipe standard is also approved by DHCS, and considered superior to DoD. DHCS only supports the COMPLETE wipe of an ENTIRE DRIVE, not the wiping of individual files, folders, or volumes. No tool can guarantee or be presumed to wipe every artifact of an individual file or folder. If a file has ever been printed, copied, moved, emailed or renamed remnants of the file will still exist that can be forensically recovered. In order to completely remove a file, the ENTIRE DRIVE MUST BE WIPED, including the Operating System. Tools such as Freeraser can only run from within the Operating System, and are most often used to attempt to wipe individual files and folders. The only acceptable way to use a tool like Freeraser is on a workstation you are attaching drives to in order to completely wipe them, as secondary disk to the Operating System running the tool. No other method is allowed when using this type of free tool.
- DHCS ISO recommends that the tool allows you to boot from media, such as a CD or Thumb Drive, and completely wipe the hard drive from there. The Department uses GDisk as an example, which is a utility that comes with Symantec Ghost desktop imaging software. You boot from a CD or Thumb drive, run a menu from a prompt and WIPE THE ENTIRE DRIVE in the system from there.
 - Keep in mind that you should be doing full disk encryption on the systems hard drive and wiping is somewhat of a formality because all content on the hard drive is already protected. Doing individual wipes of a file or folder provides little value in either situation. The DHCS standard is to have fully encrypted hard drives, which are fully wiped with GDisk any time the system is being decommissioned or changing hands to another user.

ARCHIVED