State of California—Health and Human Services Agency

Department of Health Care Services

TOBY DOUGLAS
DIRECTOR

EDMUND G. BROWN JR.
GOVERNOR

Data Use Agreement Q&A

1. **Question:** On attachment B, the first page says it is the information exchange agreement between the Social Security Administration (SSA) and the DHCS. The signatures on subsection N and O are dated 2009, and subsection XI, Duration, Modification, and Termination of Agreement, it appears the agreement effective date expired last year. Based on these three observations, it is safe to assume this attachment is for information purposes?

   Answer: No. The attached Social Security Administration (SSA) Agreement is an active contract between DHCS and the SSA. Its expiration date was extended. DHCS is required to attach the SSA Agreement to any agreement for sharing of SSA-owned data, including data matching, and the party getting the data must comply with the privacy and security requirements in the SSA Agreement. The SSA Agreement, as applicable according to Section 11 of the DUA, should be considered a part of the DUA.

2. **Question:** On attachment C, the first page says it is security controls. Does this pertain to SELPA's? 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?

   Answer: The Security Controls apply to LEA signatories and any employees or agents who will access the 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 Sutter County 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.

3. **Question:** 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?"

   Answer: 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.

4. **Question:** Please define in more detail the method required for the destruction of electronic files.IE Department of Defense methods. What does that mean?

   Answer: Please see answer to Question No.3.

5. **Question:** My LEA uses a billing service. Who fills out the DUA agreement?

   Answer: The DUA agreement is ultimately the responsibility of the billing LEA or Consortium whose NPI number is used for billing (User) so this billing LEA or Consortium will fill out and sign the DUA. If the billing LEA uses a billing service, the billing LEA must have a written agreement with the billing service that imposes the same privacy and security controls on the billing service that the billing LEA has under the DUA. The billing service may also be required to sign the DUA if they are the "Custodians of the Files" on behalf of the User.

6. **Question:** If billing begins in the middle of the school year, can the DUA be turned in after 11/30/2012?

   Answer: The DUA needs to be submitted prior to the User or Custodian of Files receiving tape match data. It may be submitted in the middle of the year; however, no tape match data will be processed until it is submitted.

7. **Question:** 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)?

   Answer: 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.

8. **Question:** Will the Social Security Number (SSN) be accepted as an input field in the tape match request?

   Answer: The LEA program may ask LEAs to transmit the full social security number of their beneficiaries as long as the social security numbers are transmitted to DHCS using a secure file transfer protocol (SFTP). By complying with the Data Use Agreement and its attachments, the LEA may provide the beneficiary social security number as an input field in the tape match request, and are encouraged to do so.

9. **Question:** How can we find out how to use the M/C web portal (POS) instead of tape match?

   Answer: For information regarding available electronic methods for eligibility transactions and claims submissions go to: http://files.medi-cal.ca.gov/pubsdoco/publications/masters-mtp/.../elect_z01.doc The Automated Eligibility Verification System (AEVS) is an interactive voice response system that allows you to verify recipient eligibility through a touch-tone telephone. For more information about AEVS go to: http://files.medi-cal.ca.gov/pubsdoco/AEVS_home.asp . The Point of Service (POS) device has swipe capabilities for all plastic identification cards associated with programs served by DHCS Fiscal Intermediary and allows you to verify recipient eligibility. For more information about POS go to: http://files.medi-cal.ca.gov/pubsdoco/publications/masters-mtp/.../point_z01.doc

10. **Question:** 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?

    Answer: 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 at: ISO@dhcs.ca.gov and DHCS will provide direction and feedback.

11. **Question:** 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?

    Answer: 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 I, the "Name of User" should be the LEA

12. **Question:** P. 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?

    Answer: 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.

13. **Question:** 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.

    Answer: 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.

14. **Question:** Regarding DUA requirements: Does the Freeraser software meet the DOD requirements? The link to the software is: http://www.freeraser.com/

    Answer: The tool needs to be able to do a complete wipe of a disk, including the free space. Use of the Gutmann wipe standard is also approved by DHCS, and considered superior to DoD. See http://en.wikipedia.org/wiki/Gutmann method

    - 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.