

## **Appendix 6.0**

### Data Library Instructions

*Prospective Proposers seeking the Data Library for both procurements are not required to submit a separate set of Data Library forms (see Appendices) for each RFP. DHCS will accept one completed set of Data Library forms from prospective Proposers that intend to submit Proposals in response to both RFPs.*

#### **1. General Information**

Due to the high level of sensitivity and confidentiality of the Data Library material, DHCS must restrict access to the Data Library to prospective Proposers only. The Data Library consists of two separate sections, the General Data Library and Business Rules Data Library, each section made available via disc (DVD). Both sections comprise the complete Data Library.

Please note the following Data Library policy:

- a. A formal, written request is required to receive the Data Library material.
- b. Each prospective Proposer must designate a Point of Contact to act as its official contact for Data Library communication. This Point of Contact is the only designated contact for the prospective Proposer, its agents and subcontractors, if any, and DHCS.
- c. Only one set of General Data Library material and one set of Business Rules Data Library material on disc will be provided to each prospective Proposer.
- d. The Data Library material is the property of DHCS and must be deleted, destroyed and/or returned to DHCS, and deleted from all media, according to the procedures stated below.
- e. These rules apply to all prospective Proposers' agents and subcontractors, if any. In order to safeguard the confidentiality of Data Library material, DHCS will authorize access to the Data Library upon submission of the required Appendices. Each prospective Proposer will be required to complete the Appendices described in this section. Each Appendix submitted to the Office of Medi-Cal Procurement (OMCP) for approval and authorization **must contain the original signature of a person authorized to legally bind the company to the provisions of each Appendix**. Photocopies, email copies, or faxed copies will not be accepted.

To access the Data Library material, please submit the following Appendices:

#### **Appendix 6.2 - Request for Data Library Material**

Prospective Proposers must submit the completed "Request for Data Library Material" to receive the confidential General Data Library (General) and BR Data Library (BR) discs. This Appendix also serves as a checklist for the prospective Proposer to ensure that all required Appendices are submitted. In addition, the prospective Proposer must check either Option 1 or Option 2 as to their preferred method for delivery/receipt of both the General and the BR discs. The password for the encrypted General and BR discs will be provided to the prospective Proposer's Point of Contact via secured email once all Appendices are received and approved, and discs are picked up in person or mailed.

## **Appendix 6.0**

### Data Library Instructions

#### **Appendix 6.3 - Health Insurance Portability and Accountability Act (HIPAA) Business Associate Addendum (Data Library)**

The “Health Insurance Portability and Accountability Act Business Associate Addendum” (Data Library) describes the contractual responsibility of all DHCS Business Associate situations and outlines DHCS policy governing the use of Protected Health Information (PHI) and Personal Information (PI) in the Data Library material. This Appendix **must be signed by the person who is authorized to legally bind the prospective Proposer** to the HIPAA provisions contained in Appendix 6.3. Only one signed copy of this Appendix per prospective Proposer is required to request the General and BR discs.

#### **Appendix 6.4 - Data Library Security and Confidentiality Agreement**

Appendix 6.4 “Data Library Security and Confidentiality Agreement” must be signed **by the individual who is authorized to legally bind the prospective Proposer to the provisions of Appendix 6.4**. The “Data Library Security and Confidentiality Agreement” requires this person to acknowledge the importance of Data Library security and confidentiality and assures their agreement to comply with the security requirements regarding access to and use of the Data Library for this procurement.

#### **Appendix 6.5 - Data Library Disc Return and Media Destruction Agreement**

The “Data Library Disc Return and Media Destruction Agreement” describes DHCS’ policy for the return and/or destruction of the Data Library material. Submit the original page 2 of Appendix 6.5, signed **by the individual who is authorized to legally bind the prospective Proposer to the provisions of this Appendix**, to acknowledge and agree to transmit the return of the Data Library discs to DHCS and for details on how to notify DHCS that all Data Library material copied to other media has been destroyed. Submit a copy of page 2 of Appendix 6.5 when returning the CD/DVD’s to DHCS. Please follow the instructions provided in Appendix 6.5.

## **2. Content**

The Data Library is fully electronic and will be available on disc. See Appendix 6.1, “Data Library Index” for details concerning the Data Library material contained on each disc. The General and BR Data Library material is on single layer 4.7 GB DVD +/- R DVDs or CDs. It is the responsibility of the prospective Proposer to have the necessary equipment to view the information contained on these discs. Discs are encrypted and the encryption password will be provided only by secured email to the prospective Proposer’s Point of Contact designated on Appendix 6.2, “Request for Data Library”.

## **3. Data Library Disc Return and Media Destruction**

The Data Library material, including all updated discs that DHCS may supply to the prospective Proposer, is the property of DHCS and must be destroyed and/or returned to DHCS within ten (10) calendar days after either the award of a Contract, a notice by DHCS of intent not to award a Contract, or upon notification by the State to return and/or destroy

**Appendix 6.0**  
Data Library Instructions

the material. These requirements apply to all prospective Proposers, whether or not a Proposal is submitted.

All DHCS Data Library material must be destroyed, including material copied to other media, when the data is no longer necessary for the purpose for which it was intended. The removal method must conform to the National Institutes of Standards and Technology (NIST). Once all Data Library material has been deleted and/or destroyed, the prospective Proposer's Point of Contact must notify DHCS of its deletion and/or destruction by sending an e-mail to: [omcprfp2@dhcs.ca.gov](mailto:omcprfp2@dhcs.ca.gov) with the subject line "Data Library Deletion/Destruction - RFP 13-90271".

**Appendix 6.1**  
General Data Library Index (discs)

<b>1.0 - 3.0 2004 CD-MMIS PROCUREMENT (CURRENT CONTRACT)</b>		Original Added	Revised or Added
1.0	2003 Dental Request for Proposal	April 2014	
2.0	2003 Delta Dental Plan of California Technical and Cost Proposal	April 2014	
3.0	Dental Contract 04-35745 (Effective 11/04)	April 2014	
<b>3.1 CHANGE ORDERS</b>		Original Added	Revised or Added
3.1.1	Change Order 1 Proposal-Beneficiary Service Dental Cap	April 2014	
3.1.2	Change Order 2 Health Insurance Portability and Accountability Act - Current Dental Terminology	April 2014	
3.1.3	Change Order 3 Annual Pure Premium Rate Phase 1	April 2014	
3.1.4	Change Order 4 Provider Telephone Service Center Bid Rates, Phase 2, 3, 4 and Contract Extension Years 1, 2 and 3	April 2014	
3.1.5	Change Order 5 Annual Pure Premium Rate Phase 2	April 2014	
3.1.6	Change Order 6 Health Insurance Portability and Accountability Act (HIPAA) - Current Dental Terminology (CDT)	April 2014	
3.1.7	Change Order 7 Conlan vs. Shewry Case – Retroactive Reimbursement of Medi-Cal Beneficiaries for Out-Of- Pocket Expenses	April 2014	
3.1.8	Change Order 8 Health Insurance Portability and Accountability Act (HIPAA) National Provider Identifier (NPI) Implementation	April 2014	
3.1.9	Change Order 9 Health Insurance Portability and Accountability Act (HIPAA) Addendum - Security Risk Assessment Process – Revision 2	April 2014	
3.1.10	Change Order 10 Annual Pure Premium Rate Phase 3	April 2014	
3.1.11	Change Order 11 Pure Premium Rate for July 2008	April 2014	
3.1.12	Change Order 12 Annual Pure Premium Rate Phase 4	April 2014	
3.1.13	Change Order 13 Temporary Beneficiary Call Center	April 2014	
3.1.14	Change Order 14 Elimination of Optional Adult Dental Services	April 2014	
3.1.15	Change Order 15 Mid-Year Pure Premium Rate Change for the Period March 2009 through June 2009	April 2014	
3.1.16	Change Order 16 Pure Premium Rate for July 2009	April 2014	
3.1.17	Change Order 17 Annual Pure Premium Rates for Extension Phase 1	April 2014	
3.1.18	Change Order 18 Ten Percent Erroneous Payment Corrections for July 1, 2008 through August 17, 2008	April 2014	
3.1.19	Change Order 19 Annual Pure Premium Rates for Extension Phase II	April 2014	
3.1.20	Change Order 20 Annual Pure premium Rates for Extension Phase III	April 2014	
3.1.21	Change Order 21 Removal of Turnover and Runout Services and Costs	April 2014	
3.1.22	Change Order 22 Mid-Year Pure Premium Rates for Extension Phase III – Extended Operations	April 2014	

**Appendix 6.1**  
General Data Library Index (discs)

3.1.23	Change Order 23	Federal Rule: Revalidation of Enrollment	April 2014	
3.1.24	Change Order 24	Federal Rule: Federal Database Checks	April 2014	
3.1(1)	Supplement to Change Orders 7, 9, 23 & 24 – DC04-13418 to DC04-13953			June 2014
3.1(2)	Supplement to Change Orders 7, 9, 23 & 24 – DC04-14519 to DC04-14972			Jan 2015
3.1(3)	Supplement to Change Orders 7, 9, 23 & 24 – DC04-15075 to DC04-15852			July 2015
3.2	Contract Waiver Letters		April 2014	
3.2(1)	Supplement to Contract Waiver Letters			June 2014
3.2(2)	Supplement to Contract Waiver Letters			Jan 2015
3.2(3)	Supplement to Contract Waiver Letters			July 2015
<b>4.0</b>	<b>DEPARTMENT OF HEALTH SERVICES LETTERS (S LETTERS) THESE ARE ALL LETTERS TO THE DENTAL F.I. INCLUDING BUT NOT LIMITED TO, DOILs, SDNs, MCDs, AND CWLs, IN CHRONOLOGICAL ORDER.</b>		<b>Original Added</b>	<b>Revised or Added</b>
4.1	S-0001 to S-1999 dated from 10/27/05 - 04/18/08		April 2014	
4.2	S-2000 to S-3999 dated from 04/18/08 - 01/14/10		April 2014	
4.3	S-4000 to S-5999 dated from 01/19/10 - 04/16/13		April 2014	
4.4	S-6000 to S-6311 dated from 04/16/13 - 09/30/13		April 2014	
4.5	S-6312 to S-6783 dated from 10/02/13 - 05/14			June 2014
4.6	S-6784 to S-7168 dated from 06/03/14 - 12/29/14			Jan 2015
4.7	S-7169 to S-7575 dated from 01/02/15 – 06/30/15			
<b>5.0</b>	<b>DENTAL FISCAL INTERMEDIARY LETTERS (D LETTERS) These are all letters to the Department of Health Services including, but not limited to, DOILs, SDNs, MCDs, and CWLs, in chronological order.</b>		<b>Original Added</b>	<b>Revised or Added</b>
5.1	D-0001 to D0099 dated from 07/26/04 - 01/24/06		April 2014	
5.2	D-1000 to D1999 dated from 12/21/05 - 08/15/06		April 2014	
5.3	D-2000 to D2999 dated from 08/15/06 - 04/10/07		April 2014	
5.4	D-3000 to D3999 dated from 04/10/07 - 11/20/07		April 2014	
5.5	D-4000 to D4999 dated from 11/20/07 - 06/27/08		April 2014	
5.6	D-5000 to D5999 dated from 06/27/08 - 02/05/09		April 2014	
5.7	D-6000 to D6999 dated from 02/09/09 - 09/26/09		April 2014	
5.8	D-7000 to D7999 dated from 09/23/09 - 06/10/10		April 2014	
5.9	D-8000 to D8997 dated from 06/10/10 - 02/18/11		April 2014	
5.10	D-9000 to D9999 dated from 02/18/11 - 11/03/11		April 2014	
5.11	D-10000 to D10999 dated from 11/03/11 - 07/09/12		April 2014	
5.12	D-11000 to D11999 dated from 07/09/12 - 03/18/13		April 2014	
5.13	D-12000 to D12889 dated from 03/18/13 - 09/30/13		April 2014	
5.14	D-12890 to D14014 dated from 10/01/13 - 05/31/14		June 2014	

**Appendix 6.1**  
General Data Library Index (discs)

5.14(a) D-14019 to D15014 dated from 06/02/14 - 12/30/14		Jan 2015
5.15 D-15015 to D15898 dated from 01/05/15 - 06/29/15		July 2015
<b>6.0 CD-MMIS MANUALS</b>	<b>Original Added</b>	<b>Revised or Added</b>
6.1 Operations Manuals	June 2014	
6.1.1 Operations Manuals Index	June 2014	
6.2 System Manuals	June 2014	
6.3 Claims Processing Flowchart	June 2014	
6.1 - 6.3 Supplement to Operations and System Manuals		Jan 2015
6.1 - 6.3 Supplement to Operations and System Manuals #2		July 2015
<b>7.0 - 8.0 ONLINE DATA LIBRARY MATERIAL</b>	<b>Original Added</b>	<b>Revised or Added</b>
7.0 Denti-Cal Provider Handbook	April 2014	Continuous
8.0 Denti-Cal Provider Bulletins/Index	April 2014	Continuous
<b>9.0 DENTAL OPERATING INSTRUCTION LETTERS (DOILs)</b>	<b>Original Added</b>	<b>Revised or Added</b>
9.0 Dental Operating Instruction Letters	April 2014	
9.0(1) Supplement to Dental Operating Instruction Letters (DOILs)		June 2014
9.0(2) Supplement to Dental Operating Instruction Letters (DOILs)		Jan 2015
9.0(3) Supplement to Dental Operating Instruction Letters (DOILs)		July 2015
<b>10.0 CD-MMIS PROGRAM SOFTWARE INDEX INCLUDES DENTAL FEE-FOR-SERVICE AND DENTAL MANAGED CARE PROGRAMS. THE TAPES ARE LISTED ON INDEX 10.0 BY NUMBER AND THE CONTENTS OF EACH TAPE ARE DESCRIBED.</b>	<b>Original Added</b>	<b>Revised or Added</b>
10.1A CD-MMIS Program Software (Mainframe)	June 2014	
10.1A.1 + 10.1A.2 Software (Mainframe) Supplement		Jan/July 15
10.1B&C CD-MMIS Program Software Source Code/Program Software (Non-Mainframe)	June 2014	
10.1B + 10.1C Program Software Source Code/Program Software (Non-Mainframe) Supplement		Jan/July 15
<b>11.0 CD-MMIS PRODUCTION JOBS</b>	<b>Original Added</b>	<b>Revised or Added</b>
11.0 CD-MMIS Production Jobs (November 2013 to May 2014)	June 2014	
11.0(a) CD-MMIS Production Jobs (June 2014 to December 2014) MN-0-180 to MN-0-185		Jan 2015

**Appendix 6.1**  
General Data Library Index (discs)

<b>12.0 SYSTEM DEVELOPMENT NOTICES (SDNs)</b>	<b>Original Added</b>	<b>Revised or Added</b>
12.0 System Development Notices (05/2005 - 09/30/2013)	April 2014	
12.0(1) Supplement to System Development Notices (10/2013 - 05/2014)		June 2014
12.0(2) Supplement to System Development Notices (06/2014 - 12/2014)		JAN 2015
12.0(3) Supplement to System Development Notices (01/2015 - 06/2015)		JULY 2015
<b>13.0 MISCELLANEOUS CHANGE DOCUMENTS (MCDs)</b>	<b>Original Added</b>	<b>Revised or Added</b>
13.0 Miscellaneous Change Documents (05/2005 - 09/30/2013)	April 2014	
13.0(1) Supplement to Miscellaneous Change Documents (10/2013 - 05/2014)		June 2014
13.0(2) Supplement to Miscellaneous Change Documents (06/2014 - 12/2014)		Jan 2014
13.0(3) Supplement to Miscellaneous Change Documents (01/2015 - 06/2015)		July 2015
<b>14.0 ELIGIBILITY SUMMARY REPORTS - Report DHS-FAM 110</b>	<b>Original Added</b>	<b>Revised or Added</b>
14.1 2006 Summary	April 2014	
14.2 2007 Summary	April 2014	
14.3 2008 Summary	April 2014	
14.4 2009 Summary	April 2014	
14.5 2010 Summary	April 2014	
14.6 2011 Summary	April 2014	
14.7 2012 Summary	April 2014	
14.8 2013 Summary	April 2014	
14.8(1) Supplement to 2013 Summary		June 2014
14.9 2014 Summary (to May 2014)		June 2014
14.10 2014 Summary (June to December 2014)		Jan 2015
14.11 2014 Summary (January to June 2015)		July 2015
<b>15.0 ADMINISTRATIVE/OPERATIONS BILLING REPORTS - Reports CP-0-495, 496 &amp; 497 (Monthly reports)</b>	<b>Original Added</b>	<b>Revised or Added</b>
15.1 Contract Year 1 - 05/05 - 06/06	April 2014	
15.2 Contract Year 2 - 07/06 - 06/07	April 2014	
15.3 Contract Year 3 - 07/07 - 06/08	April 2014	
15.4 Contract Year 4 - 07/08 - 06/09	April 2014	
15.5 Contract Year 5 - 07/09 - 06/10	April 2014	

**Appendix 6.1**  
General Data Library Index (discs)

15.6	Contract Year 6 - 07/10 - 06/11	April 2014	
15.7	Contract Year 7 - 07/12 - 06/12	April 2014	
15.8	Contract Year 8 - 07/12 - 6/30/13	April 2014	
15.9	Contract Year 9+ - 07/13 - 12/14		Jan 2015
15.9(1)	Contract Year 9+ - 01/15 - 06/15		July 2015
<b>16.0</b>	<b>REPORTS (See Item #6 Operation Manuals for a description of each report.)</b>	<b>Original Added</b>	<b>Revised or Added</b>
16.1	Report Distribution List by Report	April 2014	
<b>17.0</b>	<b>MONTHLY MR-0-015 REPORT (Lag times between dates of service and date of payment)</b>	<b>Original Added</b>	<b>Revised or Added</b>
17.0	Monthly MR-0-015 Report (01/13-09/2013)	April 2014	
17.0(1)	Supplement to Monthly MR-0-015 Report (10/13 - 05/14)		June 2014
17.0(2)	Supplement to Monthly MR-0-015 Report (06/14 - 12/14)		Jan 2015
17.0(3)	Supplement to Monthly MR-0-015 Report (01/15 - 06/15)		July 2015
<b>18.0</b>	<b>TELEPHONE SERVICE CENTER DATA - Reports MR-O-495, MR-O-496 &amp; MR-O-497 (Monthly reports)</b>	<b>Original Added</b>	<b>Revised or Added</b>
18.1	Contract Year 1 – 05/05 - 06/06	April 2014	
18.2	Contract Year 2 – 07/06 - 06/07	April 2014	
18.3	Contract Year 3 – 07/07 - 06/08	April 2014	
18.4	Contract Year 4 – 07/08 - 06/09	April 2014	
18.5	Contract Year 5 – 07/09 - 06/10	April 2014	
18.6	Contract Year 6 – 07/10 - 06/11	April 2014	
18.7	Contract Year 7 – 07/11 - 06/12	April 2014	
18.8	Contract Year 8 – 07/12 - 06/13	April 2014	
18.9	Contract Year 9+ – 07/13 - 12/14		Jan 2015
18.10	Contract Year 10 – 01/15 - 06/15		July 2015
<b>19.0</b>	<b>PROVIDER SUMMARY INFORMATION</b>	<b>Original Added</b>	<b>Revised or Added</b>
19.0	PS-O-012A, B (01/13 - 09/30/13)	April 2014	
19.0(1)	Supplement to PSI (10/13 - 05/14)		June 2014
19.0(2)	Supplement to PSI (06/14 - 12/14)		Jan 2015

**Appendix 6.1**  
General Data Library Index (discs)

19.0(3) Supplement to PSI (01/15 - 06/15)		July 2015
<b>20.0 PROBLEM STATEMENTS, AND ERRONEOUS PAYMENT Correction Runs (EPP PS)</b>	<b>Original Added</b>	<b>Revised or Added</b>
20.0 Problem Statements (01/13 - 09/30/13)	April 2014	
20.0(1) Supplement to Problem Statements (10/13 - 05/14)		June 2014
20.0(2) Supplement to Problem Statements (06/14 - 12/14)		Jan 2015
20.0(3) Supplement to Problem Statements (01/15 - 06/15)		July 2015
<b>21.0 MONTHLY NUMBER OF CLAIMS</b>	<b>Original Added</b>	<b>Revised or Added</b>
21.1 Prior Authorization, Special Claims Review (01/13-09/13) (See Item #22 Incoming and Outgoing count of Claims/NOAs and TARs Report CP-O-503B for Prior Authorization, Special Claims Reviews)	April 2014	
21.2 Manual Pricing MR-O-331		JULY 2015
<b>22.0 INCOMING AND OUTGOING COUNT OF CLAIMS/NOA'S (AND REPLATED DOCUMENTS) AND TAR'S (AND RELATED DOCUMENTS)</b>	<b>Original Added</b>	<b>Revised or Added</b>
22.0 Report CP-O-503B (03/09 - 09/13)	April 2014	
22.0(1) Incoming and Outgoing count of Claims/NOAs (and related documents) and TARs (and related documents) Report CP-O-503B (10/13 - 05/14)		June 2014
22.0(2) Incoming and Outgoing count of Claims/NOAs (and related documents) and TARs (and related documents) Report CP-O-503B (06/14 - 12/14)		Jan 2015
22.0(3) Incoming and Outgoing count of Claims/NOAs (and related documents) and TARs (and related documents) Report CP-O-503B (01/15 - 06/15)		July 2015
<b>23.0 LIST OF AD HOC REQUESTS FOR INFORMATION WITH REFERENCE NUMBERS</b>	<b>Original Added</b>	<b>Revised or Added</b>
23.0 (1/13 - 9/13) (This item only contains STARS ad hoc reports. For other ad hoc reports see Item 13 Miscellaneous Change Documents)	April 2014	
23.0(1) (10/13 - 05/14) (This item only contains STARS ad hoc reports. For other ad hoc reports see Item 13 Miscellaneous Change Documents)		June 2014
23.0(2) (06/14 - 12/14) (This item only contains STARS ad hoc reports. For other ad hoc reports see Item 13 Miscellaneous Change Documents)		Jan 2015
23.0(3) (01/15 - 06/15) (This item only contains STARS ad hoc reports. For other ad hoc reports see Item 13 Miscellaneous Change Documents)		July 2015

**Appendix 6.1**  
General Data Library Index (discs)

<b>24.0-25.0 YEARLY/QUARTERLY MR-0-334-1 REPORT, INCIDENCE OF DENTAL - Procedures (by Procedure &amp; Age)</b>	<b>Original Added</b>	<b>Revised or Added</b>
24.1 Contract Year 1 - 05/05 - 06/06	April 2014	
24.2 Contract Year 2 - 07/06 - 06/07	April 2014	
24.3 Contract Year 3 - 07/07 - 06/08	April 2014	
24.4 Contract Year 4 - 07/08 - 06/09	April 2014	
24.5 Contract Year 5 - 07/09 - 06/10	April 2014	
24.6 Contract Year 6 - 07/10 - 06/11	April 2014	
24.7 Contract Year 7 - 07/11 - 06/12	April 2014	
24.8 Contract Year 8 - 07/12 - 09/13	April 2014	
24.9(1) Quarterly 10/13 - 12/13		June 2014
25.0(1) Quarterly 01/14 - 03/14		June 2014
25.0(2) Quarterly x 2 - 04/14 - 09/14		Jan 2015
25.1 Quarterly x 2 – 10/14 - 04/15		July 2015
<b>26.0 DHCS' INFORMATION SYSTEM SECURITY PLANNING REQUIREMENTS</b>	<b>Original Added</b>	<b>Revised or Added</b>
26.0 Information System Security Planning Requirements	May 2014	

**Note:** Index entries that are identified as “Revised or Added” will be found on the supplemental disc(s) labeled with that month/year date.

All original data shown with an “Original Added” month/year date will be located on discs labeled 1 - 4 as follows:

**General Data Library**

**Disc 1 - Index Categories 1.0 to 4.0**

**Disc 2 - Index Categories 5.0 (part 1)**

**Disc 3 - Index Categories 5.0 (part 2) to 11.0**

**Disc 4 - Index Categories 12.0 to 24.0 and 26.0** (Index Category 25.0 is part of the June 2014 supplemental disc)

**Disc 5 - Supplemental Disc dated June 2014**

**Disc 6 - Supplemental Disc dated January 2015**

**Disc 7 - Supplemental Disc dated July 2015**

**Business Rules Data Library**

**Disc 8 - July 2015** (see disc for information concerning the contents and use of the information contained on the disc)

**Appendix 6.2**  
Request for Data Library Material

The prospective Proposer must submit this completed Appendix to receive the Data Library material. All Data Library material will be in electronic format. The Office of Medi-Cal Procurement (OMCP) will provide each prospective Proposer with one set of General Data Library material and one set of Business Rules (BR) Data Library material on encrypted discs. Following receipt of the required Appendices, OMCP will send the prospective Proposer-designated Point of Contact a secure email containing a password to open each encrypted disc.

**Please submit to DHCS:**

- 1) Appendix 6.2, "Request for Data Library Material", must be completed by the prospective Proposer and signed by an official with the authority to legally bind the prospective Proposer to the provisions of Appendix 6.2.
- 2) Appendix 6.3, "HIPAA Business Associate Addendum" (Data Library), must be completed and signed by an official with the authority to legally bind the prospective Proposer to the provisions of the agreement.
- 3) Appendix 6.4, "Data Library Security and Confidentiality Agreement". Appendix 6.4 must be completed by the prospective Proposer and signed by an official with the authority to legally bind the prospective Proposer to the provisions of Appendix 6.4.
- 4) Appendix 6.5, "Data Library Disc Return and Media Destruction Agreement", must be completed by the prospective Proposer and signed by an official with the authority to legally bind the prospective Proposer to the provisions of Appendix 6.5.

**Please check one of the delivery and pick-up options below to request the discs containing the Data Library material:**

**Option 1 – U.S. Mail, Overnight courier/delivery service**

The prospective Proposer may request the Data Library by mail. The General Data Library and BR Data Library discs will be mailed to the prospective Proposer's Point of Contact by OMCP via overnight delivery upon receipt of the following:

- All the required forms as noted above.
- The prospective Proposer's physical address used for overnight mail.
- A shipping label for the prospective Proposer's overnight courier/delivery service which contains the prospective Proposer's pre-paid carrier account number (Fed-Ex, UPS, etc.)

Please refer to the section below for information about sending mail to DHCS. Additionally, please allow OMCP two business days from receipt of the Data Library Appendices to process the Data Library request.

**Please mail all completed Appendices listed above as follows:**

<b>Hand Delivery or Overnight Express:</b>	<b>United State Postal Service Mail:</b>
<p><b>Request for Data Library Discs</b> <b>RFP 13-90271</b> Department of Health Care Services Office of Medi-Cal-Procurement Mail Station 4200 1501 Capitol Avenue, Suite 71.3041 Sacramento, CA 95814</p>	<p><b>Request for Data Library Discs</b> <b>RFP 13-90271</b> Department of Health Care Services Office of Medi-Cal Procurement Mail Station 4200 P.O. Box 997413 Sacramento, CA 95899-7413</p>

**Appendix 6.2**  
Request for Data Library Material

**Option 2 – In-Person Delivery of Appendices and Pick-Up of Discs at OMCP**

The prospective Proposer may hand deliver the required Appendices to DHCS' OMCP to request the General and BR Data Library discs. The prospective Proposer must contact OMCP staff to schedule an appointment to deliver the required Appendices. The General and BR Data Library discs will be provided to the prospective Proposer by OMCP upon receipt of the following:

- All the required forms as noted above.
- The name of the person who will deliver the required Appendices to DHCS at 1501 Capitol Avenue, Sacramento, CA 95814.
- The name of the person who will pick up the discs from DHCS at the address directly above.

Please allow OMCP two business days to process the Data Library request and to prepare the discs for pick-up. OMCP will contact the prospective Proposer's Point of Contact to arrange a time to pick up the Data Library discs.

The prospective Proposer's Point of Contact must present acceptable identification when delivering the required Appendices and when picking up the discs at DHCS. Acceptable picture identification includes a valid driver license, State-issued identification card, or an active identification issued by a federal agency.

The prospective Proposer may arrange appointments for the hand-delivery of the required Appendices and pickup of the Data Library discs by contacting OMCP staff through one of the following methods:

<b>Phone:</b>	<b>Email:</b>
(916) 552-8006	Send to: OMCPRFP2@dhcs.ca.gov Subject: Data Library Material Request - RFP 13-90271

**Complete the Proposer information below.**

Name of Firm		
Address		
City	State	Zip
Prospective Proposer's Point of Contact <i>(print)</i>		
Prospective Proposer's Point of Contact Signature <i>(original signature required)</i>		
Title		
Email	Phone	FAX
Company Official <i>(print)</i> <i>(Person authorized to legally bind the prospective Proposer to all of the provisions in this Appendix.)</i>		
Official's Signature <i>(original signature required)</i> <i>(Person authorized to legally bind the prospective Proposer to all of the provisions in this Appendix.)</i>		
Title		

**Appendix 6.2**  
Request for Data Library Material



**FOR DHCS USE**

Option 1 – U.S. Mail, Overnight Courier/Delivery Service

Prospective Proposer's request received on: (date) <small>(by staff)</small>	All Appendices Confirmed: Yes <input type="checkbox"/> No <input type="checkbox"/> <small>(by staff)</small>
Discs mailed by OMCP: (date) <small>(by staff )</small>	Password emailed on: (date) <small>(by staff)</small>
Carrier:	Tracking #:

Option 2 – In-Person Delivery of Appendices and Pick-Up of Discs at OMCP

Prospective Proposer's request received on: (date) <small>(by staff)</small>	All Appendices Confirmed: Yes <input type="checkbox"/> No <input type="checkbox"/> <small>(by staff)</small>
Appointment delivery: (date) (time) <small>(by staff)</small>	
Disc pick-up: (date) (time) <small>(by staff)</small>	
ID verification:	Password emailed on: (date) <small>(by staff)</small>

SIGNED BY \_\_\_\_\_

(OMCP Official)

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)**I. Recitals**

- A. This Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate Addendum (Data Library) ("BAA" or "Addendum") accompanies the Request for Proposal (RFP); it has been determined necessary to require a business associate relationship under HIPAA, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ('the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Health Care Services ("DHCS") wishes to disclose to Business Associate certain information pursuant to the terms of this BAA, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in this BAA, prospective Proposer, here and after, is the Business Associate of DHCS that receives, maintains, or uses PHI and/or PI. DHCS and Business Associate are each a party to this BAA and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, or used pursuant to this BAA, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that DHCS must enter into an agreement containing specific requirements with prospective Proposer prior to the disclosure of PHI and PI to prospective Proposer, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**II. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.
- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI and PI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act, and the HIPAA regulations.

**III. Terms of the BAA****A. Permitted Uses of PHI and PI by Business Associate**

**Permitted Uses.** Except as otherwise indicated in this Addendum, Business Associate may use PHI and PI only to perform functions, activities or services specified in this BAA, for, or on behalf of DHCS, provided that such use would not violate the HIPAA regulations, if done by DHCS. Any such use must,

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2.

1. **Specific Use Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:

**a. Use for management and administration.** Use PHI and PI for the proper management and administration of the Business Associate.

**B. Prohibited Uses**

1. Business Associate shall not disclose PHI and PI in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI and PI, except with the prior written consent of DHCS and as permitted by 42 U.S.C. section 17935(d)(2).

**C. Responsibilities of Business Associate**

Business Associate agrees:

1. **Nondisclosure.** Not to use PHI and PI other than as permitted or required by this BAA or as required by law.
2. **Safeguards.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI and PI, including electronic PHI and PI, that it creates, receives, maintains, or uses on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use of PHI and PI other than as provided for by this BAA. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Business Associate will provide DHCS with its current and updated policies.
3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
  - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in using PHI and/or PI under this BAA;
  - c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130,

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

- d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI and/or PI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of this BAA.

Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with DHCS.

- D. *Mitigation of Harmful Effects.*** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use of PHI and/or PI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

**E. *Business Associate's Agents and Subcontractors.***

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of DHCS, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act the HIPAA regulations, and the Final Omnibus Rule, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business associates are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, or maintains protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract, subaward or agreement to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.
2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; or
  - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)**F. Availability of Information to DHCS and Individuals.** To provide access and information:

1. To provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI and PI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.
2. If Business Associate receives data from DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

**G. Amendment of PHI and PI.** To make any amendment(s) to PHI and PI that DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by DHCS.**H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use of PHI and PI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.**I. Documentation of Disclosures.** If and as applicable, to document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI and PI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI and PI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for DHCS as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for DHCS after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.**J. Breaches and Security Incidents.** During the term of this BAA, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. **Notice to DHCS.** (1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

**within twenty-four (24) hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this BAA and this Addendum, or potential loss of confidential data affecting this BAA. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Notice shall be provided to the Chief, Office of Medi-Cal Procurement (OMCP) the DHCS Privacy Officer and the DHCS Information Security Officer. *If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS Enterprise Innovation Technology Services (EITS) Service Desk.* Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website ([www.dhcs.ca.gov](http://www.dhcs.ca.gov), then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, Business Associate shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Chief, OMCP, the DHCS Privacy Officer, and the DHCS Information Security Officer:
3. **Complete Report.** To provide a complete report of the investigation to the Chief, OMCP, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve or disapprove the determination of whether a breach occurred, is reportable to the appropriate entities, if individual notifications are required, and the corrective action plan.

**Appendix 6.3**

Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days. The Chief, OMCP, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.
  
5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI and/or PI involves more than five hundred (500) residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to Business Associate, Business Associate shall notify DHCS, and DHCS and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
  
6. **DHCS Contact Information.** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum to which it is incorporated.

Chief, OMCP	DHCS Privacy Officer	DHCS Information Security Officer
See the RFP Main for OMCP contact information	Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413  Email: <a href="mailto:privacyofficer@dhcs.ca.gov">privacyofficer@dhcs.ca.gov</a>  Telephone: (916) 445-4646  Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413  Email: <a href="mailto:iso@dhcs.ca.gov">iso@dhcs.ca.gov</a> Fax: (916) 440-5537  Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874

- K. **Termination of BAA.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by DHCS of this Addendum, it shall take the following steps:
  1. Provide an opportunity for DHCS to cure the breach or end the violation and terminate the BAA if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or
  2. Immediately terminate the BAA if DHCS has breached a material term of the Addendum and cure is not possible.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

- L. *Due Diligence.*** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.
- M. *Sanctions and/or Penalties.*** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

**IV. Obligations of DHCS**

DHCS agrees to:

- A. *Notice of Privacy Practices.*** Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx> or the DHCS website at [www.dhcs.ca.gov](http://www.dhcs.ca.gov) (select "Privacy in the left column and "Notice of Privacy Practices" on the right side of the page).
- B. *Permission by Individuals for Use of PHI and/or PI.*** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use PHI and/or PI, if such changes affect the Business Associate's permitted or required uses.
- C. *Notification of Restrictions.*** Notify the Business Associate of any restriction to the use of PHI and/or PI that DHCS has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use of PHI and/or PI.
- D. *Requests Conflicting with HIPAA Rules.*** Not request the Business Associate to use PHI and PI in any manner that would not be permissible under the HIPAA regulations if done by DHCS.

**V. Audits, Inspection and Enforcement**

- A.** From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':
1. Failure to detect, or
  2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' enforcement rights under this Addendum.
- B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify DHCS and provide DHCS with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

**VI. Termination**

- A. Term.** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond either the date of the notice of intent to award or the date of the decision to not award the Contract, and shall terminate when all the PHI and PI provided by DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, is destroyed or returned to DHCS, in accordance with 45 CFR 164.504(e)(2)(ii)(I) and as stated in RFP Main, Data Library section.
- B. Termination for Cause.** In accordance with 45 CFR section 164.504(e)(1)(ii), upon DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS shall:
1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this BAA if Business Associate does not cure the breach or end the violation within the time specified by DHCS; or
  2. Immediately terminate this BAA if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. Judicial or Administrative Proceedings.** Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this BAA if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this BAA if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. Effect of Termination.** Upon termination or expiration of this BAA for any reason, Business Associate shall return or destroy all PHI and PI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI and PI. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI and/or PI. Business Associate shall continue to extend the protections of this Addendum to such PHI and PI, and shall limit further use of such PHI and/or PI to those purposes that make the return or destruction of such PHI and PI infeasible. This provision shall apply to PHI and PI that is in the possession of subcontractors or agents of Business Associate.

**VII. Miscellaneous Provisions**

- A. Disclaimer.** DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI and PI.
- B. Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

HIPAA regulations and other applicable laws relating to the security or privacy of PHI and PI. Upon DHCS' request, Business Associate agrees to promptly enter into negotiations with DHCS concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. DHCS may terminate this BAA upon thirty (30) calendar days written notice in the event:

1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by DHCS pursuant to this Section; or
2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI and PI that DHCS in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

**C. Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this BAA, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

**D. No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

**E. Interpretation.** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.

**F. Regulatory References.** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.

**G. Survival.** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of this BAA.

**H. No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)**Attachment A**

## Business Associate Data Security Requirements

**I. Personnel Controls**

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access DHCS PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six years following the BAA termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. The prospective Proposer shall retain each person's written confidentiality statement for DHCS inspection for a period of six years following the BAA termination.
- D. *Background Check.*** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The prospective Proposer shall retain each workforce member's background check documentation for a period of three years following BAA termination.

**II. Technical Security Controls**

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
- B. *Server Security.*** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes, etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

- E. *Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. *Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) calendar days of vendor release.
- G. *User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours after transfer or termination. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every ninety (90) calendar days, preferably every sixty (60) calendar days. Passwords must be changed if revealed or compromised within twenty-four (24) hours of revelation or compromising situation. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Arabic numerals (0-9)
  - Non-alphanumeric characters (punctuation symbols)
- H. *Data Destruction.*** When no longer needed, all DHCS PHI and PI must be cleared, purged, or destroyed consistent with National Institutes of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization such that the PHI and PI cannot be retrieved.
- I. *System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
- J. *Warning Banners.*** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. *System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.
- L. *Access Controls.*** The system providing access to DHCS PHI and/or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)

**M. *Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

**III. Audit Controls**

**A. *System Security Review.*** All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

**B. *Log Reviews.*** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

**C. *Change Control.*** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

**IV. Business Continuity / Disaster Recovery Controls**

**A. *Emergency Mode Operation Plan.*** Prospective Proposer must establish a documented plan to enable continuation of protection of the security of electronic DHCS PHI and PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work to protect PHI and PI required under this BAA for more than twenty-four (24) hours.

**B. *Data Backup Plan.*** Prospective Proposer must have established documented procedures to backup DHCS PHI and PI to maintain retrievable exact copies of DHCS PHI and PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI and PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

**V. Paper Document Controls**

**A. *Supervision of Data.*** DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

**B. *Escorting Visitors.*** Visitors to areas where DHCS PHI and/or PI is contained shall be escorted and DHCS PHI and PI shall be kept out of sight while visitors are in the area.

**C. *Confidential Destruction.*** DHCS PHI and PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

**D. *Removal of Data.*** DHCS PHI and PI must not be removed from the premises of the prospective Proposer except with express written permission of DHCS.

**Appendix 6.3**Health Insurance Portability and Accountability Act of 1996  
Business Associate Addendum (Data Library)**Complete the prospective Proposer information below:**

Name of Firm		
Address		
City	State	Zip
<b>Name of person who is <u>authorized to legally bind the prospective Proposer to this Business Associate Agreement</u> (print)</b>		
Signature (original signature required)		
Title		
Email	Phone	Fax

**Note:** This Appendix 6.3 pertains to all Data Library material. The Health Insurance Portability and Accountability Act Business Associate Addendum is also contained as an exhibit within the RFP. Should a Contract ultimately be awarded, a new Health Insurance Portability and Accountability Act Business Associate Addendum will be a part of the Contract. Therefore, this Appendix **must be signed by a person who is authorized to legally bind the prospective Proposer to this Business Associate Agreement.**

**Appendix 6.4**  
Data Library Security and Confidentiality Agreement

**THIS AGREEMENT** is entered into this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_ by and between the State of California, Department of Health Care Services, Office of Medi-Cal Procurement, through its duly authorized representative, hereafter called "the State", and \_\_\_\_\_, hereafter called "prospective Proposer's Point of Contact".

**RECITALS**

- A. For the purposes of facilitating the preparation of Proposals for this Procurement, a Data Library has been established. The data and materials in the Data Library are confidential and otherwise unavailable for public review.
- B. It is essential that specified measures be taken by each prospective Proposer being accorded access to the Data Library materials in order to safeguard the confidentiality of such materials.
- C. The parties desire to define and set forth the precautions and specific safeguards to be taken by the prospective Proposer and the State in order to preserve the confidentiality of the Data Library materials.

NOW THEREFORE, the parties hereto agree as follows:

**SECTION I: GENERAL INFORMATION ABOUT THE DATA LIBRARY**

- A. **Prospective Proposer's Point of Contact** – The prospective Proposer's Point of Contact hereby certifies that he/she understands that the materials contained in the Procurement Project Data Library are confidential in nature, and agrees that the Data Library materials provided by the State of California are provided solely for the purpose of preparing a response to the Request for Proposal (RFP). Prospective Proposer's Point of Contact is responsible for all access to the Data Library content by any affiliate personnel and subcontractors.
- B. **Security Procedures** - It is agreed that any confidential information contained in the Data Library, or future information made available, is designated by the State as confidential, including information on a medium other than paper. Such information will not be disclosed to anyone other than the prospective Proposer's Point of Contact who will use the materials exclusively in the performance of their duties while working on the Proposal.
- C. **Prohibited Use** - It is further agreed that the prospective Proposer's Point of Contact will not copy or otherwise reproduce any Data Library information without the express written approval of the State and that such information remains the property of the State and must be returned intact, deleted, and/or destroyed, including copies, on demand, or within ten (10) calendar days after the Proposal due date, a notice by the State of an intent not to award a Contract or upon notification by the State to return the material.

**SECTION II: APPLICANT AND RECIPIENT PERSONAL INFORMATION**

- A. **Confidentiality Agreement** - The prospective Proposer's Point of Contact agrees that by receiving materials from the Data Library, it is bound by the provisions of the California Welfare and Institutions Code 14100.2, to the same extent that a public officer or agency is bound in connection with the administration of the Medi-Cal program. Subdivision (a) of section 14100.2 sets forth the requirement that personal information concerning applicants and recipients be kept confidential. That subsection specifically provides as follows:

**Appendix 6.4**  
Data Library Security and Confidentiality Agreement

“Except as provided in this section and to the extent permitted by federal law or regulation, all information about applicants and recipients as provided for in subdivision (a) to be safeguarded includes, but is not limited to, names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation of personal information, and medical data, including diagnosis and past history of disease or disability”.

The prospective Proposer’s Point of Contact further understands that unauthorized disclosure of confidential information can expose it to criminal liability.

- B. The prospective Proposer and its employees, agents, and subcontractors shall protect from unauthorized disclosure names and all identifying information (such as Social Security Numbers, addresses, phone numbers, financial information [bank accounts] credit card information, etc.) concerning persons or beneficiaries either receiving services pursuant to this Agreement or persons or beneficiaries whose names or identifying information become available or are disclosed to the prospective Proposer, its employees, agents, and subcontractors as a result of services performed under this Agreement, except for statistical information not identifying any such person.
- C. The prospective Proposer, its employees, agents, and subcontractors shall use such identifying information as may be provided solely for the purpose of preparing a Proposal in response to the RFP released.
- D. The prospective Proposer shall promptly transmit to the State all requests for disclosure of such identifying information.
- E. The prospective Proposer shall not disclose, except as otherwise specifically permitted by this Agreement, any such identifying information to anyone other than the State without prior written authorization from the State.
- F. For purposes of this section, identity shall include, but not be limited to, name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.

**SECTION III: INDEMNIFICATION BY THE PROSPECTIVE PROPOSER**

- A. The prospective Proposer agrees to indemnify, defend, and save harmless the State, its officers, agents, and employees:
  - 1. From any and all claims and losses if those claims and losses result from actions taken by prospective Proposer in connection with this procurement;
  - 2. From any and all claims and losses accruing or resulting to any person, firm, corporation, or other entity injured or damaged by the error, omission, or negligent act or willful misconduct (including, without limitation, failure to comply with federal and State Medi-Cal regulations) of the prospective Proposer, its officers and/or employees in connection with this procurement;
  - 3. From any and all claims and losses resulting to any person or firm injured or damaged by the prospective Proposer, its officers and/or employees by the publication, reproduction, delivery, performance, use, disclosure or disposition of any information gathered pursuant to this procurement in a manner prohibited or not authorized by this procurement, or by any federal or State laws or regulations;

**Appendix 6.4**  
Data Library Security and Confidentiality Agreement

4. From any and all claims and losses resulting from the release of Protected Health Information (PHI) and/or Personal Information (PI) in violation of the requirements of the attached Health Insurance Portability and Accountability Act (HIPAA) Business Associate Addendum (BAA) (Data Library) if those claims and losses result from actions taken by prospective Proposer in connection with this procurement; and
5. Notify DHCS immediately should any PHI and/or PI be discovered during review of the Data Library material.

**SECTION IV: OTHER PROVISIONS**

- A. The prospective Proposer' Point of Contact shall return all Data Library materials, including updates provided by the State, and any copies thereof, within ten (10) calendar days after the Proposal due date, a notice by the State of intent not to award a Contract, or upon notification by the State to return the material. These requirements also apply to prospective Proposers who ultimately do not submit a Proposal, and the prospective Proposer's agents and subcontractors. A failure to return such materials shall be deemed a breach of this Agreement.
- B. By the signatures below, the Officer and prospective Proposer's Point of Contact acknowledge and agree to observe the terms and conditions of this Agreement.

**Complete the prospective Proposer information below.**

Name of Firm		
Address		
City	State	Zip
Prospective Proposer's Point of Contact <i>(print)</i>		
Signature <i>(original signature required)</i>		
Title		
Email	Phone	Fax
Official's Name <i>(print) (Person authorized to bind the prospective Proposer to all provisions in this Appendix)</i>		
Official's Signature <i>(original signature required)</i>		

**Appendix 6.5**  
Data Library CD/DVD Return and Media Destruction Agreement

**Access to the Data Library**

The **person authorized to legally bind the prospective Proposer to this Appendix** must agree to the provisions described in this Appendix entitled “Data Library CD/DVD Return and Media Destruction Agreement”. The prospective Proposer confirms understanding and acceptance of this policy by signing and returning the original completed and signed page 2 of this Appendix along with completed and signed Data Library Appendices 6.2, 6.3 and 6.4 when requesting the Data Library materials.

**Return of the Data Library CD/DVDs**

Under separate cover from the Narrative Proposal and Cost Proposal, the prospective Proposer must return to DHCS within ten (10) calendar days after the Proposal due date, a notice by the State of an intent not to award a Contract, or upon notification by the State to return the materials the following:

- 1) A copy of the original completed and signed page 2 of Appendix 6.5, “Data Library CD/DVD Return and Media Destruction Agreement”.
- 2) All CD/DVDs containing the Data Library material, including all updated discs, supplied to the prospective Proposer by DHCS.

Return discs and Appendix 6.5, copy of page 2, as follows to:

<b>Hand Delivery or Overnight Express:</b>	<b>United State Postal Service Mail:</b>
<p><b>Request for Data Library Discs RFP 13-90271</b> Department of Health Care Services Office of Medi-Cal-Procurement Mail Station 4200 1501 Capitol Avenue, Suite 71.3041 Sacramento, CA 95814</p>	<p><b>Request for Data Library Discs RFP 13-90271</b> Department of Health Care Services Office of Medi-Cal Procurement Mail Station 4200 P.O. Box 997413 Sacramento, CA 95899-7413</p>

**Data Library Media Destruction**

**All** DHCS Data Library material copied to other media must be returned to DHCS, deleted, and/or destroyed by the prospective Proposer, its agents and subcontractors. The prospective Proposer’s Point of Contact, on behalf of the prospective Proposer, its agents and subcontractors, shall notify DHCS that all Data Library material copied to other media has been deleted and/or destroyed by sending a confirmation notice to the following email address:

<b>Email:</b>
Send to: <a href="mailto:omcprfp2@dhcs.ca.gov">omcprfp2@dhcs.ca.gov</a>
Subject: Data Library Media Destruction RFP 13-90271

Include the following information in the confirmation email:

- Name of Firm
- Prospective Proposer’s Point of Contact Name, Title, Address, E-mail and Phone Number

**Appendix 6.5**  
Data Library CD/DVD Return and Media Destruction Agreement

- Prospective Proposer's agents and subcontractors' Names, Addresses, Email addresses and Phone Numbers given access to the Data Library material
- Description of deleted and/or destroyed Data Library material including, but not limited to:
  - All discs and other electronic media copied to other media by the prospective Proposer, its agents and subcontractors
  - All hard copies of Data Library material printed by the prospective Proposer, its agents and subcontractors
  - All Data Library material saved to computer network and/or hard drive by the prospective Proposer, its agents and subcontractors

My firm, its agents and subcontractors agree to return to DHCS all Data Library materials that DHCS supplied on CD/DVD, as well as return and/or destroy all Data Library material copied to other media.

Name of Firm \_\_\_\_\_

Print Prospective Proposer's Point of Contact

Name \_\_\_\_\_

Prospective Proposer's Point of Contact Signature \_\_\_\_\_  
(Original signature required)

Date \_\_\_\_\_

Print Official's Name \_\_\_\_\_

Official's Signature \_\_\_\_\_ Date \_\_\_\_\_  
(Original signature required) (Person authorized to legally bind the prospective Proposer to the provisions of this Appendix)



**FOR OMCP USE**

Date CD/DVDs received with copy of Appendix 6.5: _____
Received: Y N CD/DVD's Data Library material Number released by DHCS _____ Number returned _____
Updated CD/DVDs supplied by DHCS: Number released by DHCS _____ Number returned _____
Date Data Library Media Destruction email received by DHCS: _____
Signed _____ (OMCP Official)