California Association of Health and Education Linked Professions
Joint Powers Authority (CAHELP JPA)
DESERT/MOUNTAIN SELPA STEERING and FINANCE COMMITTEE MEETING
September 24, 2021 – 9:00 a.m. Virtual via Videoconference
Desert Mountain Educational Service Center, 17800 Highway 18, Apple Valley CA 92307

AGENDA

NOTICE: This meeting will be held virtually only. If members of the public wish to participate in the meeting and/or make public comment, please follow the instructions below to participate telephonically:

PARTICIPATE BY PHONE:
Dial Access Number: 1-415-655-0003
When prompted - enter Access Code: 2453 632 0258
Follow directions as a Participant; an Attendee I.D. is not required to participate.

If you wish to make a public comment at this meeting, prior to the meeting please submit a request to address the Steering and Finance Committee to the recording secretary via fax at 1-760-242-5363 or email jamie.adkins@cahelp.org. Please include your name, contact information and which item you want to address.

Reasonable Accommodation: if you wish to request reasonable accommodation to participate in the meeting telephonically, please contact the recording secretary (via contact information noted above) at least 48 hours prior to the meeting.

1.0 CALL TO ORDER

2.0 ROLL CALL

3.0 PUBLIC PARTICIPATION

The public is encouraged to participate in the deliberation of the Desert/Mountain SELPA Steering and Finance Committee. Several opportunities are available during the meeting for the Council to receive oral communication regarding the presentations of any items listed on the agenda. Please ask for recognition either before a presentation or after the presentation has been completed. Please complete and submit a "Registration Card to Address the Desert/Mountain SELPA Steering Committee" to the Recording Secretary and adhere to the provisions described therein.

4.0 ADOPTION OF THE AGENDA

4.1 **BE IT RESOLVED** that the September 24, 2021 Desert/Mountain SELPA Steering and Finance Committee Meeting Agenda be approved as presented.

5.0 PRESENTATIONS

5.1 SBCSS D/M Operations Final 2020-21 Local Control Funding Formula (LCFF) Revenue Transfer

The SBCSS D/M Operations Fiscal Year 2020-21 LCFF Revenue Transfer will be presented by the San Bernardino County Superintendent of Schools (SBCSS) Internal Business Program Manager.

5.2 SBCSS D/M Operations 2020-21 Fee-For-Service Year-End Actuals

The SBCSS D/M Operations Fiscal Year 2020-21 Fee-For-Service Year-End Actuals will be presented by the SBCSS Internal Business Program Manager.

5.3 SBCSS D/M Operations 2020-21 Fee-for-Service Return

The SBCSS D/M Operations 2020-21 Fee-For-Service Return will be presented by the SBCSS Internal Business Program Manager.

6.0 INFORMATION/ACTION

6.1 Desert/Mountain Children’s Center Electronic Health Record Policy (**ACTION)**

Policies and procedures governing the operation of special education programs within the Desert/Mountain SELPA are developed, reviewed and revised throughout the year upon the recommendation of the Program Team. Policies and Procedures are modified as necessary in order to ensure that special education programs are operated in an efficient, effective and legally compliant manner. Suggested revisions to SELPA Policy and Procedures are submitted to the D/M SELPA Steering Committee consideration and approval.

6.1.1 **BE IT RESOLVED** that the Desert/Mountain Children’s Center Electronic Health Record Policy be approved as presented.

7.0 CONSENT ITEMS

It is recommended that the Steering and Finance Committee consider approving several Agenda items as a Consent list. Consent Items are routine in nature and can be enacted in one motion without further discussion. Consent items may be called up by any Committee Member at the meeting for clarification, discussion, or change.

7.1 **BE IT RESOLVED** that the following Consent Items be approved as presented:

7.1.1 Approve the August 27, 2021 Desert/Mountain SELPA Steering and Finance Committee Meeting Minutes.

8.0 CHIEF EXECUTIVE OFFICER AND STAFF REPORTS

8.1 State SELPA Legislative Update

Jenae Holtz will present the State SELPA Legislative Update.

8.2 COVID Decision Tree

Jenae Holtz will a COVID decision tree.

8.3 Learning Recovery Support and Alternative Dispute/Prevention/Resolution Grants

Jenae Holtz will present information on Learning Recovery Support and Alternative Dispute/Prevention/Resolution Grants.

8.4 Desert/Mountain Children's Center Client Services Reports and Updates

Linda Llamas will present the D/M Children's Center Client Services monthly reports and updates.

8.5 Professional Learning Summary and Update

Heidi Chavez will present the D/M SELPA's Professional Learning Summary and update.

8.6 Resolution Support Services Summary

Kathleen Peters will present the D/M SELPA's Resolution Support Services Summary.

8.7 Prevention and Intervention Updates

Kami Murphy will present Prevention and Intervention updates.

8.8 Transition Partnership Program (TPP) Beginning of the Year Meeting

Adrienne Shepherd-Myles will present the flyer for the TPP Beginning of the Year Meeting.

8.9 Compliance Update

Peggy Dunn will present an update on compliance items from the California Department of Education (CDE).

8.10 Nonpublic School/Nonpublic Agency Update

Peggy Dunn will provide a nonpublic school/nonpublic agency update.

9.0 FINANCE COMMITTEE REPORTS

10.0 INFORMATION ITEMS

10.1 Monthly Occupational & Physical Therapy Services Reports

10.2 Monthly Nonpublic School/Agency Placement Report

10.3 Upcoming Professional Learning Opportunities

11.0 STEERING COMMITTEE MEMBERS COMMENTS / REPORTS

12.0 CEO COMMENTS

13.0 MATTERS BROUGHT BY THE PUBLIC

This is the time during the agenda when the Desert/Mountain SELPA Steering and Finance Committee is again prepared to receive the comments of the public regarding items on this agenda or any school related special education issue.

When coming to the podium, speakers are requested to give their name and limit their remarks to three minutes.

Persons wishing to make complaints against Desert/Mountain SELPA Steering and Finance Committee personnel must have filed an appropriate complaint form prior to the meeting.

When the Desert/Mountain SELPA Steering and Finance Committee goes into Closed Session, there will be no further opportunity for general public to address the Council on items under consideration.

14.0 ADJOURNMENT

The next regular meeting of the Desert/Mountain SELPA Steering and Finance Committee will be held on Friday, October 22, 2021, at 9:00 a.m., at the Desert Mountain Educational Service Center, Aster/Cactus Room, 17800 Highway 18, Apple Valley, CA 92307.

Individuals requiring special accommodations for disabilities are requested to contact Jamie Adkins at (760) 955-3555, at least seven days prior to the date of this meeting.

San Bernardino County Superintendent of Schools
DESERT MOUNTAIN COUNTY OPERATED SPECIAL EDUCATION PROGRAM

2020-21 LCFF Revenue Transfer
District Funded Students
Final Transfer

District of Residence	UPP %	Grades TK/K-3	Grades 4-6	Grades 7-8	Grades 9-12	Total
Adelanto	81.8600%	11,037.06	10,147.92	10,449.06	-	
P-2/Annual ADA		28.48	21.56	15.87	-	**65.91**
Total		**314,335.58**	**218,789.16**	**165,826.60**		**698,951.35**
Apple Valley	73.7200%	10,552.56	9,702.45	9,990.37	11,879.23	
P-2/Annual ADA		31.38	24.26	13.22	29.40	**98.26**
Total		**331,139.43**	**235,381.45**	**132,072.72**	**349,249.51**	**1,047,843.11**
Barstow	79.8000%	10,914.45	10,035.18	10,332.98	12,286.62	
P-2/Annual ADA		25.80	13.34	4.81	9.19	**53.14**
Total		**281,592.83**	**133,869.37**	**49,701.63**	**112,914.03**	**578,077.86**
Bear Valley	71.4600%	10,418.05	9,578.77	9,863.02	11,727.81	
P-2/Annual ADA		4.17	2.74	2.66	-	**9.57**
Total		**43,443.25**	**26,245.83**	**26,235.64**	**-**	**95,924.72**
Helendale	56.7700%	9,543.68	9,774.85	9,035.24	10,743.52	
P-2/Annual ADA		2.55	2.31	0.89	-	**5.75**
Total		**24,336.39**	**20,269.89**	**8,041.36**	**-**	**52,647.64**
Hesperia	73.9400%	10,565.66	9,714.49	10,002.77	11,893.98	
P-2/Annual ADA		10.17	4.76	7.67	60.47	**83.07**
Total		**107,452.74**	**46,240.97**	**76,721.24**	**719,228.71**	**949,643.67**
Lucerne	87.8600%	11,394.19	10,476.28	10,787.16	12,826.67	
P-2/Annual ADA		5.68	1.57	2.06	8.83	**18.14**
Total		**64,719.00**	**16,447.75**	**22,221.55**	**113,259.51**	**216,647.81**
Needles	76.5100%	10,718.63	9,855.14	10,147.59	12,066.18	
P-2/Annual ADA		5.57	5.43	4.00	7.05	**22.05**
Total		**59,702.75**	**53,513.39**	**40,590.35**	**85,066.54**	**238,873.04**
Oro Grande	94.4400%	11,785.84	10,836.37	-	-	
P-2/Annual ADA		1.02	0.76	-	-	**1.78**
Total		**12,021.56**	**8,235.64**	**-**	**-**	**20,257.20**
Silver Valley	57.2000%	9,569.28	8,798.38	9,059.47	10,772.33	
P-2/Annual ADA		-	-	0.94	1.75	**2.69**
Total		**-**	**-**	**8,515.90**	**18,851.58**	**27,367.48**
Snowline	70.3800%	10,353.76	9,519.67	9,802.16	11,655.44	
P-2/Annual ADA		30.33	12.63	4.10	22.91	**69.97**
Total		**314,029.63**	**120,233.38**	**40,188.87**	**267,026.17**	**741,478.04**
Trona	72.9600%	10,507.33	9,660.86	9,947.55	11,828.31	
P-2/Annual ADA		2.46	0.90	0.02	2.66	**6.04**
Total		**25,848.02**	**8,694.77**	**198.95**	**31,463.31**	**66,205.06**
Victor Elementary	86.0700%	11,287.65	10,378.32	-	-	
P-2/Annual ADA		114.86	55.78	-	-	**170.64**
Total		**1,296,499.19**	**578,902.51**	**-**	**-**	**1,875,401.70**
Victor Valley Union High	86.8700%	-	-	10,731.37	12,760.34	
P-2/Annual ADA		-	-	27.59	72.79	**100.38**
Total				**296,078.62**	**928,824.97**	**1,224,903.59**

Summary

District Number	District	Using 19/20 Hold Harmless ADA	First 50% Transfer	Final transfer
201	Adelanto	698,951.35	349,381.44	349,569.91
203	Apple Valley	1,047,843.11	525,310.47	522,532.64
208	Barstow	578,077.86	289,448.76	288,629.10
206	Bear Valley	95,924.72	47,682.86	48,241.86
224	Helendale	52,647.64	25,974.14	26,673.50
228	Hesperia	949,643.67	476,881.49	472,762.18
232	Lucerne	216,647.81	108,465.38	108,182.43
241	Needles	238,873.04	119,542.64	119,330.40
246	Oro Grande	20,257.20	10,128.60	10,128.60
252	Silver Valley	27,367.48	13,448.59	13,918.89
254	Snowline	741,478.04	370,994.78	370,483.26
255	Trona	66,205.06	33,237.54	32,967.52
257	Victor Elementary	1,875,401.70	937,898.64	937,503.06
268	Victor Valley Union High	1,224,903.59	605,280.21	619,623.38
	Total	**7,834,222.27**	**3,913,675.54**	**3,920,546.73**

FEE-FOR-SERVICE BUDGET to ACTUALS COMPARISON- 2020-21

SELPA	Desert Mountain				Budget	Actuals	+Increase/-Decrease
A. REVENUES					April 2020	September 2021	
	RS	OB	GL	FC			
1. AB602 Special Ed Funding	6500	8311	5001	0000	$ 45,133,619	$ 47,909,141	$ 2,775,522
2. Property Tax Transfer	6500	8097	5001	0000		$ 5,154,151	
3. Property Tax Transfer Adjustment between 2020-21 P-2 and Annual						$ (212,236)	
4. Federal IDEA (Local Assistance Entitlement)	3310	8181	5001	0000		$ 1,648,551	
5. Net FFS State Aid (A1-A2-A3-A4)	6500	8311	5001	0000		$ 41,318,675	
6. LCFF ADA Revenue Transfer	6500	8710	5001	0000	$ 7,947,419	$ 7,834,222	$ (113,197)
7. Federal Preschool	3315	8182	5730	0000	$ 142,099	$ 150,570	$ 8,471
8. Preschool Local Entitlement	3320	8182	5730	0000	$ 418,344	$ 412,411	$ (5,933)
9. Infant Part C	3385	8182	5710	0000	$ 37,210	$ 122,098	$ 84,888
10. Infant State Apportionment	6510	8311	5710	0000	$ 855,937	$ 855,937	$ -
11. Local Revenue	6500	8699	5001	0000	$ -	$ 4,148	$ 4,148
12. Infant Discretionary	6515	8590	5710	0000	$ 18,605	$ 119,835	$ 101,230
13. Local Revenue - Interagency Agreements	6500	8311	5001	0000	$ -	$ -	$ -
14. Other Local Revenue	6500	8699	5001	0000	$ -	$ -	$ -
15. Contrib. frm Unrestricted	6500	8981	5001	0000	$ 161,081	$ 85,230	$ (75,851)
TOTAL REVENUES					**$ 54,714,314**	**$ 57,493,592**	**$ 2,779,278**
B. EXPENDITURES							
1. SAI Services - SDC					$ 28,704,649	$ 24,483,788	$ (4,220,861)
2. Related Services - DIS					$ 8,017,793	$ 7,705,202	$ (312,591)
3. Itinerant					$ 1,769,646	$ 1,685,364	$ (84,282)
4. 1:1 Aide Services					$ 5,903,730	$ 4,925,440	$ (978,290)
5. Bus Aides					$ 222,910	$ 8,035	$ (214,875)
6. Interpreter Services					$ 1,096,271	$ 709,726	$ (386,545)
7. Preschool Assessments					$ 307,897	$ 297,076	$ (10,821)
8. Preschool Intensive Autism					$ 3,286,742	$ 2,592,648	$ (694,094)
9. Preschool SDC					$ 2,668,969	$ 2,318,021	$ (350,948)
10. Preschool Related Services - DIS					$ 1,536,105	$ 1,762,993	$ 226,888
11. Early Start					$ 1,199,604	$ 1,139,736	$ (59,868)
TOTAL EXPENDITURES					**$ 54,714,314**	**$ 47,628,030**	**$ (7,086,284)**
C. PRIOR YEAR ADJUSTMENTS							
	RS	OB	GL	FC			
1. Prior Year AB602 Revenue Funding Adjustment	6500	8319	5001	0000	$ -	$ -	$ -
2. Beginning Balance					$ -	$ -	$ -
TOTAL PRIOR YEAR ADJUSTMENTS					**$ -**	**$ -**	**$ -**
D. 2020-21 ENDING BALANCE							
1. Total Revenues (Section A)					$ 54,714,314	$ 57,493,592	$ 2,779,278
2. Plus Total Prior Year Revenue Adjustments (Section C)						$ -	$ -
3. Less Total Expenditures (Section B)					$ 54,714,314	$ 47,628,030	$ (7,086,284)
4. Plus Unused 2020-21 Reserve					$ -	$ 1,641,430	$ 1,641,430
5. 2020-21 Fee-For-Service Ending Balance					**$ 0**	**$ 11,506,991**	**$ 11,506,990**

Service Counts	Budget	Actuals	Diff
SAI Services - SDC	808	871.83	63.83
Related Services - DIS	1040	1353.59	313.59
Itinerant	263	298	35
1:1 Aide Services	94	100.17	6.17
Bus Aides	36	23.75	-12.25
Interpreters	11	7.17	-3.83
Preschool Assessments	74	42	-32
Preschool Intensive Autism	100	65.08	-34.92
Preschool SDC	110	120.17	10.17
Preschool Related Services - DIS	373	329.17	-43.83
Early Start	64	56.83	7.17

ADA	
Estimated ADA - Budget	710.13
ADA - 19/20 Hold Harmless	707.39

San Bernardino County Superintendent of Schools

Desert Mountain County Operated Special Education 2020-21 Year-End Actuals
September 2021

				SAI SERVICES > 50% SDC	RELATED SERVICES DIS	ITINERANT	1 TO 1 AIDE SERVICES	BUS AIDES	INTERPRETER SERVICES	PRESCHOOL ASSESSMENT	PRESCHOOL INTENSIVE AUTISM	PRESCHOOL SDC	PRESCHOOL RELATED SERVICES DIS	EARLY START	TOTAL
1			RATE	$ 29,063.00	$ 6,369.00	$ 5,559.00	$ 51,887.00	$ 5,115.00	$ 82,335.00	$ 3,862.00	$ 30,506.00	$ 22,520.00	$ 3,822.00		
2		**OBJECT**	**EXPENSE**												
3		1000-1999	Certificated Salaries	8,301,007	2,273,957	917,978	-	-	-	170,052	851,706	769,428	798,356	596,484	14,678,966
4		2000-2999	Classified Salaries	4,243,137	1,613,791	66,950	2,225,127	5,332	199,284	-	435,946	391,869	170,775	55,315	9,407,526
5		3000-3999	Employee Benefits	6,804,690	1,491,046	396,212	1,800,344	1,157	116,443	60,684	717,229	639,649	399,658	261,141	12,688,252
6		4000-4999	Books & Supplies	86,231	12,735	3,475	-	-	-	-	-	-	1,195	1,625	105,260
7		5000-5999	Services & Other Operating Expenditures	793,746	974,605	7,854	43,990	150	270,657	538	13,498	3,636	2,509	9,589	2,120,772
8		6000-6999	Capital Outlay	-	-	-	-	-	-	-	-	-	-	-	-
9															
10			Sub total	20,228,811	6,366,134	1,392,469	4,069,460	6,639	586,385	231,274	2,018,379	1,804,582	1,372,492	924,153	39,000,776
11			% of Total	**0.61957**	**0.19498**	**0.04265**	**0.12464**	**0.00020**	**0.01796**	**0.04262**	**0.37193**	**0.33254**	**0.25291**	N/A	
12															
13			Allocated Cost (GL 5001 & 5730; FN 2100, 2105, 2700, 8100)	2,441,363	768,312	168,054	491,133	801	70,769	43,796	382,221	341,734	259,909	131,473	5,099,566
14			Sub total 1000-5000 costs	22,670,174	7,134,446	1,560,523	4,560,593	7,440	657,154	275,070	2,400,600	2,146,316	1,632,401	1,055,626	44,100,342
15															
16		7300-7380	Indirect Cost @ 8.0%	1,813,614	570,756	124,842	364,847	595	52,572	22,006	192,048	171,705	130,592	84,110	3,527,687
17															
18			**TOTAL EXPENSE**	**24,483,788**	**7,705,202**	**1,685,364**	**4,925,440**	**8,035**	**709,726**	**297,076**	**2,592,648**	**2,318,021**	**1,762,993**	**1,139,736**	**47,628,030**
19	**RESOURCE**	**OBJECT**	**REVENUE**												
20	6500	8097	Property Tax Revenue	2,540,454	799,497	174,874	511,067	834	73,642	30,825	269,015	240,519	182,929	118,260	4,941,915
21	3310	8181	Federal Local Assistance	847,458	266,700	58,336	170,484	278	24,566	10,283	89,739	80,234	61,023	39,450	1,648,551
22	6500	8311	AB602 FFS Revenue	21,950,180	7,554,776	1,423,372	4,515,797	120,369	491,861	121,097	1,626,678	2,385,400	1,014,123	97,927	41,301,578
23			**Total FFS Revenue (Lines 20-24)**	**25,338,092**	**8,620,973**	**1,656,582**	**5,197,348**	**121,481**	**590,068**	**162,204**	**1,985,432**	**2,706,153**	**1,258,075**	**255,636**	**47,892,044**
24	**RESOURCE**	**OBJECT**	**Revenue**												
25			**LCFF Distribution (based on % of total expense of applicable program)**	**0.61957**	**0.19498**	**0.04265**	**0.12464**	**0.00020**	**0.01796**						
26	6500	8710	Local Control Funding Formula Revenue	4,853,828	1,527,530	334,118	976,452	1,593	140,701						7,834,222
27	3315	8182	Federal Preschool							6,417	56,002	50,070	38,081		150,570
28	3320	8182	Preschool Local Entitlement							17,576	153,389	137,141	104,304		412,411
29	3385	8182	Part C Early Intervention											122,098	122,098
30	6510	8311	Infant I-50 Apportionment											855,937	855,937
31	6513	8182	Federal Preschool - Backfill for RS 3315												0
32	6515	8590	Infant Discretionary											119,835	119,835
34	6512	8590	Mental Health												0
35	6535	8590	Staff Development												0
36	6500	8311	AB602 Base Revenue												0
37	6500	89XX	Contrib to Restricted (JCS TRANSFER)												0
38	6500	8699	Local	4,148											4,148
39	6500	8311	Needles (Contracted Nurse)	17,097											17,097
40	6500	8989	Contribution from Unrestricted	85,230								-	-	0	85,230
41			Beginning Balance												0
42			**TOTAL REVENUE:**	**$ 30,298,396**	**$ 10,148,503**	**$ 1,990,700**	**$ 6,173,800**	**$ 123,074**	**$ 730,769**	**$ 186,197**	**$ 2,194,823**	**$ 2,893,364**	**$ 1,400,460**	**$ 1,353,506**	**$ 57,493,592**
43															
44			***Excess Cost Per Program***	***5,814,608***	***2,443,302***	***305,335***	***1,248,359***	***115,039***	***21,042***	***(110,879)***	***(397,825)***	***575,343***	***(362,533)***	***213,770***	***9,865,563***
45															
46			**Number of Services - Final**	**871.83**	**1,353.59**	**298.00**	**100.17**	**23.75**	**7.17**	**42.00**	**65.08**	**120.17**	**329.17**	**56.83**	
47			**2020-21 Fee-For-Service Rates**	**$ 29,063**	**$ 6,369**	**$ 5,559**	**$ 51,887**	**$ 5,115**	**$ 82,335**	**$ 3,862**	**$ 30,506**	**$ 22,520**	**$ 3,822**	**4,498**	
48			**Total 2020-21 Fee-For-Service Revenue**	**$ 25,338,092**	**$ 8,620,973**	**$ 1,656,582**	**$ 5,197,348**	**$ 121,481**	**$ 590,068**	**$ 162,204**	**$ 1,985,432**	**$ 2,706,153**	**$ 1,258,075**	**$ 255,636**	**$ 47,892,045**
49															

	SUMMARY	
50		
51	2020-21 Total Revenue	$ 57,493,592
52	2020-21 Total Expense	$ 47,628,030
53	**Subtotal**	**$ 9,865,562**
55	**Net Estimated FFS Ending Balance**	**$ 9,865,562**
56	2020-21 Unused Reserve	1,641,430
57	**Total Ending Balance**	**$ 11,506,991**

8/10/2021

San Bernardino County Superintendent of Schools
Desert Mountain County Operated Special Education Program
2020-21 Fee-For-Service Return

District	SAI Services	% of Services	Total Return	Related Services DIS	% of Services	Total Return	Itinerant	% of Services	Total Return	1:1 Aides	% of Services	Total Return	Bus Aides	% of Services	Total Return
			$ 5,814,608			$ 2,443,302			$ 305,335			$ 1,248,359			$ 115,039
Academy for Academic Excellence	0.00	0%	$ -	0.00	0%	$ -	1.17	0%	$ 1,265	0.00	0%	$ -	0.00	0%	$ -
Norton Science and Language	0.00	0%	$ -	0.25	0%	$ 540	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -
Adelanto Elementary	82.25	10%	$ 600,947	155.75	14%	$ 336,188	24.17	9%	$ 26,124	10.75	11%	$ 138,821	1.42	6%	$ 6,878
Apple Valley Unified	114.83	14%	$ 838,987	140.92	12%	$ 304,177	31.75	11%	$ 34,316	17.33	18%	$ 223,793	4.83	20%	$ 23,395
Baker Valley Unified*															
Barstow Unified	66.75	8%	$ 487,698	65.00	6%	$ 140,303	22.42	8%	$ 24,232	2.00	2%	$ 25,827	0.25	1%	$ 1,211
Bear Valley Unified	16.92	2%	$ 123,623	32.67	3%	$ 70,519	4.08	1%	$ 4,410	2.17	2%	$ 28,023	0.00	0%	$ -
Excelsior	0.00	0%	$ -	0.00	0%	$ -	5.58	2%	$ 6,031	0.00	0%	$ -	0.00	0%	$ -
Helendale Elementary*															
Hesperia Unified	105.42	13%	$ 770,235	87.75	8%	$ 189,409	73.67	26%	$ 79,625	20.92	22%	$ 270,153	2.92	12%	$ 14,144
Lucerne Valley Unified*															
Needles*															
Oro Grande Elementary	4.00	1%	$ 29,225	4.84	0%	$ 10,447	6.50	2%	$ 7,025	1.00	1%	$ 12,914	0.00	0%	$ -
Silver Valley Unified	4.42	1%	$ 32,294	7.09	1%	$ 15,304	3.83	1%	$ 4,140	0.00	0%	$ -	0.00	0%	$ -
Snowline Jt. Unified	90.58	11%	$ 661,809	129.50	11%	$ 279,527	25.83	9%	$ 27,918	7.25	7%	$ 93,624	1.00	4%	$ 4,844
Trona Jt. Unified*															
Victor Elementary	181.58	23%	$ 1,326,686	260.33	23%	$ 561,925	28.25	10%	$ 30,534	9.83	10%	$ 126,941	0.00	0%	$ -
Victor Valley Union High	129.08	16%	$ 943,103	247.84	22%	$ 534,961	54.25	19%	$ 58,635	25.42	26%	$ 328,264	13.33	56%	$ 64,567
Encore - Hesperia	0.00	0%	$ -	0.00	0%	$ -	1.00	0%	$ 1,081	0.00	0%	$ -	0.00	0%	$ -
Total	**795.83**	**100%**	**$ 5,814,608**	**1131.94**	**100%**	**$ 2,443,302**	**282.50**	**100%**	**$ 305,335**	**96.67**	**100%**	**$ 1,248,359**	**23.75**	**100%**	**$ 115,039**

District	Interpreters	% of Services	Total Return	Preschool SDC	% of Services	Total Return	Preschool Related Services	% of Services	Total Return	Preschool Intensive Autism	% of Services	Total Return	Preschool Assessment	% of Services	Total Return	Early Start	% of Services	Total Return	Grand Total
			$ 21,042			$ 575,343			$ (362,533)			$ (397,825)			($110,879)			$ 213,770	$ 9,865,563
Academy for Academic Excellence	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 1,265
Norton Science and Language	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 540
Adelanto Elementary	0.00	0%	$ -	20.33	17%	$ 98,707	83.75	27%	$ (96,692)	18.25	29%	$ (115,684)	26.00	68%	($75,864)	7.00	13%	$ 26,841	$ 946,266
Apple Valley Unified	2.00	28%	$ 5,870	6.83	6%	$ 33,161	59.50	19%	$ (68,694)	16.42	26%	$ (104,083)	0.00	0%	$0	8.33	15%	$ 31,941	$ 1,322,863
Baker Valley Unified*													0.00	0%	$0				$ -
Barstow Unified	1.17	16%	$ 3,434	9.50	8%	$ 46,125	38.92	12%	$ (44,934)	6.17	10%	$ (39,111)	12.00	32%	($35,014)	8.42	15%	$ 32,286	$ 642,057
Bear Valley Unified	0.00	0%	$ -	4.33	4%	$ 21,023	7.75	2%	$ (8,948)	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 238,650
Excelsior	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 6,031
Helendale Elementary*													0.00	0%	$0				$ -
Hesperia Unified	0.00	0%	$ -	29.67	25%	$ 144,054	42.08	13%	$ (48,582)	0.17	0%	$ (1,078)	0.00	0%	$0	9.17	16%	$ 35,162	$ 1,453,122
Lucerne Valley Unified*													0.00	0%	$0				$ -
Needles*													0.00	0%	$0				$ -
Oro Grande Elementary	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 59,612
Silver Valley Unified	0.00	0%	$ -	0.25	0%	$ 1,214	1.67	1%	$ (1,928)	1.58	3%	$ (10,015)	0.00	0%	$0	2.17	4%	$ 8,321	$ 49,329
Snowline Jt. Unified	0.00	0%	$ -	11.17	9%	$ 54,233	18.17	6%	$ (20,978)	0.25	0%	$ (1,585)	0.00	0%	$0	5.33	10%	$ 20,438	$ 1,119,829
Trona Jt. Unified*													0.00	0%	$0				$ -
Victor Elementary	0.00	0%	$ -	36.42	31%	$ 176,827	62.17	20%	$ (71,777)	19.92	32%	$ (126,269)	0.00	0%	$0	15.33	27%	$ 58,782	$ 2,083,649
Victor Valley Union High	4.00	56%	$ 11,739	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 1,941,270
Encore - Hesperia	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$ -	0.00	0%	$0	0.00	0%	$ -	$ 1,081
Total	**7.17**	**100%**	**$ 21,042**	**118.50**	**100%**	**$ 575,343**	**314.01**	**100%**	**$ (362,533)**	**62.76**	**100%**	**$ (397,825)**	**38.00**	**100%**	**($110,879)**	**55.75**	**100%**	**$ 213,770**	**$ 9,865,563**

***Districts receiving small school district protection are not included in the current year calculated return. Service counts have been removed for these districts and funds are reallocated to the remaining districts.**

	Col. A	Col. B	Col. C	Col. D	Col. E
District	**Unused 20/21 Reserve**	**20/21 FFS Ending Balance**	**20/21 Total Ending Balance**	***21/22 3% Reserve $1,675,863***	***Balance to Return $9,831,130***
Academy for Academic Excellence	$ -	$ 1,265	$ 1,265	$ 181	$ 1,084
Norton Science & Language	$ -	$ 540	$ 540	$ 77	$ 463
Adelanto Elementary	$ 163,415	$ 946,266	$ 1,109,681	$ 159,213	$ 950,468
Apple Valley Unified	$ 262,469	$ 1,322,863	$ 1,585,332	$ 227,458	$ 1,357,874
Baker Valley Unified*	$ -	$ -	$ -	$ -	$ -
Barstow Unified	$ 55,643	$ 642,057	$ 697,700	$ 100,104	$ 597,596
Bear Valley Unified	$ 23,707	$ 238,650	$ 262,357	$ 37,642	$ 224,715
Excelsior	$ 1,627	$ 6,031	$ 7,658	$ 1,099	$ 6,559
Helendale Elementary*	$ -	$ -	$ -	$ -	$ -
Hesperia Unified	$ 254,910	$ 1,453,122	$ 1,708,032	$ 245,063	$ 1,462,969
Lucerne Valley Unified*	$ 12,210	$ -	$ 12,210	$ 12,210	$ -
Needles*	$ -	$ -	$ -	$ -	$ -
Oro Grande Elementary	$ 9,907	$ 59,612	$ 69,519	$ 9,974	$ 59,545
Silver Valley Unified	$ 4,727	$ 49,329	$ 54,056	$ 7,756	$ 46,300
Snowline Jt. Unified	$ 152,737	$ 1,119,829	$ 1,272,566	$ 182,584	$ 1,089,982
Trona Jt. Unified*	$ 16,836	$ -	$ 16,836	$ 16,836	$ -
Victor Elementary	$ 321,535	$ 2,083,649	$ 2,405,184	$ 345,088	$ 2,060,096
Victor Valley Union High	$ 361,706	$ 1,941,270	$ 2,302,976	$ 330,423	$ 1,972,553
Encore - Hesperia	$ -	$ 1,081	$ 1,081	$ 155	$ 926
Total	**$ 1,641,430**	**$ 9,865,563**	**$ 11,506,992**	**$ 1,675,863**	**$ 9,831,130**

8/10/2021

Introduction

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was designed to accomplish a number of objectives, one of which is to protect the privacy of individually identifiable health information. Protection standards exist for protected health information (PHI) in all forms, including electronic formats (ePHI).

The standards set forth by HIPAA apply to "covered entities," including health care providers and the agencies they work within. The Desert/Mountain Children's Center (DMCC) is a covered entity and is thus required to comply with the regulations specified by HIPAA. This manual details the policies and procedures established for the DMCC to ensure HIPAA compliance.

HIPAA Privacy and Security Plan

The HIPAA Act of 1996 and its implementing regulations restrict DMCC's abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information is information that is created or received by the DMCC and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Participant's chart record number
- Participant's demographic information (i.e., address, telephone number)
- Information clinicians, psychologists, and other health care providers put in a participant's clinical record
- Images of the participant
- Conversations a provider has about a participant's care or treatment with other staff
- Information about a participant in a provider's computer system or a health insurer's computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is DMCC's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with HIPAA Policies and Procedures (See Appendix A). For purposes of this plan and DMCC's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, student interns, board members, and other persons whose work performance is under the direct control of DMCC, whether or not they are paid by DMCC. The term "employee" or "staff member" includes all of these types of workers.

No third party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. DMCC reserves the right to amend or change this plan at any time without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation a staff member is found to have violated the organization's HIPAA privacy and information security policies, then the staff member will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

E-PHI

The federal HIPAA's Security Regulation requires mental health and other small health care practices to meet administrative, physical, and technical standards to protect the confidentiality, integrity, and accessibility of their Protected Health Information (ePHI). The Regulation is in large part intended to prevent computer hacking, identity theft-related crime, and similar issues posed by the use of electronic information technology in health care practices and to create a general "culture of security" in those practices.

The federal Health Information Technology for Economic and Clinical Health (HITECH) Act was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA) and it broadens the privacy and security protections under HIPAA. Specifically, HITECH requires covered entities to notify affected individuals and the Secretary of Health and Human Services (HHS) in the event of a breach of their "unsecured PHI". Many state laws impose similar or overlapping obligations on businesses.

Another significant change brought about by HITECH is that a covered entity's "business associates" (and their subcontractors) are now directly subject to HIPAA's Security Regulation. HITECH also broadened, (and in some cases, narrowed) the definition of "business associate". Thus, a practice's security program should require the practice to keep a closer eye on its business associate relationships, as discussed in greater detail below.

The HIPAA Final Rule released on January 17, 2013, amended HIPAA's privacy and security rules to implement the foregoing HITECH requirements. The definition of what constitutes a "breach" of PHI was also broadened by the Final Rule, which now requires a practice to "presume" that any non-permitted acquisition, access, use or disclosure of PHI is a breach under HIPAA requiring notification to affected individuals and HHS in accordance with HIPAA regulations. In determining whether a covered entity can overcome the presumption of a breach, the Final Rule requires covered entities to undergo a "risk assessment" based on several factors to determine whether there was a low probability that the PHI was compromised by the non-permitted acquisition, access, use or disclosure. The Final Rule also increased civil money penalties payable to HHS for uncorrected violations and willful neglect of HIPAA requirements.

HITECH and the Final Rule made few changes to the technical standards of the Security Regulation and a full analysis of HITECH and the Final Rule is therefore beyond the scope of this Manual. Nevertheless, in implementing and maintaining a security program, practices should be aware of the changes summarized above. Now more than ever, HHS is bringing enforcement actions against providers and business associates for breaches of unsecured PHI. Given this heightened enforcement environment and the broadening of the privacy and security rules under HITECH and the Final Rule, practices are well advised to increase their focus and involvement in maintaining a strong security program consistent with the Security Regulation.

The Security Regulation applies only to electronic data used, transmitted, or maintained by the practice (unlike the HIPAA Privacy Regulation which covers health information on paper or in any other form). However, practitioners should remember that the Regulation's definition of electronic Protected Health Information includes demographic, health and financial information which might include name, address, social security number, credit card numbers, insurance plan numbers, or other identifiers.

The HIPAA Security Regulation is not highly specific. The Regulation essentially requires health care practices to take ***reasonable and appropriate*** measures to protect against ***reasonably anticipatable*** threats to the practice's ePHI. The Regulation sets a series of 18 standards for the protection of electronic health information and a total of 36 implementation specifications to help health care providers address what needs to be done to meet those standards. The HIPAA Security Regulation is outlined in the following pages with standards and implementation specifications.

Compliance with ***all*** standards is ***required.*** In most cases, compliance with the implementation specifications under a standard will constitute compliance with the standard. Implementation specifications are divided into ***required*** specifications that must be implemented exactly as indicated and ***addressable*** specifications which can be adapted in a manner reasonable and appropriate to the practice so as to address reasonably anticipatable risks to ePHI. However, the Centers for Medicare and Medicaid Services (CMS), the enforcement agency for the Regulation, emphasizes that "addressable" does not mean "optional". Should a practice not implement an addressable measure exactly as indicated, the practice must document alternative measures and the reason they were taken. **Compliance with all the standards and specifications must be documented.**

Section I: Descriptions and Definitions

Administrative Safeguards: Administrative safeguards refer to these policies and procedures used by the Desert/Mountain Children's Center (DMCC) to comply with HIPAA standards.

I. Security/Privacy Officer

The Director of the DMCC is the designated Security/Privacy Officer and is responsible for knowing HIPAA regulations, training the DMCC staff which includes, clinical staff (student interns, Intervention Specialists, Behavioral Health Counselor I, Behavioral Health Counselor II, Clinical Counselors and Behavioral Health Counselor Supervisors), administrative staff, and support staff (business, clerical, and student workers) in HIPAA compliance, and assuring that HIPAA related policies and procedures are instituted and followed. The Security/Privacy Officer will:

- Update HIPAA policies and procedures
- Oversee the implementation of the policies and procedures contained in this Manual
- Ensure that all clinic personnel are trained regarding HIPAA and the policies and procedures of the clinic on an annual basis
- Review activity that takes place in the clinic to detect security risks
- Investigate and respond to security incidents and take appropriate action in the event of a breach in security, and eliminate or mitigate any damaging effects.

II. Training Program

All clinic personnel are required to participate in a formal HIPAA training program. The training program was instituted at DMCC in the fall of 2007, and all existing personnel were required to complete the training. All new employees receive the training within 30 days of their employment with DMCC.

The training involves attending the HIPAA Training for covered Entities, and signing the Employee Agreement for both HIPAA and the Omnibus rules. Additionally, this Manual is available to all DMCC personnel through the web-based Live Binder. It is also available as a hard copy in the clinic office.

III. Documentation of Training

Training of DMCC personnel will be recorded in an electronic HIPAA Training Log.

IV. HIPAA Notification

All clients who receive DMCC services are given a *HIPAA Notice of Privacy Practices (NOPP)* document before their first session. They sign a document indicating they have received the Notification. Additionally, a HIPAA Notification document is posted in the waiting room of the clinic.

V. Release of Information

Client PHI is only released to another party when the release is requested, in writing, by the client or the client's legal guardian. The *Release of Health Information* form is completed when a request is made.

The exceptions to the release of PHI without a signed release of information occurs only in accordance with strict policies (i.e., harm to self and/or others).

Ensuring Disclosures are the Minimum Necessary

When a request is received to disclose PHI, the request is reviewed by a DMCC program manager. The document will clearly state what is to be released and the minimum will be disclosed. The principle guiding the release of PHI is to limit disclosure of information not reasonably necessary to accomplish the purpose for which the request is made.

Accounting for Disclosures

The DMCC support staff will identify in its database, per child any disclosures to external agencies whenever a release of information is requested by a client.

Request for File Review and Copy

Clients and/or legal guardians of clients, who have records with the DMCC may request to inspect and obtain a copy of their PHI in the "designated record set," defined as the medical and billing records maintained by the clinic and used to make decisions about the client. The request must be made in writing, and will be fulfilled within 30 days of receipt. HIPAA does not allow clients to have access to their therapist's psychotherapy notes.

Requests to Amend a Record

Clients and/or legal guardians of clients, have the right to amend their record if they believe the record is incomplete or not accurate. The amendment will become part of their ongoing file. Requests for record amendments must be made in writing. Clients may not expunge any prior information or part of the Record.

VI. Security Assessment and Reporting

The DMCC Director will engage in a yearly assessment of the clinic's adherence to the policies detailed in this manual. As part of the annual facility assessment, teams consisting of administrative staff and clinicians will be asked to conduct an assessment of any potential security problems and to recommend additional security measures.

Reporting of Security Violations

DMCC personnel are required to report any violations of HIPAA standards to the Security/Privacy Officer.

Responding to Violations and Preventing Further Violations

When security incidents or deficiencies are reported or discovered, the Security/Privacy Officer will investigate the situation and complete the *HITECH Act Breach Notification Risk Assessment Tool* (see Appendix B). The breach tool will contain any corrective measures as needed. Corrective measure may include personnel re-education, policy revision, building modification, and/or equipment alterations.

VII. Policies and Procedures to Access Protected Health Information

Access to PHI is limited to DMCC personnel and business associates and further restricted to the information needed by personnel to complete a job function and/or clinical training.

VIII. Business Associates

"Business associates" are defined by HIPAA as third parties who provide services to DMCC and may have access to electronic patient health information. The DMCC currently has business associate agreements. In the event DMCC enters into an additional arrangement with a business associate, a Business Associate Agreement will be adopted and utilized.

IX. Research Activities

Client information may not be used for research or marketing purposes unless the client has agreed to allow his/her PHI to be used in this manner. All research projects must also be approved by the CAHELP Institutional Review Board.

X. Clinic Visitors

Occasionally visitors tour the DMCC facility as they are learning to create their own programs. All visitors must be escorted by DMCC personnel who ensure PHI is not disclosed or visible.

Section II: Physical Safeguards

Physical safeguards refer to the processes in place in which DMCC controls physical access to protected information.

Building Access

Access to the DMCC, with the exception of the lobby is limited to DMCC personnel who are given a key(s) to the building and are required to wear their identification badge to enter into the treatment rooms and/or administrative staff area. Keys are dispersed by the Operations Officer of the CAHELP who maintains a record of key distribution and a signed document from the employee of receipt of the key(s). Upon termination, DMCC administrative staff will collect the key(s) from the employee and return it to the Operations Officer of CAHELP.

Mailboxes

Written communication pertaining to DMCC and clinical work is distributed via personnel mailboxes housed within DMCC offices. These mailboxes are kept behind locked doors.

Session Recordings

Recordings are made of certain sessions with the permission of the client and/or guardian of the client depending on the type of treatment they are receiving (i.e., Parent-Child Interaction Therapy – PCIT, Theraplay, etc.). Recordings are digitized and maintained in a locked file. The recordings are not allowed to leave the premises. Recordings are only to be utilized for the purpose as clearly identified on the permission to record document.

Documentation

Session notes are recorded in Athena Software (Penelope) and Netsmart myEvolv, both secure electronic medical records system. Report copies may also be kept in the client files.

Document Retention

Electronic medical records on Penelope and myEvolv are maintained indefinitely in this secure medium. Any client paper files are maintained in a file cabinet that is open during business hours and locked thereafter. The room holding client files is locked after hours as well. Any files maintained are housed in locked cabinets behind two sets of locked doors when DMCC is not open for business. Paper files of terminated clients are scanned in Penelope and/or myEvolv and stored at a secured facility.

Section III: Technical Safeguards

Technical safeguards refer to the procedures in place to control access and/or interception to computer systems and to protect all communications containing PHI transmitted electronically.

Electronic Medical Records System (Penelope)

DMCC uses both Penelope and myEvolv software, electronic medical records systems designed specifically for counseling centers and psychology training clinics. Penelope and myEvolv may only be accessed by DMCC personnel, each of which has a unique user name and password. Access is restricted by safety measures in the system that restrict users from being able to view records of clients who are not their own. Once files are saved they cannot be changed or erased without a clear electronic tracking of any activity and clear identification of who accessed records. Full access to Penelope is granted only to limited staff including the administrative staff, support staff and technology personnel to maintain the program.

Computer Workstations

All computer access is secure from clients, parents and/or visitors to the DMCC. The reception area computer (which is behind glass and locked doors) is turned off each day after business hours. All DMCC personnel log off of Penelope and documents before leaving them unattended. Documents are kept, completed and maintained in Penelope through the network server and/or client hard files.

Mobile Devices

All organizationally purchased mobile devices used by the DMCC staff have a Mobile Device Management (MDM) application installed on them that allows for remote management and wiping of the device if it is lost or stolen.

Computer Flash Drive

The use of flash drives or portable electronic media to store ePHI data is prohibited.

Cloud Storage

The use of cloud storage to store ePHI is allowed when it is a DMCC approved HIPAA compliant cloud storage.

Faxing

The fax machine at DMCC is housed in a locked area of the clinic. The fax machine is checked throughout the day to ensure faxed documents are not left unattended.

If faxing, only the PHI needed is sent, and a cover letter with a confidentiality statement accompanies the information to help prevent casual reading. Additionally, frequently used fax numbers are programmed into the machine to ensure accuracy in dialing. New fax numbers are verified before PHI is transmitted. The machine does not have the capacity to save copies of faxed information.

Email

DMCC uses an encrypted email solution when emailing client PHI information to entities outside of the network. The encryption process is accomplished with software on our email gateway server. All DMCC personnel have been trained to use “Encrypt” on the subject line to ensure proper encryption. Client level information is attached with a privacy statement in the body of the email. Privacy notices on all emails is appended as part of the sending process and is enforced from the system.

Telephone

Phone calls are made to clients and/or guardians from the office area for routine appointment reminders and appointment clarification. The office area is behind locked doors and a glass partition. All information occurs away from all clients, guardians, and visitors.

Electronic Health Records Policy and Procedures

Electronic Health Records (EHR) complies with HIPAA, and all state and federal laws related to protection of personal health information. EHRs can be encrypted (making the document(s) unreadable to anyone other than an authorized user) and security access parameters set to only authorized individuals can view them. EHRs also offer the added security of an electronic tracking system that provides an accounting of the history of when records have been accessed and by whom.

General Information

System users who send, receive, store and access ePHI must comply with DMCC's Electronic Health Records Policy and Procedures.

I. Policy

DMCC provides physical attributes required to protect information systems and related infrastructure from unauthorized access in accordance with HIPAA Security Rules to protect the availability, confidentiality, and integrity of client and departmental confidential information.

DMCC personnel are responsible for maintaining the physical security of DMCC's computer resources under their control. They are also responsible for protecting the integrity and privacy of the data maintained on the computer by using appropriate lockdown devices, password controlled access, data encryption, virus protection software, and routine backup procedures.

DMCC is under the umbrella of the California Association of Health and Education Linked Professions (CAHELP), which is a department of San Bernardino County Superintendent of Schools (SBCSS). SBCSS, CAHELP, and DMCC reserve the right to inspect all data and to monitor the use of all its computer systems.

All computer users have no right to privacy with regard to information on organizationally supplied computers. Personnel are not allowed to place any client information (ePHI) on personally owned technology devices. The organization reserves the right to remotely access, monitor, control, and configure organizationally-supplied computers and any software residing on said device. Non-compliance with this policy is subject to management review and action up to and including termination of employment, vendor contract, and/or legal action.

- All computers are equipped with updated software for detecting the presence of malicious software (i.e., computer viruses). All computing devices have current versions of anti-virus software enabled. Operating systems have all critical updates installed.
- All computers are positioned or located in a manner that minimizes the exposure of displayed patient and/or sensitive business information.

- DMCC personnel accessing the DMCC network or information from remote locations are trained to utilize appropriate security safeguards.
- DMCC through the CAHELP and with SBCSS's direction and approval shall have the in ability to recommend and implement hardware, operating systems, and connectivity solutions to be supported. System support of any proposed solutions will need to be included in the purchasing decision.
- DMCC personnel may not independently install hardware or software solutions that allow remote access to organizationally-purchased devices.
- DMCC personnel must comply with DMCC's policies and state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

II. PURPOSE

The DMCC is committed and required to provide security to protect its computerized clinical and business information systems. DMCC computer system hardware and software as well as the information and data carried by the system are the property of the CAHELP/SBCSS. Any misuse of DMCC computers may result in denial of access to the system network and systems, DMCC information, and data. The intent of this policy is to:

- Ensure each system containing ePHI has the necessary access controls to restrict unauthorized users and programs from accessing patient health or sensitive business information.
- Ensure software on each computer on the network is internally compatible and will not lead to degradation of the system.
- Ensure users are oriented and trained on computer use and maintenance of information integrity, privacy, and resource security.
- Establish security requirements for the appropriate use of mobile computing resources including laptops and mobile computing devices that access DMCC information or interface with the DMCC network.

III. SCOPE

This policy applies to all DMCC personnel, vendors, contractors, and business associates who have access to DMCC client information, either clinical and/or business related, stored on DMCC computers or have access to its computer resources or network. The scope of this policy includes the usage of all and any device that directly or remotely accesses the DMCC network.

IV. DEFINITION

Portable-Computer Device: A portable-computing device is a computer that is easily transported by hand and has the ability to store DMCC client and/or business information. "Portable computing device" generally refers to laptop computers, smart clipboards, and mobile computing devices but can include other emerging technologies that allow storage of and access to information, and are capable of connection (physical or wireless) to the computer network, including connection to any server or computer on the computer network.

V. PROCEDURES

General

1. Users are required to log-off of applications containing client health and/or sensitive business information before leaving their computers.
2. Users must save work that contains ePHI in accordance with approved data storage policies.
3. All laptops and any other portable computer equipment must be secured (protected) when not in use.
4. Storing ePHI information on ANY Device that is not encrypted is prohibited.
5. Storing of PHI information on a personal device is prohibited.
6. Employees are responsible for breaches of security related to devices in their possession.
7. All computers require a complex-level password protection with the computer system. In order to access any client health and/or business information, a second level of authentication protection is required to access information.
8. There are no circumstances when security provisions are allowed to be disabled.
9. DMCC personnel are required to have appropriate clearance prior to access to computers and the Penelope network.
10. Upon termination or change of job position, users will have network access removed or modified as deemed appropriate by administration.
11. All computer devices shall be tagged and tracked by administration in accordance with SBCSS's asset management policies and procedures.

Desktop Computers

DMCC has established standard configurations for desktop technologies deployed throughout the organization. All computers, computer peripherals, and software as well as printers, faxes, and other miscellaneous hardware purchased with DMCC funds or attached to any component of the DMCC network must meet these standards.

Installation of any personal software, whether purchased or downloaded, by employees is prohibited. Software required for end user productivity must be approved by the Director and installed by CAHELP/SBCSS helpdesk staff.

Desktop computers are located in areas that are physically separate and face away from the public.

Computer access and password training provided by the DMCC administrative staff must be completed prior to granting access privileges to ensure adequate training has occurred.

Desktop computers are equipped with security hardware and/or software. Computers **must** comply with all software updates for detecting the presence of malicious software. All devices will have current versions of anti-virus software enabled. Operating systems will have all critical updates installed.

Mobile devices that store ePHI will be secured using compliant measures.

Organizationally-Supplied Portable/Mobile Computer Devices

The loss or theft of any portable computer device storing DMCC client and/or sensitive business information shall be immediately reported to the employee's supervisor. The supervisor will contact the DMCC Security/Privacy Officer.
Startup authentication and authorization passwords (user name and password) are required on all computers. Storing or caching username and passwords on any device is prohibited.

Organizationally-supplied portable computer devices storing data belonging to the DMCC may not be shared with others, especially non-employees, who are not authorized to access the information unless the information is stored as encrypted password protected files.

DMCC reserves the right to identify sensitive information and initiate methods to secure this information.

Personally-Supplied Portable/Mobile Computer Devices

The use of personally-supplied devices by DMCC/CAHELP personnel in support of the organization's mission or work is strictly prohibited.

Remote Access

Access to DMCC's internal remote location will be done through appropriate Virtual Private Network (VPN) services and must be approved by the Security/Privacy Officer.

Access to DMCC's internal network from outside of its defined network perimeter will be controlled by VPN access controls that may only be established by technical staff.

Users are not authorized to install hardware or software solutions that would allow remote access to their organizationally-supplied computing devices.

VPN connections will be strictly controlled, implemented, and maintained by SBCSS technical staff.

VI. Staff Use of System and Privileges

Monitoring of computer use

Personnel utilizing DMCC systems should have no expectation of privacy. The DMCC will log, review, or monitor any data stored or transmitted on its information systems to manage those assets to ensure compliance with the agency's policies.

Removal of staff privileges

The DMCC may remove or deactivate any employee's network privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

System Security

Each computing device used to access, transmit, receive, or store ePHI must comply with DMCC policies. If any policy requirement is not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The system must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The computer must not be used to send, receive, or store ePHI

VII. Data Maintenance and Emergency Procedures

Server

Since 2007, private health information at the DMCC that is ePHI is maintained by an Electronic Medical Records System (Penelope). Penelope is a cloud-based system that provides for redundancy and disaster recovery solutions. The data sheet for Penelope can be found at:

http://www.athenasoftware.net/resources/Penelope_PRIVACY_AND_SECURITY_Whitepaper_2014.pdf

Since March 2020, private health information at the DMCC that is ePHI is maintained by an Electronic Medical Records System (Netsmart myEvolv). myEvolv is a cloud-based system that provides for redundancy and disaster recovery solutions. The data sheet for myEvolv can be found in Appendix D.

Technical staff are responsible to ensure all servers used to access, transmit, receive or store ePHI are appropriately secured with this policy.

1. Server Location

DMCC in-house (non-cloud) servers currently reside at a secure facility. All data not stored in the cloud solution is stored on these systems.

- Servers are located in a physically-secure environment
- The system administrator account is password protected
- A user identification and password authentication mechanism is implemented to control user access to the system
- A security patch and update procedure is established and implemented to ensure all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- Servers are located on a secure network with firewall protection
- All unused or unnecessary services are disabled

2. Computer Security

Technical staff are responsible to ensure each computer system used to access, transmit, receive, or store ePHI is appropriately secured in accordance with this policy. A user identification and password authentication mechanism is implemented to control user access to the system.

- All users must be issued a unique user name for accessing PII
- Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, within 24 hours
- Passwords are not to be shared
- Passwords must be at least eight characters and complex
- Passwords must not be cached
- Passwords must be changed every 180 days.
- Passwords must be changed if revealed or compromised.
- 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)
- A security patch and update procedure is established and implemented to ensure all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected: All computers and devices that process and/or store PII must have critical security patches applied including those patches that require a system reboot. The patch management process determines installation timeframe based on risk assessment and vendor recommendations. All applicable patches deemed as high risk must be installed as soon as practical. Applications and systems unable to be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

- A malware detection system is implemented including a procedure to ensure the detection software is maintained and up-to-date
- All unused or unnecessary services are disabled
- An automatic logoff or inactivity timeout mechanism is implemented
- The computer screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen may be used
- Laptop devices will have hardware level disk encryption
- **Data Destruction:** When an electronic storage device that contains PII is sent for destruction, it is erased using the US Department of Defense clearing and sanitizing standard DoD 5220.22-M or equivalent
- **System Timeout:** The system providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 30 minutes of activity
- **System Logging:** The system maintains an automated audit trail that can identify the user or system process, initiates a request for PII, or alters PII. 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 PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence
- **Access Controls:** The system providing access to PII must use role based access controls for all user authentications, enforcing the principle of least privilege
- **Transmission Encryption:** All data transmission of PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email
- **Intrusion Detection:** All systems involved in accessing, holding, transporting, and protecting PII, which are accessible through the Internet, must be protected by a comprehensive intrusion detection and prevention solution

3. Logoff Procedures

To ensure security to all servers and computers accessing, transmitting, receiving, and/or ePHI, the following procedures must be followed:

Automatic Logoff Procedures

- Servers, computers and other electronic devices containing ePHI must employ inactivity timers or automatic logoff mechanisms
- Servers, computers and other electronic devices containing ePHI must terminate a user session after a maximum of, but not limited to, 30 minutes of inactivity

- When a system requires the use of an inactivity timer or automatic logoff mechanism but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
  - The system must be upgraded to support the minimum HIPAA Security
  - The system must be moved into a secure environment
  - ePHI must be removed and relocated to a system supporting the minimum requirements

Logging off the System

When a server, computer, or other electronic device is unattended users must lock or activate the systems Automatic Logoff Mechanism (e.g., CTRL, ALT, DELETE and Lock computer), or logout of all applications and database systems containing confidential information.

Network and Privacy Settings

Schedule for Backups

Backups are scheduled nightly and are encrypted to offsite, encrypted storage. Backups are maintained for a two-week period.

Recovery Plan for Data

On premises servers are backed up regularly using VM-level backups. Servers and data can restore all data necessary to the version from the night before. There is also a database-level backup of Penelope data that is performed daily. Details for back and recovery for clouds servers can be found in (See Appendix C).

Security Protocols for Access to Data

Password resets are in effect every 180 days for all users.

Encryption security level

- Computers and server storage is encrypted where necessary
- Intra site communication is direct and secure so no special encryption is necessary.

Firewalls

The DMCC has firewalls installed at internet connection points at the primary datacenter and disaster recovery datacenter. Firewalls are maintained and patched by a firewall vendor. Inbound access is analyzed using an IPS/IDS, Intrusion Prevention Systems and Intrusion Detection system, device which scans all inbound and outbound traffic for malicious attacks. Both datacenters are secured and access is controlled with the use of a key card access system. Only authorized personnel are permitted to access our datacenters. The primary data center power is protected using a natural gas generator and halon fire suppression system.

Remote Access

Access from outside of DMCC is available only through approved VPN secured connections with encrypted and physical security checks.

VIII. Electronically-Signed Records

For the purpose of this policy an electronically signed record is a financial, program, or medical record that (1) is required to be signed under California or Federal law, California or Federal regulation, or organizational policy or procedure, and (2) may be requested during an audit.

Standards for Electronic Signatures in Electronically Signed Records

Electronic signatures in electronically-signed records will be viewed as equivalent to a manual signature affixed by hand for financial, program, and medical records for audit purposes as defined under the California Code of Regulations, Title 9.

DMCC's policy for electronic signature meets the following requirements:

1. DMCC's computer system (Penelope and myEvolv) utilizes electronic signatures that comply with the following Certification Commission for Healthcare Information Technology (CCHIT) certification criteria or equivalent: *Security: Access Control, Security: Audit, and Security: Authentication.*
2. The electronic signature mechanism is (a) unique to the signer, (b) under the signer's sole control, (c) capable of being verified, and (d) linked to the data so that, if the data are changed, the signature is invalidated. Additionally, DMCC will maintain physical signatures for all clinical staff on file as backup.
3. DMCC will maintain an Electronic Signature Agreement for the terms of use of an electronic signature signed by both the individual requesting electronic signature authorization and the county mental health director or his/her designee.
4. DMCC will request and maintain an Electronic Signature Certification from entities where contracts are held through the Department of Behavioral Health where such is required.
5. The signed *Electronic Signature Certification* and signed *Electronic Signature Agreements* forms will be available to the auditor at the time of an audit.

Information Security Considerations

DMCC's standard encryption of data is also employed in the electronically-signed record.

Obtaining Consumer Signatures

In many situations, the mental health consumer, or his/her representative, must acknowledge his/her willingness to participate in and accept the treatment plan. In paper-based systems, the consumer, or his/her representative, physically signs a document to that effect. As an alternative to paper, it is DMCC's policy the following approaches will be utilized: (1) scanning paper consent documents, treatment plans, or other medical record documents containing consumer signatures or (2) capturing signature images from a signature pad.

DMCC will maintain all information and will be in full compliance with all applicable HIPAA electronic signature standards. Upon future publication of HIPAA electronic signature regulations, the DMCC will be in full compliance within the timelines and all requirements established by state and federal government.

Requirements for Electronically-Signed Records

The DMCC will utilize electronic records and electronically-signed records to replace all paper-based records for purposes of an audit. When an audit is conducted, the DMCC shall make available the following upon arrival of the auditor at the audit site:

- Physical access to electronic health record systems
- Adequate computer access to the electronic health records needed for the audit review
- System or network access to electronic records such as user IDs and passwords
- Access to printers and capability to print necessary documents
- Technical assistance as requested
- Scanned documents, if needed, which are readable and complete

PHI – Personal Health Information

PHI and PII Use and Disclosure

PHI Definition and Data Elements

Below is an excerpt from the U.S. Department of Health & Human Services defining PHI and PHI data elements:

Protected Health Information: The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information *protected health information* (PHI).

Individually identifiable health information is information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- The individual's identity or for which there is a reasonable basis to believe it can be used to identify the individual

Individually identifiable health information includes many common identifiers (i.e., name, address, birth date, Social Security Number) and generally encompasses all PII (see below). All PHI is protected by both HIPAA and ethical standards.

PII Definition and Data Elements

Per the Executive Office of the President, Office of Management and Budget (OMB) and the U.S. Department of Commerce, Office of the Chief Information Officer, The term *personally identifiable information* refers to information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Any information that is personal is protected by privacy laws.

California Senate Bill SB 1386: *personal information* means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social Security Number
2. Driver's license number or California Identification Care number
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

Use and Disclosure Defined

The DMCC will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use* – The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the company, or by a business associate of the company
- *Disclosure* – for information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within DMCC with a business "need to know" PHI

Access to PHI is Limited to Certain Employees

All personnel who perform Participant functions directly on behalf of the DMCC or on behalf of group health plans will have access to PHI as determined by their supervisor, job description, and as granted by IT. These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed is limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Personnel may not access either through the information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members, or other individuals for personal or other non-work-related purposes, even if written or oral participant authorization has been given. If the employee is a participant in DMCC's plans, the employee must go through their provider in order to request their own PHI.

In the very rare circumstance when an employee's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she will immediately report the situation to his/her supervisor who will assign a different staff member to complete the task involving the specific participant.

Personal access to your own PHI is based on the same procedures available to other participants not based on job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your provider for the information or make a written request to the Security/Privacy Officer. Employees may not access their own information; they must go through all the appropriate channels as participants are required to do.

Disclosure of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization satisfying HIPAA requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

Permissive Disclosures of PHI: For Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. DMCC's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- About victims-of-abuse, neglect or domestic violence;
- For judicial and administrative proceedings – with appropriate subpoenas;
- For law enforcement purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

Complying with the "Minimum-Necessary" Standard

HIPAA requires when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum-necessary" to accomplish the purpose of the use or disclosure. The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Labor;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

Minimum-Necessary When Disclosing PHI

For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum-necessary amount of information will be disclosed. All other disclosures must be reviewed on an individual basis with the Security/Privacy Officer to ensure the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum-Necessary When Requesting PHI

For making request for disclosure of PHI from business associates, providers, or participants for the purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Security/Privacy Officer to ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Protected Health Information (PHI): Patient information, including demographic information, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient; and
- Identifies the patient or can be used to identify a patient.

Lobby Interactions

DMCC personnel are not to reveal PHI in the lobby with clients. DMCC personnel will ask clients and/or parents to step into a confidential, private office to conduct conversations related to PHI.

Consequences of Violations

Personnel violations of DMCC systems as described above will be subject to disciplinary action that may include termination of employment.

Disclosure of PHI to Business Associates

Based on the approval of the Security/Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the company's business associates and allow the DMCC's business associates to create or receive PHI on its behalf. However, prior to doing so, the DMCC must obtain assurances from the business associate agreeing to appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of "business associate" employees must contact the Security/Privacy Officer and verify that a business associate contract is in place.

"Business associate" is an entity that:

- Performs or assists in performing a company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Disclosures of D-Identified Information

The DMCC may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual. Respect is given to the fact that there is no reasonable basis to believe the information can be used to identify an individual. There are two ways a covered entity can determine when information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers listed below – relating to the participant, employee, relatives, or employer, and being certain there is no other available information that could be used alone or in combination to identify an individual.

1. Names
2. Geographic subdivision smaller than a state
3. All elements of dates (except year) related to an individual – including dates of admission, discharge, birth, death – and for persons >89 years old, the year of birth cannot be used
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social security number
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos and comparable images
18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small regarding the information that could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. This person is required to document the methods and justification for this determination.

Disclosure to Family, Friends or Others – Participant Location

There are instances when a participant's friend or family member contacts the DMCC to ask about the location of a client or whether the client has been seen at the DMCC. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, and at the discretion of the Director of the DMCC, a minimum amount of information may be released in order to assist in resolving an emergency situation.

Guidance

Situation: Friends or family are concerned about the whereabouts of a person. They contact the DMCC and ask if a person is at the DMCC or has been seen as a client recently.

Response

For any inquiry regarding a current or past client, DMCC clinic staff should take the name of the caller, purpose for calling and state the caller will receive a return call from DMCC. DMCC staff should check if releases of information are on file. If they are on file, DMCC should make contact with the parent/client to inform them of the nature of the release of information. If parent/client agrees, DMCC will return the call and provide only the minimum information required.

If releases of information are not on file, DMCC must inform the caller that DMCC cannot confirm or deny the person is a client. If the friends and/or family are concerned about the person's wherabouts, DMCC can recommend they call other relatives of the person and/or contact the local police department to inquire about safety.

Situation: An individual comes to DMCC and tells the receptionist they have arrived to pick up a client.

Response

The DMCC serves children birth to 22 years old. Parents, guardians, or a responsible adult brining the child to treatment is expected to remain on the premises throughout the child's treatment service. In the event, the parent, guardian, or responsible adult leaves the premises, the child will contact the parent by phone. Any individual requesting information about a client will only be given information if a Release of Information is on file allowing the DMCC to share information with that specific individual.

Removing PHI from Company Premises

PHI is not allowed to leave the organization's premises at any time.

Introduction

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was designed to accomplish a number of objectives, one of which is to protect the privacy of individually identifiable health information. Protection standards exist for protected health information (PHI) in all forms, including electronic formats (ePHI).

The standards set forth by HIPAA apply to "covered entities," including health care providers and the agencies they work within. The Desert/Mountain Children's Center (DMCC) is a covered entity and is thus required to comply with the regulations specified by HIPAA. This manual details the policies and procedures established for the DMCC to ensure HIPAA compliance.

HIPAA Privacy and Security Plan

The HIPAA Act of 1996 and its implementing regulations restrict DMCC's abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information is information that is created or received by the DMCC and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Participant's chart record number
- Participant's demographic information (i.e., address, telephone number)
- Information clinicians, psychologists, and other health care providers put in a participant's clinical record
- Images of the participant
- Conversations a provider has about a participant's care or treatment with other staff
- Information about a participant in a provider's computer system or a health insurer's computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is DMCC's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with HIPAA Policies and Procedures (See Appendix A). For purposes of this plan and DMCC's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, student interns, board members, and other persons whose work performance is under the direct control of DMCC, whether or not they are paid by DMCC. The term "employee" or "staff member" includes all these types of workers.

No third-party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. DMCC reserves the right to amend or change this plan at any time without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation a staff member is found to have violated the organization's HIPAA privacy and information security policies, then the staff member will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

E-PHI

The federal HIPAA's Security Regulation requires mental health and other small health care practices to meet administrative, physical, and technical standards to protect the confidentiality, integrity, and accessibility of their Protected Health Information (ePHI). The Regulation is in large part intended to prevent computer hacking, identity theft-related crime, and similar issues posed by the use of electronic information technology in health care practices and to create a general "culture of security" in those practices.

The federal Health Information Technology for Economic and Clinical Health (HITECH) Act was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA) and it broadens the privacy and security protections under HIPAA. Specifically, HITECH requires covered entities to notify affected individuals and the Secretary of Health and Human Services (HHS) in the event of a breach of their "unsecured PHI". Many state laws impose similar or overlapping obligations on businesses.

Another significant change brought about by HITECH is that a covered entity's "business associates" (and their subcontractors) are now directly subject to HIPAA's Security Regulation. HITECH also broadened, (and in some cases, narrowed) the definition of "business associate". Thus, a practice's security program should require the practice to keep a closer eye on its business associate relationships, as discussed in greater detail below.

The HIPAA Final Rule released on January 17, 2013, amended HIPAA's privacy and security rules to implement the foregoing HITECH requirements. The definition of what constitutes a "breach" of PHI was also broadened by the Final Rule, which now requires a practice to "presume" that any non-permitted acquisition, access, use or disclosure of PHI is a breach under HIPAA requiring notification to affected individuals and HHS in accordance with HIPAA regulations. In determining whether a covered entity can overcome the presumption of a breach, the Final Rule requires covered entities to undergo a "risk assessment" based on several factors to determine whether there was a low probability that the PHI was compromised by the non-permitted acquisition, access, use or disclosure. The Final Rule also increased civil money penalties payable to HHS for uncorrected violations and willful neglect of HIPAA requirements.

HITECH and the Final Rule made few changes to the technical standards of the Security Regulation and a full analysis of HITECH and the Final Rule is therefore beyond the scope of this Manual. Nevertheless, in implementing and maintaining a security program, practices should be aware of the changes summarized above. Now more than ever, HHS is bringing enforcement actions against providers and business associates for breaches of unsecured PHI. Given this heightened enforcement environment and the broadening of the privacy and security rules under HITECH and the Final Rule, practices are well advised to increase their focus and involvement in maintaining a strong security program consistent with the Security Regulation.

The Security Regulation applies only to electronic data used, transmitted, or maintained by the practice (unlike the HIPAA Privacy Regulation which covers health information on paper or in any other form). However, practitioners should remember that the Regulation's definition of electronic Protected Health Information includes demographic, health and financial information which might include name, address, social security number, credit card numbers, insurance plan numbers, or other identifiers.

The HIPAA Security Regulation is not highly specific. The Regulation essentially requires health care practices to take ***reasonable and appropriate*** measures to protect against ***reasonably anticipatable*** threats to the practice's ePHI. The Regulation sets a series of 18 standards for the protection of electronic health information and a total of 36 implementation specifications to help health care providers address what needs to be done to meet those standards. The HIPAA Security Regulation is outlined in the following pages with standards and implementation specifications.

Compliance with ***all*** standards is ***required.*** In most cases, compliance with the implementation specifications under a standard will constitute compliance with the standard. Implementation specifications are divided into ***required*** specifications that must be implemented exactly as indicated and ***addressable*** specifications which can be adapted in a manner reasonable and appropriate to the practice so as to address reasonably anticipatable risks to ePHI. However, the Centers for Medicare and Medicaid Services (CMS), the enforcement agency for the Regulation, emphasizes that "addressable" does not mean "optional". Should a practice not implement an addressable measure exactly as indicated, the practice must document alternative measures and the reason they were taken. **Compliance with all the standards and specifications must be documented.**

Section I: Descriptions and Definitions

Administrative Safeguards: Administrative safeguards refer to these policies and procedures used by the Desert/Mountain Children's Center (DMCC) to comply with HIPAA standards.

I. Security/Privacy Officer

The Director of the DMCC is the designated Security/Privacy Officer and is responsible for knowing HIPAA regulations, training the DMCC staff which includes, clinical staff (student interns, Intervention Specialists, Behavioral Health Counselor I, Behavioral Health Counselor II, Clinical Counselors and Behavioral Health Counselor Supervisors), administrative staff, and support staff (business, clerical, and student workers) in HIPAA compliance, and assuring that HIPAA related policies and procedures are instituted and followed. The Security/Privacy Officer will:

- Update HIPAA policies and procedures
- Oversee the implementation of the policies and procedures contained in this Manual
- Ensure that all clinic personnel are trained regarding HIPAA and the policies and procedures of the clinic on an annual basis
- Review activity that takes place in the clinic to detect security risks
- Investigate and respond to security incidents and take appropriate action in the event of a breach in security and eliminate or mitigate any damaging effects.

II. Training Program

All clinic personnel are required to participate in a formal HIPAA training program. The training program was instituted at DMCC in the fall of 2007, and all existing personnel were required to complete the training. All new employees receive the training within 30 days of their employment with DMCC.

The training involves attending the HIPAA Training for covered Entities and signing the Employee Agreement for both HIPAA and the Omnibus rules. Additionally, this Manual is available to all DMCC personnel through the web-based Live Binder. It is also available as a hard copy in the clinic office.

III. Documentation of Training

Training of DMCC personnel will be recorded in an electronic HIPAA Training Log.

IV. HIPAA Notification

All clients who receive DMCC services are given a *HIPAA Notice of Privacy Practices (NOPP)* document before their first session. They sign a document indicating they have received the Notification. Additionally, a HIPAA Notification document is posted in the waiting room of the clinic.

V. Release of Information

Client PHI is only released to another party when the release is requested, in writing, by the client or the client's legal guardian. The *Release of Health Information* form is completed when a request is made.

The exceptions to the release of PHI without a signed release of information occurs only in accordance with strict policies (i.e., harm to self and/or others).

Ensuring Disclosures are the Minimum Necessary

When a request is received to disclose PHI, the request is reviewed by a DMCC program manager. The document will clearly state what is to be released and the minimum will be disclosed. The principle guiding the release of PHI is to limit disclosure of information not reasonably necessary to accomplish the purpose for which the request is made.

Accounting for Disclosures

The DMCC support staff will identify in its database, per child any disclosures to external agencies whenever a release of information is requested by a client.

Request for File Review and Copy

Clients and/or legal guardians of clients, who have records with the DMCC may request to inspect and obtain a copy of their PHI in the "designated record set," defined as the medical and billing records maintained by the clinic and used to make decisions about the client. The request must be made in writing and will be fulfilled within 30 days of receipt. HIPAA generally gives providers discretion to disclose the individual's own protected health information (including psychotherapy notes) directly to the individual or the individual's personal representative.

Deleted: HIPAA does not allow clients to have access to their therapist's psychotherapy notes.

Requests to Amend a Record

Clients and/or legal guardians of clients, have the right to amend their record if they believe the record is incomplete or not accurate. The amendment will become part of their ongoing file. Requests for record amendments must be made in writing. Clients may not expunge any prior information or part of the Record.

VI. Security Assessment and Reporting

The DMCC Director will engage in a yearly assessment of the clinic's adherence to the policies detailed in this manual. As part of the annual facility assessment, teams consisting of administrative staff and clinicians will be asked to assess any potential security problems and to recommend additional security measures.

Reporting of Security Violations

DMCC personnel are required to report any violations of HIPAA standards to the Security/Privacy Officer.

Responding to Violations and Preventing Further Violations

When security incidents or deficiencies are reported or discovered, the Security/Privacy Officer will investigate the situation and complete the *HITECH Act Breach Notification Risk Assessment Tool* (see Appendix B). The breach tool will contain any corrective measures as needed. Corrective measure may include personnel re-education, policy revision, building modification, and/or equipment alterations.

VII. Policies and Procedures to Access Protected Health Information

Access to PHI is limited to DMCC personnel and business associates and further restricted to the information needed by personnel to complete a job function and/or clinical training.

VIII. Business Associates

"Business associates" are defined by HIPAA as third parties who provide services to DMCC and involve the use or disclosure of protected health information. The DMCC currently has business associate agreements. In the event DMCC enters into an additional arrangement with a business associate, a Business Associate Agreement will be adopted and utilized.

Deleted: may have access to electronic patient health information…

IX. Research Activities

Client information may not be used for research or marketing purposes unless the client has agreed to allow his/her PHI to be used in this manner. All research projects must also be approved by the CAHELP Institutional Review Board.

X. Clinic Visitors

Occasionally visitors tour the DMCC facility as they are learning to create their own programs. All visitors must be escorted by DMCC personnel who ensure PHI is not disclosed or visible.

Section II: Physical Safeguards

Physical safeguards refer to the processes in place in which DMCC controls physical access to protected information.

Building Access

Access to the DMCC, except for the lobby is limited to DMCC personnel who are given a key(s) to the building and are required to wear their identification badge to enter the treatment rooms and/or administrative staff area. Keys are dispersed by the Operations Officer of the CAHELP who maintains a record of key distribution and a signed document from the employee of receipt of the key(s). Upon termination, DMCC administrative staff will collect the key(s) from the employee and return it to the Operations Officer of CAHELP.

Mailboxes

Written communication pertaining to DMCC and clinical work is distributed via personnel mailboxes housed within DMCC offices. These mailboxes are kept behind locked doors.

Session Recordings

Recordings are made of certain sessions with the permission of the client and/or guardian of the client depending on the type of treatment they are receiving (i.e., Parent-Child Interaction Therapy – PCIT, Theraplay, etc.). Recordings are digitized and maintained in a locked file. The recordings are not allowed to leave the premises. Recordings are only to be utilized for the purpose as clearly identified on the permission to record document.

Documentation

Session notes are recorded in Athena Software (Penelope) and Netsmart myEvolv, both secure electronic medical records systems. Report copies may also be kept in the client files.

Document Retention

Electronic medical records in Penelope and myEvolv are maintained indefinitely in this secure medium. Any client paper files are maintained behind a locked chart room in a file cabinet. The room holding client files is locked after hours as well. Any files maintained are housed in locked cabinets behind two sets of locked doors when DMCC is not open for business. Paper files of terminated clients are scanned in Penelope and/or myEvolv and stored at a secured facility.

Deleted: on

Deleted: in

Deleted: that is open during business hours and locked thereafter

Section III: Technical Safeguards

Technical safeguards refer to the procedures in place to control access and/or interception to computer systems and to protect all communications containing PHI transmitted electronically.

Electronic Medical Records System (Penelope)

DMCC uses both Penelope and myEvolv software, electronic medical records systems designed specifically for counseling centers and psychology training clinics. Penelope and myEvolv may only be accessed by DMCC personnel, each of which has a unique username and password. Access is restricted by safety measures in the system that restrict users from being able to view records of clients who are not their own. Once files are saved, they cannot be changed or erased without a clear electronic tracking of any activity and clear identification of who accessed records. Full access to Penelope is granted only to limited staff including the administrative staff, support staff and technology personnel to maintain the program.

Computer Workstations

All computer access is secure from clients, parents and/or visitors to the DMCC. The reception area computer (which is behind glass and locked doors) is turned off each day after business hours. All DMCC personnel log off of Penelope and myEvolv before leaving them unattended. Documents are kept, completed and maintained in Penelope through the network server and/or client hard files.

Mobile Devices

All organizationally purchased mobile devices used by the DMCC staff have a Mobile Device Management (MDM) application installed on them that allows for remote management and wiping of the device if it is lost or stolen.

Computer Flash Drive

The use of flash drives or portable electronic media to store ePHI data is prohibited.

Cloud Storage

The use of cloud storage to store ePHI is allowed when it is a DMCC approved HIPAA compliant cloud storage.

Faxing

The fax machine at DMCC is housed in a locked area of the clinic. The fax machine is checked throughout the day to ensure faxed documents are not left unattended.

If faxing, only the PHI needed is sent, and a cover letter with a confidentiality statement accompanies the information to help prevent casual reading. Additionally, frequently used fax numbers are programmed into the machine to ensure accuracy in dialing. New fax numbers are verified before PHI is transmitted. The machine does not have the capacity to save copies of faxed information.

Email

DMCC uses an encrypted email solution when emailing client PHI information to entities outside of the network. The encryption process is accomplished with software on our email gateway server. All DMCC personnel have been trained to use “Encrypt” on the subject line to ensure proper encryption. Client level information is attached with a privacy statement in the body of the email. Privacy notices on all emails is appended as part of the sending process and is enforced from the system.

Telephone

Phone calls are made to clients and/or guardians from the office area for routine appointment reminders and appointment clarification. The office area is behind locked doors and a glass partition. All information occurs away from all clients, guardians, and visitors.

Electronic Health Records Policy and Procedures

Electronic Health Records (EHR) complies with HIPAA, and all state and federal laws related to protection of personal health information. EHRs can be encrypted (making the document(s) unreadable to anyone other than an authorized user) and security access parameters set to only authorized individuals can view them. EHRs also offer the added security of an electronic tracking system that provides an accounting of the history of when records have been accessed and by whom.

General Information

System users who send, receive, store and access ePHI must comply with DMCC's Electronic Health Records Policy and Procedures.

I. Policy

DMCC provides physical attributes required to protect information systems and related infrastructure from unauthorized access in accordance with HIPAA Security Rules to protect the availability, confidentiality, and integrity of client and departmental confidential information.

DMCC personnel are responsible for maintaining the physical security of DMCC's computer resources under their control. They are also responsible for protecting the integrity and privacy of the data maintained on the computer by using appropriate lockdown devices, password-controlled access, data encryption, virus protection software, and routine backup procedures.

DMCC is under the umbrella of the California Association of Health and Education Linked Professions (CAHELP), which is a department of San Bernardino County Superintendent of Schools (SBCSS). SBCSS, CAHELP, and DMCC reserve the right to inspect all data and to monitor the use of all its computer systems.

All computer users have no right to privacy regarding information on organizationally supplied computers. Personnel are not allowed to place any client information (ePHI) on personally owned technology devices. The organization reserves the right to remotely access, monitor, control, and configure organizationally supplied computers and any software residing on said device. Non-compliance with this policy is subject to management review and action up to and including termination of employment, vendor contract, and/or legal action.

- All computers are equipped with updated software for detecting the presence of malicious software (i.e., computer viruses). All computing devices have current versions of anti-virus software enabled. Operating systems have all critical updates installed.
- All computers are positioned or located in a manner that minimizes the exposure of displayed patient and/or sensitive business information.

- DMCC personnel accessing the DMCC network or information from remote locations are trained to utilize appropriate security safeguards.
- DMCC through the CAHELP and with SBCSS's direction and approval shall have the ability to recommend and implement hardware, operating systems, and connectivity solutions to be supported. System support of any proposed solutions will need to be included in the purchasing decision.
- DMCC personnel may not independently install hardware or software solutions that allow remote access to organizationally purchased devices.
- DMCC personnel must comply with DMCC's policies and state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

II. PURPOSE

The DMCC is committed and required to provide security to protect its computerized clinical and business information systems. DMCC computer system hardware and software as well as the information and data carried by the system are the property of the CAHELP/SBCSS. Any misuse of DMCC computers may result in denial of access to the system network and systems, DMCC information, and data. The intent of this policy is to:

- Ensure each system containing ePHI has the necessary access controls to restrict unauthorized users and programs from accessing patient health or sensitive business information.
- Ensure software on each computer on the network is internally compatible and will not lead to degradation of the system.
- Ensure users are oriented and trained on computer use and maintenance of information integrity, privacy, and resource security.
- Establish security requirements for the appropriate use of mobile computing resources including laptops and mobile computing devices that access DMCC information or interface with the DMCC network.

III. SCOPE

This policy applies to all DMCC personnel, vendors, contractors, and business associates who have access to DMCC client information, either clinical and/or business related, stored on DMCC computers or have access to its computer resources or network. The scope of this policy includes the usage of all and any device that directly or remotely accesses the DMCC network.

IV. DEFINITION

Portable-Computer Device: A portable-computing device is a computer that is easily transported by hand and could store DMCC client and/or business information. "Portable computing device" generally refers to laptop computers, smart clipboards, and mobile computing devices but can include other emerging technologies that allow storage of and access to information and are capable of connection (physical or wireless) to the computer network, including connection to any server or computer on the computer network.

V. PROCEDURES

General

1. Users are required to log-off of applications containing client health and/or sensitive business information before leaving their computers.
2. Users must save work that contains ePHI in accordance with approved data storage policies.
3. All laptops and any other portable computer equipment must be secured (protected) when not in use.
4. Storing ePHI information on ANY Device that is not encrypted is prohibited.
5. Storing of PHI information on a personal device is prohibited.
6. Employees are responsible for breaches of security related to devices in their possession.
7. All computers require a complex-level password protection with the computer system. In order to access any client health and/or business information, a second level of authentication protection is required to access information.
8. There are no circumstances when security provisions are allowed to be disabled.
9. DMCC personnel are required to have appropriate clearance prior to access to computers and the Penelope network.
10. Upon termination or change of job position, users will have network access removed or modified as deemed appropriate by administration.
11. All computer devices shall be tagged and tracked by administration in accordance with SBCSS's asset management policies and procedures.

Desktop Computers

DMCC has established standard configurations for desktop technologies deployed throughout the organization. All computers, computer peripherals, and software as well as printers, faxes, and other miscellaneous hardware purchased with DMCC funds or attached to any component of the DMCC network must meet these standards.

Installation of any personal software, whether purchased or downloaded, by employees is prohibited. Software required for end user productivity must be approved by the Director and installed by CAHELP/SBCSS helpdesk staff.

Desktop computers are located in areas that are physically separate and face away from the public.

Computer access and password training provided by the DMCC administrative staff must be completed prior to granting access privileges to ensure adequate training has occurred.

Desktop computers are equipped with security hardware and/or software. Computers **must** comply with all software updates for detecting the presence of malicious software. All devices will have current versions of anti-virus software enabled. Operating systems will have all critical updates installed.

Mobile devices that store ePHI will be secured using compliant measures.

Organizationally Supplied Portable/Mobile Computer Devices

The loss or theft of any portable computer device storing DMCC client and/or sensitive business information shall be immediately reported to the employee's supervisor. The supervisor will contact the DMCC Security/Privacy Officer.
Startup authentication and authorization passwords (username and password) are required on all computers. Storing or caching username and passwords on any device is prohibited.

Organizationally supplied portable computer devices storing data belonging to the DMCC may not be shared with others, especially non-employees, who are not authorized to access the information unless the information is stored as encrypted password protected files.

DMCC reserves the right to identify sensitive information and initiate methods to secure this information.

Personally Supplied Portable/Mobile Computer Devices

The use of personally supplied devices by DMCC/CAHELP personnel in support of the organization's mission or work is strictly prohibited.

Remote Access

Access to DMCC's internal remote location will be done through appropriate Virtual Private Network (VPN) services and must be approved by the Security/Privacy Officer.

Access to DMCC's internal network from outside of its defined network perimeter will be controlled by VPN access controls that may only be established by technical staff.

Users are not authorized to install hardware or software solutions that would allow remote access to their organizationally supplied computing devices.

VPN connections will be strictly controlled, implemented, and maintained by SBCSS technical staff.

VI. Staff Use of System and Privileges

Monitoring of computer use

Personnel utilizing DMCC systems should have no expectation of privacy. The DMCC will log, review, or monitor any data stored or transmitted on its information systems to manage those assets to ensure compliance with the agency's policies.

Removal of staff privileges

The DMCC may remove or deactivate any employee's network privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

System Security

Each computing device used to access, transmit, receive, or store ePHI must comply with DMCC policies. If any policy requirement is not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The system must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The computer must not be used to send, receive, or store ePHI

VII. Data Maintenance and Emergency Procedures

Server

Since 2007, private health information at the DMCC that is ePHI is maintained by an Electronic Medical Records System (Penelope). Penelope is a cloud-based system that provides for redundancy and disaster recovery solutions. The data sheet for Penelope can be found at:

http://www.athenasoftware.net/resources/Penelope_PRIVACY_AND_SECURITY_Whitepaper_2014.pdf

Since March 2020, private health information at the DMCC that is ePHI is maintained by an Electronic Medical Records System (Netsmart myEvolv). myEvolv is a cloud-based system that provides for redundancy and disaster recovery solutions. The data sheet for myEvolv can be found in Appendix D.

Technical staff are responsible to ensure all servers used to access, transmit, receive or store ePHI are appropriately secured with this policy.

1. Server Location

DMCC in-house (non-cloud) servers currently reside at a secure facility. All data not stored in the cloud solution is stored on these systems.

- Servers are located in a physically secure environment
- The system administrator account is password protected
- A user identification and password authentication mechanism is implemented to control user access to the system
- A security patch and update procedure is established and implemented to ensure all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected
- Servers are located on a secure network with firewall protection
- All unused or unnecessary services are disabled

2. Computer Security

Technical staff are responsible to ensure each computer system used to access, transmit, receive, or store ePHI is appropriately secured in accordance with this policy. A user identification and password authentication mechanism is implemented to control user access to the system.

- All users must be issued a unique username for accessing PII
- Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, within 24 hours
- Passwords are not to be shared
- Passwords must be at least eight characters and complex
- Passwords must not be cached
- Passwords must be changed every 180 days.
- Passwords must be changed if revealed or compromised.
- 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)
- A security patch and update procedure are established and implemented to ensure all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected: All computers and devices that process and/or store PII must have critical security patches applied including those patches that require a system reboot. The patch management process determines installation timeframe based on risk assessment and vendor recommendations. All applicable patches deemed as high risk must be installed as soon as practical. Applications and systems unable to be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

- A malware detection system is implemented including a procedure to ensure the detection software is maintained and up to date
- All unused or unnecessary services are disabled
- An automatic logoff or inactivity timeout mechanism is implemented
- The computer screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen may be used
- Laptop devices will have hardware level disk encryption
- **Data Destruction:** When an electronic storage device that contains PII is sent for destruction, it is erased using the US Department of Defense clearing and sanitizing standard DoD 5220.22-M or equivalent
- **System Timeout:** The system providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 30 minutes of activity
- **System Logging:** The system maintains an automated audit trail that can identify the user or system process, initiates a request for PII, or alters PII. 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 PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence
- **Access Controls:** The system providing access to PII must use role-based access controls for all user authentications, enforcing the principle of least privilege
- **Transmission Encryption:** All data transmission of PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm that is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email
- **Intrusion Detection:** All systems involved in accessing, holding, transporting, and protecting PII, which are accessible through the Internet, must be protected by a comprehensive intrusion detection and prevention solution

3. Logoff Procedures

To ensure security to all servers and computers accessing, transmitting, receiving, and/or ePHI, the following procedures must be followed:

Automatic Logoff Procedures

- Servers, computers, and other electronic devices containing ePHI must employ inactivity timers or automatic logoff mechanisms
- Servers, computers, and other electronic devices containing ePHI must terminate a user session after a maximum of, but not limited to, 30 minutes of inactivity

- When a system requires the use of an inactivity timer or automatic logoff mechanism but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
  - The system must be upgraded to support the minimum HIPAA Security
  - The system must be moved into a secure environment
  - ePHI must be removed and relocated to a system supporting the minimum requirements

Logging off the System

When a server, computer, or other electronic device is unattended users must lock or activate the systems Automatic Logoff Mechanism (e.g., CTRL, ALT, DELETE and Lock computer), or logout of all applications and database systems containing confidential information.

Network and Privacy Settings

Schedule for Backups

Backups are scheduled nightly and are encrypted to offsite, encrypted storage. Backups are maintained for a two-week period.

Recovery Plan for Data

On premises servers are backed up regularly using VM-level backups. Servers and data can restore all data necessary to the version from the night before. There is also a database-level backup of Penelope data that is performed daily. Details for back and recovery for clouds servers can be found in (See Appendix C).

Security Protocols for Access to Data

Password resets are in effect every 180 days for all users.

Encryption security level

- Computers and server storage is encrypted where necessary
- Intra site communication is direct and secure so no special encryption is necessary.

Firewalls

The DMCC has firewalls installed at internet connection points at the primary datacenter and disaster recovery datacenter. Firewalls are maintained and patched by a firewall vendor. Inbound access is analyzed using an IPS/IDS, Intrusion Prevention Systems and Intrusion Detection system, device which scans all inbound and outbound traffic for malicious attacks. Both datacenters are secured, and access is controlled with the use of a key card access system. Only authorized personnel are permitted to access our datacenters. The primary data center power is protected using a natural gas generator and halon fire suppression system.

Remote Access

Access from outside of DMCC is available only through approved VPN secured connections with encrypted and physical security checks.

VIII. Electronically Signed Records

For the purpose of this policy an electronically signed record is a financial, program, or medical record that (1) is required to be signed under California or Federal law, California or Federal regulation, or organizational policy or procedure, and (2) may be requested during an audit.

Standards for Electronic Signatures in Electronically Signed Records

Electronic signatures in electronically signed records will be viewed as equivalent to a manual signature affixed by hand for financial, program, and medical records for audit purposes as defined under the California Code of Regulations, Title 9.

DMCC's policy for electronic signature meets the following requirements:

1. DMCC's computer system (Penelope and myEvolv) utilizes electronic signatures that comply with the following Certification Commission for Healthcare Information Technology (CCHIT) certification criteria or equivalent: *Security: Access Control, Security: Audit, and Security: Authentication.*
2. The electronic signature mechanism is (a) unique to the signer, (b) under the signer's sole control, (c) capable of being verified, and (d) linked to the data so that, if the data are changed, the signature is invalidated. Additionally, DMCC will maintain physical signatures for all clinical staff on file as backup.
3. DMCC will maintain an Electronic Signature Agreement for the terms of use of an electronic signature signed by both the individual requesting electronic signature authorization and the county mental health director or his/her designee.
4. DMCC will request and maintain an Electronic Signature Certification from entities where contracts are held through the Department of Behavioral Health where such is required.
5. The signed *Electronic Signature Certification* and signed *Electronic Signature Agreements* forms will be available to the auditor at the time of an audit.

Information Security Considerations

DMCC's standard encryption of data is also employed in the electronically signed record.

Obtaining Consumer Signatures

In many situations, the mental health consumer, or his/her representative, must acknowledge his/her willingness to participate in and accept the treatment plan. In paper-based systems, the consumer, or his/her representative, physically signs a document to that effect. As an alternative to paper, it is DMCC's policy the following approaches will be utilized: (1) scanning paper consent documents, treatment plans, or other medical record documents containing consumer signatures or (2) capturing signature images from a signature pad.

DMCC will maintain all information and will be in full compliance with all applicable HIPAA electronic signature standards. Upon future publication of HIPAA electronic signature regulations, the DMCC will be in full compliance within the timelines and all requirements established by state and federal government.

Requirements for Electronically Signed Records

The DMCC will utilize electronic records and electronically signed records to replace all paper-based records for purposes of an audit. When an audit is conducted, the DMCC shall make available the following upon arrival of the auditor at the audit site:

- Physical access to electronic health record systems
- Adequate computer access to the electronic health records needed for the audit review
- System or network access to electronic records such as user IDs and passwords
- Access to printers and capability to print necessary documents
- Technical assistance as requested
- Scanned documents, if needed, which are readable and complete

PHI – Personal Health Information

PHI and PII Use and Disclosure

PHI Definition and Data Elements

Below is an excerpt from the U.S. Department of Health & Human Services defining PHI and PHI data elements:

Protected Health Information: The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information *protected health information* (PHI).

Individually identifiable health information is information, including demographic data, that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual,
- The individual's identity or for which there is a reasonable basis to believe it can be used to identify the individual

Individually identifiable health information includes many common identifiers (i.e., name, address, birth date, Social Security Number) and generally encompasses all PII (see below). All PHI is protected by both HIPAA and ethical standards.

PII Definition and Data Elements

Per the Executive Office of the President, Office of Management and Budget (OMB) and the U.S. Department of Commerce, Office of the Chief Information Officer, The term *personally identifiable information* refers to information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Any information that is personal is protected by privacy laws.

California Senate Bill SB 1386: *personal information* means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social Security Number
2. Driver's license number or California Identification Care number
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

Use and Disclosure Defined

The DMCC will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use* – The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the company, or by a business associate of the company
- *Disclosure* – for information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within DMCC with a business "need to know" PHI

Access to PHI is Limited to Certain Employees

All personnel who perform Participant functions directly on behalf of the DMCC or on behalf of group health plans will have access to PHI as determined by their supervisor, job description, and as granted by IT. These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed is limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Personnel may not access either through the information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members, or other individuals for personal or other non-work-related purposes, even if written or oral participant authorization has been given. If the employee is a participant in DMCC's plans, the employee must go through their provider in order to request their own PHI.

In the very rare circumstance when an employee's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she will immediately report the situation to his/her supervisor who will assign a different staff member to complete the task involving the specific participant.

Personal access to your own PHI is based on the same procedures available to other participants not based on job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your provider for the information or make a written request to the Security/Privacy Officer. Employees may not access their own information; they must go through all the appropriate channels as participants are required to do.

Disclosure of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization satisfying HIPAA requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

Permissive Disclosures of PHI: For Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. DMCC's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- About victims-of-abuse, neglect or domestic violence;
- For judicial and administrative proceedings – with appropriate subpoenas;
- For law enforcement purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

Complying with the "Minimum-Necessary" Standard

HIPAA requires when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum-necessary" to accomplish the purpose of the use or disclosure. The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual;
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Department of Labor;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

Minimum-Necessary When Disclosing PHI

For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum-necessary amount of information will be disclosed. All other disclosures must be reviewed on an individual basis with the Security/Privacy Officer to ensure the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum-Necessary When Requesting PHI

For making request for disclosure of PHI from business associates, providers, or participants for the purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Security/Privacy Officer to ensure the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Protected Health Information (PHI): Patient information, including demographic information, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient; and
- Identifies the patient or can be used to identify a patient.

Lobby Interactions

DMCC personnel are not to reveal PHI in the lobby with clients. DMCC personnel will ask clients and/or parents to step into a confidential, private office to conduct conversations related to PHI.

Consequences of Violations

Personnel violations of DMCC systems as described above will be subject to disciplinary action that may include termination of employment.

Disclosure of PHI to Business Associates

Based on the approval of the Security/Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the company's business associates and allow the DMCC's business associates to create or receive PHI on its behalf. However, prior to doing so, the DMCC must obtain assurances from the business associate agreeing to appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of "business associate" employees must contact the Security/Privacy Officer and verify that a business associate contract is in place.

"Business associate" is an entity that:

- Performs or assists in performing a company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Disclosures of D-Identified Information

The DMCC may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual. Respect is given to the fact that there is no reasonable basis to believe the information can be used to identify an individual. There are two ways a covered entity can determine when information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers listed below – relating to the participant, employee, relatives, or employer, and being certain there is no other available information that could be used alone or in combination to identify an individual.

1. Names
2. Geographic subdivision smaller than a state
3. All elements of dates (except year) related to an individual – including dates of admission, discharge, birth, death – and for persons >89 years old, the year of birth cannot be used
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social security number
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos and comparable images
18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small regarding the information that could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. This person is required to document the methods and justification for this determination.

Disclosure to Family, Friends or Others – Participant Location

There are instances when a participant's friend or family member contacts the DMCC to ask about the location of a client or whether the client has been seen at the DMCC. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, and at the discretion of the Director of the DMCC, a minimum amount of information may be released in order to assist in resolving an emergency situation.

Guidance

Situation: Friends or family are concerned about the whereabouts of a person. They contact the DMCC and ask if a person is at the DMCC or has been seen as a client recently.

Response

For any inquiry regarding a current or past client, DMCC clinic staff should take the name of the caller, purpose for calling and state the caller will receive a return call from DMCC. DMCC staff should check if releases of information are on file. If they are on file, DMCC should make contact with the parent/client to inform them of the nature of the release of information. If parent/client agrees, DMCC will return the call and provide only the minimum information required.

If releases of information are not on file, DMCC must inform the caller that DMCC cannot confirm or deny the person is a client. If the friends and/or family are concerned about the person's whereabouts, DMCC can recommend they call other relatives of the person and/or contact the local police department to inquire about safety.

Situation: An individual comes to DMCC and tells the receptionist they have arrived to pick up a client.

Response

The DMCC serves children birth to 22 years old. Parents, guardians, or a responsible adult brining the child to treatment is expected to remain on the premises throughout the child's treatment service. In the event, the parent, guardian, or responsible adult leaves the premises, the child will contact the parent by phone. Any individual requesting information about a client will only be given information if a Release of Information is on file allowing the DMCC to share information with that specific individual.

Removing PHI from Company Premises

PHI is not allowed to leave the organization's premises at any time.

California Association of Health and Education Linked Professions
Joint Powers Authority (CAHELP JPA)
DESERT/MOUNTAIN SELPA STEERING and FINANCE COMMITTEE MEETING
August 27, 2021 – 9:00 a.m. Virtual via Videoconference
Desert Mountain Educational Service Center, 17800 Highway 18, Apple Valley CA 92307

MINUTES

D/M SELPA MEMBERS PRESENT:
Academy for Academic Excellence – Marcelo Congo, Samantha Gonzalez, Adelanto SD –Michael Baird, Apple Valley USD – Renee Castillo, David Wheeler, Baker Valley USD – Cecil Edwards, Barstow USD – Heather Reid, Desert/Mountain Operations (SBCSS) – Rich Frederick, Excelsior Charter Schools – Marie Silva, Health Science and Middle – Brian Kennedy, Kristen Kosaka, Helendale SD – Mike Esposito, Hesperia USD – Eric Land, Teri McCollum, Elaine Nelson, Lucerne Valley SD – Vici Miller, Needles USD – Jamie Wiesner, Oro Grande SD – Nelda Colvin, Scott Heitman, Snowline JUSD – Robert Chacon, Lori Delgado, Victor Elementary SD – Tanya Benitez, Melanie Madoo, and Victor Valley UHSD – Margaret Akinnusi, Rama Bassham, Wennifer Beard.

OTHERS PRESENT:
Waneka Cabrera – Options for Youth, Christina Leal – Options for Youth.

CAHELP, SELPA, & DMCC STAFF PRESENT:
Heidi Chavez, Craig Cleveland, Danielle Cote, Tara Deavitt, Lindsey Devor, Peggy Dunn, Adrien Faamausili, Thomas Flores, Marina Gallegos, Bonnie Garcia, Renee Garcia, Derek Hale, Jenae Holtz, Linda Llamas, Angela Mgbeke, Lisa Nash, Sheila Parisian, Karina Quezada, Jennifer Rountree, Veronica Rousseau, Jessica Soto, Stephanie Sweem, Erica Vargas, and Athena Vernon.

1.0 CALL TO ORDER

The regular meeting of the California Association of Health and Education Linked Professions Joint Powers Authority (CAHELP JPA) Desert/Mountain SELPA Steering and Finance Committee Meeting was called to order by Chairperson Jenae Holtz, at 9:02 a.m., at the Desert/Mountain Educational Service Center, Apple Valley.

2.0 ROLL CALL

3.0 PUBLIC PARTICIPATION

None.

4.0 ADOPTION OF THE AGENDA

4.1 **BE IT RESOLVED** that a motion was made by Teri McCollum, seconded by Cheri Rigdon, to approve the August 27, 2021, Desert/Mountain SELPA Steering and Finance Committee Meeting Agenda as presented. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

5.0 INFORMATION/ACTION

5.1 Desert/Mountain SELPA D/M 66 Assessment Plan (**ACTION)**

Forms used in the operations of special education programs within the Desert/Mountain SELPA are developed, reviewed, and revised throughout the year upon the recommendation of the Program Team. Forms are modified as necessary in order to support the operations of special education programs in an efficient, effective and legally compliant manner. Suggested revisions to SELPA Forms are submitted to the D/M SELPA Steering Committee for consideration and approval.

Lisa Nash explained that each time an assessment plan is provided to a parent there should also be a Prior Written Notice (PWN) provided. The D/M 66 includes the elements required in a PWN to eliminate duplicate work.

Jenae Holtz said there is some redundancy in the form but it will ensure that parents clearly understand what is happening with their children.

Lisa said it is not intended to list specific assessments being given but instead to the general nature of what is going to be evaluated.

5.1.1 **BE IT RESOLVED** that a motion was made by Cecil Edwards, seconded by Marie Silva, to approve the Desert/Mountain SELPA D/M 66 Assessment Plan as presented. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

5.2 Desert/Mountain SELPA Policy and Procedures Chapter 1 **(ACTION)**

Policies and procedures governing the operation of special education programs within the Desert/Mountain SELPA are developed, reviewed, and revised throughout the year upon the recommendation of the Program Team. Policies and Procedures are modified as necessary in order to ensure that special education programs are operated in an efficient, effective and legally compliant manner. Suggested revisions to SELPA Policy and Procedures are submitted to the D/M SELPA Steering Committee consideration and approval.

Sheila Parisian explained this change allows a child to be accounted for in CalPads immediately upon transfer. She said this is for any transfer to an LEA.

5.2.1 **BE IT RESOLVED** that a motion was made by Marie Silva, seconded by Michael Baird, to approve the Desert/Mountain SELPA Policy & Procedures Chapter 1 as presented. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

5.3 Desert/Mountain SELPA Interim Placement Form (**ACTION)**

Forms used in the operations of special education programs within the Desert/Mountain SELPA are developed, reviewed, and revised throughout the year upon the recommendation of the Program Team. Forms are modified as necessary in order to support the operations of special education programs in an efficient, effective and legally compliant manner. Suggested revisions to SELPA Forms are submitted to the D/M SELPA Steering Committee for consideration and approval.

Sheila Parisian confirmed the Interim Placement Form is to be completed when the child is transferred, then an addendum IEP is done in 30 days. Sheila stated the form will not be finalized like an IEP as it is behind the scenes notifying CALPADS that the student has transferred in, and an IEP will be held within 30 days.

Jenae Holtz reiterated the form is completed then given to the LEA CALPADS person who enters the data in CALPADS to show the student belongs with the new LEA, that they are a transfer in, and what services will be provided. She continued that this will help reduce errors in CALPADS as well as identifying which LEA is accountable for the student.

5.3.1 **BE IT RESOLVED** that a motion was made by Cheri Rigdon, seconded by Maria Silva, to approve the Desert/Mountain SELPA Interim Placement Form as presented. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

6.0 CONSENT ITEMS

It is recommended that the Steering and Finance Committee consider approving several Agenda items as a Consent list. Consent Items are routine in nature and can be enacted in one motion without further discussion. Consent items may be called up by any Committee Member at the meeting for clarification, discussion, or change.

6.1 **BE IT RESOLVED** that a motion was made by Cheri Rigdon, seconded by Vici Miller, to approve the following Consent Items be approved as presented. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

6.1.1 Approve the June 18, 2021, Desert/Mountain SELPA Steering and Finance Committee Meeting Minutes.

7.0 CHIEF EXECUTIVE OFFICER AND STAFF REPORTS

7.1 California's Special Education Governance and Accountability (SEGA) Study

Jenae Holtz presented information on California's Special Education Governance and Accountability (SEGA) study. She stated WestEd is a private organization that was hired to review special education accountability and governance. Jenae continued there are agendas for change statewide for SELPAs to exist under county offices of education but more for districts to handle SELPA duties. She said this does impact charters and small LEAs the most because in D/M SELPA, the LEAs work together with the superintendents' making decisions about where the money is used. Jenae also said there are arguments against it because there are not enough resources for each LEA to have the structure of due process, compliance, and professional development. Jenae continued that D/M SELPA being part of CAHELP JPA, the member districts choose to be members and agree to the policies and procedures with input as stakeholders. Jenae said it would be a huge change legislatively to make the change in California. State SELPA has met with and talked with the researchers about what their findings are. She reported in doing their research, WestEd did not include schools in Los Angeles USD which is the largest district in the state. Jenae will continue to share findings with Steering Committees. Jenae reiterated that being a JPA protects D/M Charter SELPA and D/M SELPA because they are already a consortium of LEAs.

7.2 California State Testing Updates

Jenae Holtz called on Karina Quezada to present on the latest California state testing updates. Karina reported the Physical Fitness Test (PFT) was suspended last year but has been resumed for the current school year. The test is to be administered February through May and it is important to begin preparation now. Karina continued the PFT is administered to students in 5th, 7th, and 9th grades including students on 504 plans and with IEPs based on the recommendations of their respective teams.

Karina stated California Department of Education (CDE) is allowing remote testing for the 2021-22 administration of California Assessment of Student Performance and Progress (CAASP) and English Language Proficiency Assessments for California (ELPAC). CDE is encouraging in-person testing whenever possible to provide the most accessibility and secure testing experience.

Karina continued those students who have been identified as having a specific learning disability are no longer eligible to receive the California Alternate Assessments (CAA) or the Alternate ELPAC. The reason is that the alternate assessments are meant for students that have significant cognitive disabilities and by nature, students with a specific learning disability do not meet that criterion. Karina reported that once a student is designated as taking one alternate assessment, they will be automatically enrolled in all other alternate assessments. Karina continued that Moodle is the website where CDE houses the trainings for the Alternate ELPAC, and CAA and trainings need to be completed by October 15, 2021.

7.3 Desert Mountain Operations Updates

No update was provided for Desert Mountain Operations.

7.4 Desert/Mountain Children's Center Client Services Reports and Updates

Linda Llamas presented the Desert/Mountain Children's Center (DMCC) Client Services monthly reports and updates. She then shared a Referral Report is being created and will be disseminated in the same manner as the monthly service reports beginning with the September Steering meeting. Students will populate on the reports if the LEA or a staff member is listed on the referral. Linda said she is working to fill staffing vacancies and making up services. She continued that DMCC has entered a partnership with Kids First Foundation for part-time and full-time positions.

Vici Miller shared that the crisis debriefing team did a phenomenal job with her district. She said she will email Linda Llamas some of the teacher and staff feedback. Vici shared it made a huge difference for the staff as well as the students.

7.5 Strategies to Increase Student and Caregiver Engagement in the School Environment

Linda Llamas provided statistics on youth mental health stating the pandemic has exacerbated the concerns for the youth. Linda provided three strategies to increase student and caregiver engagement to include opportunities for artistic expression, student support groups, and connection with the community. These strategies used in the school environment will help students acclimate to the school climate as well as process the past year's experiences. Linda concluded by asking to be contacted with any questions or concerns.

7.6 Professional Learning Summary and Update

Heidi Chavez presented the D/M SELPA's Professional Learning Summary. She shared for 2020-21, there were 5,800 participants with 2,186 participants for onsite trainings and 3,614 participants attending regional trainings. Heidi said there could be instances that in-person trainings are switched to virtual trainings and her team is prepared for that. She continued that there also may be times that even a virtual setting is not feasible which would cause a training to be canceled. Heidi appreciates the understanding from the LEAs.

Heidi reported the next Community Advisory Committee (CAC) meeting will be held at the Hesperia USD District Office on September 23, 2021. She said the meeting will be offered in-person as well as via Zoom. Dr. Ron Powell will be presenting on the impact of Covid-19 on mental health with tips and techniques to overcome stress and help the family thrive. The business meeting will start at 5:00 p.m. with the presentation for parents beginning at 5:30 p.m.

Teri McCollum shared that there are two rooms booked at Hesperia USD for the CAC meeting. She said this will allow room for social distancing.

Heidi shared this year's Integrated Multi-Tiered System of Support (IMTSS) Symposium will be held on March 2, 2022. She said there will be a limited number of in-person seating and will be offered virtually as well. Books and resources will be mailed to virtual participants. The presenters will be Kevin Hines and Anne Moss Rogers.

7.7 Resolution Support Services Summary

Jenae Holtz reported the CAHELP JPA team consults with attorneys before presenting information at committee meetings. She said there are different opinions regarding Assembly Bill (AB) 130 and independent study and assured the committee members that her team will work through concerns and issues as they arise. Jenae stated in working together and giving grace, we will continue to help children and families in a very different season of life the best way we can.

Lisa Nash presented the D/M SELPA's Resolution Support Services Summary (RSS). She reported one of the filings this year has been initiated against a parent. Lisa continued the number of filings is a little below average for this time of the school year but the RSS team expects the number to increase as schools return to session and with AB 130 being a compounding factor.

7.8 Assembly Bills 104 and 130 Updates

Sheila Parisian provided information pertaining to the amendment of AB 104 stating the purpose was to provide guidelines for LEAs to consider for their retention policies. She said AB 104 is for the 2021-22 school year and applies to students in kindergarten through grade 11 in 2020-21 who received deficient grades. Sheila continued if a parent requests retention the LEA must have a discussion regarding learning loss recovery options, discuss research on the effects of retention and considering the student's data as well as information relevant to whether retention is in the best interest of the student.

Sheila then provided guidance on AB 130. She said there have been many questions about moving forward with independent study for children in special education. Sheila continued that in working with attorneys and colleagues, the Alternative Dispute Resolution (ADR) Participants and Agreement form was created but will be renamed Alternative Dispute Resolution Compromise and Release. Sheila reiterated it is not a D/M SELPA document and is not required. She said items 1-6 are acknowledgements and describe the reason for the conversation. The document will help the parents understand the district's obligation to offer FAPE and to provide the best education for the student as well as facilitate an agreement to avoid litigation by both parties. Sheila said it is important that the parent has consented to the most recent in-person offer of FAPE with an addendum being created to reflect services the student will be receiving while in independent study with the end date being no later than June 30, 2022.

After some discussion, Jenae Holtz agreed that for a majority of students with disabilities, independent study is not an appropriate offer of FAPE. However, once a parent says they want independent study, the IEP team can note they do not agree independent study meets FAPE but will offer services to support the student while in independent study. She continued that is not an offer of FAPE but an offer of services. Jenae stated to make that clear in the notes to protect everyone involved. In the notes, it should be documented that the IEP team does not agree with independent study but are honoring the parent's request based on AB 130 by providing the listed supports.

It was suggested that the services line to read the offer of FAPE services with an end date, the beginning date and end date of independent study and appropriate services, then the original offer of FAPE with the date of the next school year. It would also include a statement that the LEA is allowing the services requested by the parent based on AB 130. Jenae agreed that would be appropriate.

Jenae said the document would continue to be reviewed and revised by the D/M SELPA team to address the concerns brought up by the committee members. She asked the committee members to contact Sheila if they want to participate in updating the form. The changes will need to be done quickly.

Several of the directors reported that they have hired special education teachers to assist with students that are receiving independent study. Jenae said she will work with the Governance Council to support smaller districts with independent study.

There was discussion around how much instruction time should be provided to students in independent study. It was suggested for the IEP team to determine what supports and how much time could be provided. Sheila Parisian said to review the distance learning plans to help gauge how much time a child could focus their attention as a guide.

Jenae concluded that the input from the committee members is valued and that D/M SELPA is wanting to help however possible.

7.9 Office of Administrative Hearings Decision

Jenae Holtz called on Lisa Nash to review an Office of Administrative Hearings (OAH) decision. Lisa provided a brief synopsis of Parent on Behalf of Student v. Long Beach Unified School District. The school district did use prior written notice (PWN) but failed to follow up on the notices by not filing due process to enforce their Independent Education Evaluation (IEE) cost criteria which caused them to be found to have violated a free appropriate public education (FAPE).

7.10 Alternative Dispute Resolution (ADR) Planning Committee Update

Karina Quezada shared an update from the ADR Planning Committee. She shared that there will be flyers being distributed soon regarding the upcoming meetings and training dates. Karina said the first meeting is scheduled for September 14 and a Key2Ed training in January. She continued that Kathleen Peters will be hosting Zoom meetings on Tuesday, August 31 and Thursday, September 2 at 3:30pm to discuss the utilization of available ADR grant funds.

7.11 You be the Judge Scenario

Jenae Holtz called on Lisa Nash to present a You be the Judge scenario for committee member participation. Lisa shared a Michigan case in which a parent received a truancy letter shortly after complaining to school staff about the student's placement. The letter stated because of the student's unexcused absences, the parent could be prosecuted under law. Lisa continued that the attendance agent was not aware of the placement concerns and after 12 unexcused absences, action needed to be taken based on district policies and practices. The judge found the truancy letter was not a reprisal for the parent's placement complaints as the attendance agent and special education staff did not communicate about the concerns and that the student had in fact accumulated enough unexcused absences to trigger the issuance of a truancy letter.

7.12 Prevention and Intervention Updates

Athena Vernon presented Prevention and Intervention updates. She stated the CDE website has Transformative Social and Emotional Learning (T-SEL) resources that stemmed from a 2020 initiative. Athena shared there is a 2-day restorative practices training December 8-9, 2021, for using circles effectively.

7.13 2020-21 Career Technical Education (CTE) Reports

Heidi Chavez presented the 2020-21 CTE Reports on behalf of Adrienne Shepherd-Myles.

7.14 Compliance Update

Peggy Dunn presented an update on compliance items from the California Department of Education (CDE). For Significant Disproportionality, the quarterly progress and expenditures report has been submitted. 2019-20 Disproportionality follow up has been approved with five LEAs in disproportionality for 2020-21. CDE will be reviewing student files through Web IEP. She said it is important for IEPs to be completed with supporting documentation uploaded. Peggy continued that the Personnel Data Reports have been completed and certified along with the Annual Service Plans. The Desired Results Development Profile (DRDP) have also been completed and certified. CALPADS End of Year 3 and 4 for June pupil counts have been completed and certified. Peggy shared the Management Information System (MIS) Users' Meeting – CALPAD Errors is scheduled for September 21, 2021, at 9:00am-11:00am.

Jenae Holtz said she will speak with Rich Frederick and Colette Garland about Inland Regional Center (IRC) staff having access to Web IEP so they can enter Individualized Family Service Plans (IFSP) for families that receive services.

7.15 Nonpublic School/Nonpublic Agency Update

Peggy Dunn provided a nonpublic school/nonpublic agency update. She shared that NPAs are working to secure nurses that must be CDE certified in order to be utilized.

Peggy Dunn shared that Anita Padilla is the new principal at Desert View NPS.

8.0 FINANCE COMMITTEE REPORTS

8.1 2021-22 P-2 Special Education Revenue Projection

Marina Gallegos presented the 2021-22 P-2 Special Education Revenue Projection. She said the figures shared are based on the governor's final budget increasing the base rate was increased from $625 to $715 average daily attendance (ADA).

9.0 INFORMATION ITEMS

9.1 Monthly Occupational & Physical Therapy Services Reports

9.2 Monthly Nonpublic School/Agency Placement Report

9.3 Upcoming Professional Learning Opportunities

10.0 STEERING COMMITTEE MEMBERS COMMENTS / REPORTS

Jenae Holtz reported that Desert/Mountain Children's Center has several contracts with Department of Behavioral Health (DBH). DBH has required DMCC to have a database of vaccination cards and/or negative covid tests effective August 23, 2021. All other staff will follow suit prior to October 15, 2021. Jenae said CAHELP is following San Bernardino County Superintendent of Schools (SBCSS) guidelines. Jenae stated as far as showing vaccination cards or negative test results to campus staff, she has posed the questions to SBCSS Human Resources (HR) to ensure staff rights are not being violated. Jenae is waiting for an answer and will share it with the committee members when she receives a response. She said if an LEA is not comfortable with a service provider coming on to campus, services can continue to be provided virtually. Jenae continued that if a nonpublic agency is contracted through CAHELP, CAHELP will also reach out for their information.

Teri McCollum asked for a weekly list of staff that have been cleared via negative covid test or vaccination be provided to the LEAs so they know who is safe to be on campus. She suggested maybe a Google Doc that is constantly updated for the LEAs to view.

Jenae responded there would have to be a contact person at each LEA that would have access and she did like the idea of a Google Doc if approved by HR.

Jenae reiterated that Peggy Dunn is working hard to find CDE approved nonpublic agencies to provide nurses for children that have those services on their IEPs.

Derek Hale shared that he has been in contact with the CEO of Academy for Advancement of Children with Autism. The building the organization was planning to use for the local site fell through, so they are continuing their search. He asked if there were any LEAs with any buildings or space that could be temporarily leased while they search for their own building.

Derek reported that nonpublic schools are not certified or allowed to provide independent study so if a family is adamant about their student being placed in independent study, the student will have to be go back to the district to be served.

Jenae added that some SELPAs are advising parents they can sign their child out of special education. Jenae advises against that.

11.0 CEO COMMENTS

Jenae Holtz shared that the appreciates the hard work of the committee members and remaining focused on children.

12.0 MATTERS BROUGHT BY THE PUBLIC

None.

13.0 ADJOURNMENT

Having no further business to discuss, a motion was made by Cheri Rigdon, seconded by Teri McCollum, to adjourn the meeting. The motion was carried on the following vote 17:0: Ayes: Akinnusi, Baird, Benitez, Colvin, Congo, Delgado, Edwards, Esposito, Frederick, Kennedy, Land, Miller, Reid, Rigdon, Silva, Wheeler, and Wiesner.

The next regular meeting of the Desert/Mountain SELPA Steering and Finance Committee will be held on Friday, September 24, 2021, at 9:00 a.m., at the Desert Mountain Educational Service Center, Aster/Cactus Room, 17800 Highway 18, Apple Valley, CA 92307.

Individuals requiring special accommodations for disabilities are requested to contact Jamie Adkins at (760) 955-3555, at least seven days prior to the date of this meeting.

SELPA Administrators
September Legislative Update

Legislative Committee

SELPA
Administrators of California
Special Education Local Plan Area

Legislative Calendar

★ September 10th-- Last day for each house to pass bills

★ October 10th -- Deadline for Governor to Sign Bills into Law

and the looming issue of………

★ September 14th -- Special Election: Governor Recall - early polling indicates the recall effort will not be successful

SELPA Association Tracked Bills: Sponsor/Support Bills

- **SB 639 (Durazo) – Minimum Wage for People with Disabilities**

  Status: Passed Appropriations; Moved to Assembly

- **AB 586 (O'Donnell) – Pupil Health: Mental Health Services Funding**

  Status: Pending in the Senate Education Committee. May be acted upon in January 2022

Bills of interest

- **SB 692 (Cortese) – LCAP State Priorities: LRE**
  Status: Held in Appropriations - Suspense (Becomes a 2 year bill). This bill was held with support from the sponsors. We continue to engage with the author's office and advocate staffing the bill.

- **AB 313 (C. Garcia) – State Hiring Goals for Persons with Disabilities** *Status: Passed Appropriations; Moved to Senate*

- **AB 104 (Gonzalez) – COVID-19 Pupil Impacts, Alternative Options** *Status: Chaptered (Governor Signed)*

Bills of Interest

- **SB 328 (Portantino) – school start time clean-up; exempts certain rural school districts and rural charter school**
  Status: Pending in the Assembly Education Committee.

- **SB 237 (Portantino) – Dyslexia Risk Screening**
  Status: Pending in the Assembly Education Committee.

AB 167/SB 167 Trailer Bills related to AB 130

- Allows ADA apportionment for IS for quarantined students, including students exposed and waiting for testing.
- The J13A emergency process is not appropriate for COVID quarantine because the state is giving LEAs ability to earn ADA through IS.
- Allows apportionment during staff shortages
- There are 2 ways to earn apportionment under IS: (1) Packet model: Students must complete work product and then teachers assign time value. Auditors then check time value. (2) Course based IS allows students to earn apportionment depending on percentage of completion of the course.

AB 167/SB 167 Trailer Bills Resources/Press

- CalMatters Article
- EdSource Article
- Capitol Advisors Summary
- AB 130 Clean Up Needed - Document created by Adam Stein

Capitol Advisors reached out to our GRR firm, Erin Evans-Fudem to get the Special Education perspective and barriers related to AB 130 Independent Study Rules.

COVID Related

- Masking Mandate and CDPH Guidance
- Independent Study/AB 130 Issues -- Potential Clean Up Needed (Big Thanks to Emily Mostovoy-Luna for providing F3 legal opinions). We are providing language/guidance to GRR who is connecting with other coalitions working on these issues.
- School Employees Vaccine or Test Mandate
- Alert from GRR: There were attempts to have a broad vaccine mandate in multiple sectors, however, it never materialized. This could come back through different vehicles.

Hot Topics
Future Needs & Support from Your Leg Committee

➔ Continued work with the ADR and Finance Committees on the COVID ADR and Learning Recovery Grant Plans and Reporting

➔ October and November Study/Reports to Legislature:
- ✔ Assist in writing templates and grassroots advocacy efforts pending report delivery; working with Studies WorkGroup on how to best do this and timing. GRR working with Studies WorkGroup as well.
- ✔ If you have strong CACs or relationships with local representatives, consider making an appointment when they are in your district

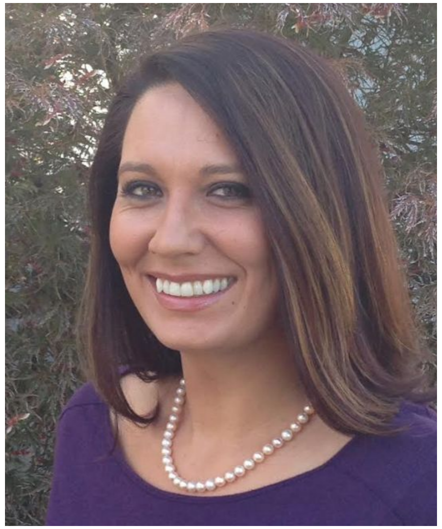
➔ Currently working on:
- ✔ AB 130 Independent Study issues
- ✔ Speech/Language Pathologist State Shortage
- ✔ Consideration of Sponsoring Legislation again! Will work towards goals and priorities this fall
- ✔ Preschool Licensing Barriers to LRE
- ✔ CCS Issues

SELPA Legislative Advocates

Alice Kessler
GreenbergTraurig

Erin Evans-Fudem,
Lighthouse Public Affairs

SELPA Legislative Committee



Veronica Coates, Tehama County SELPA

Adam Stein, Sonoma County SELPA; Sonoma County Charter SELPA

Ray Avila, Santa Barbara County SELPA

Leah Davis, Riverside County SELPA

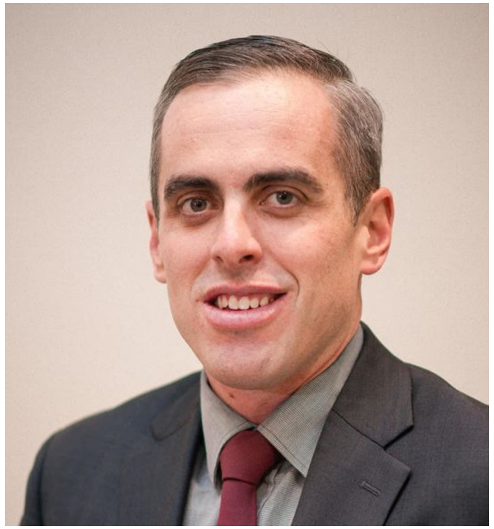
Dina Parker, Tri-City SELPA

Dr. Mayra Helguera, Santa Ana Unified School District/Single District SELPA

Former Legislative Committee Members -- Executive Committee Liaisons to Leg Committee

Mindy Fattig, Humboldt-Del Norte SELPA

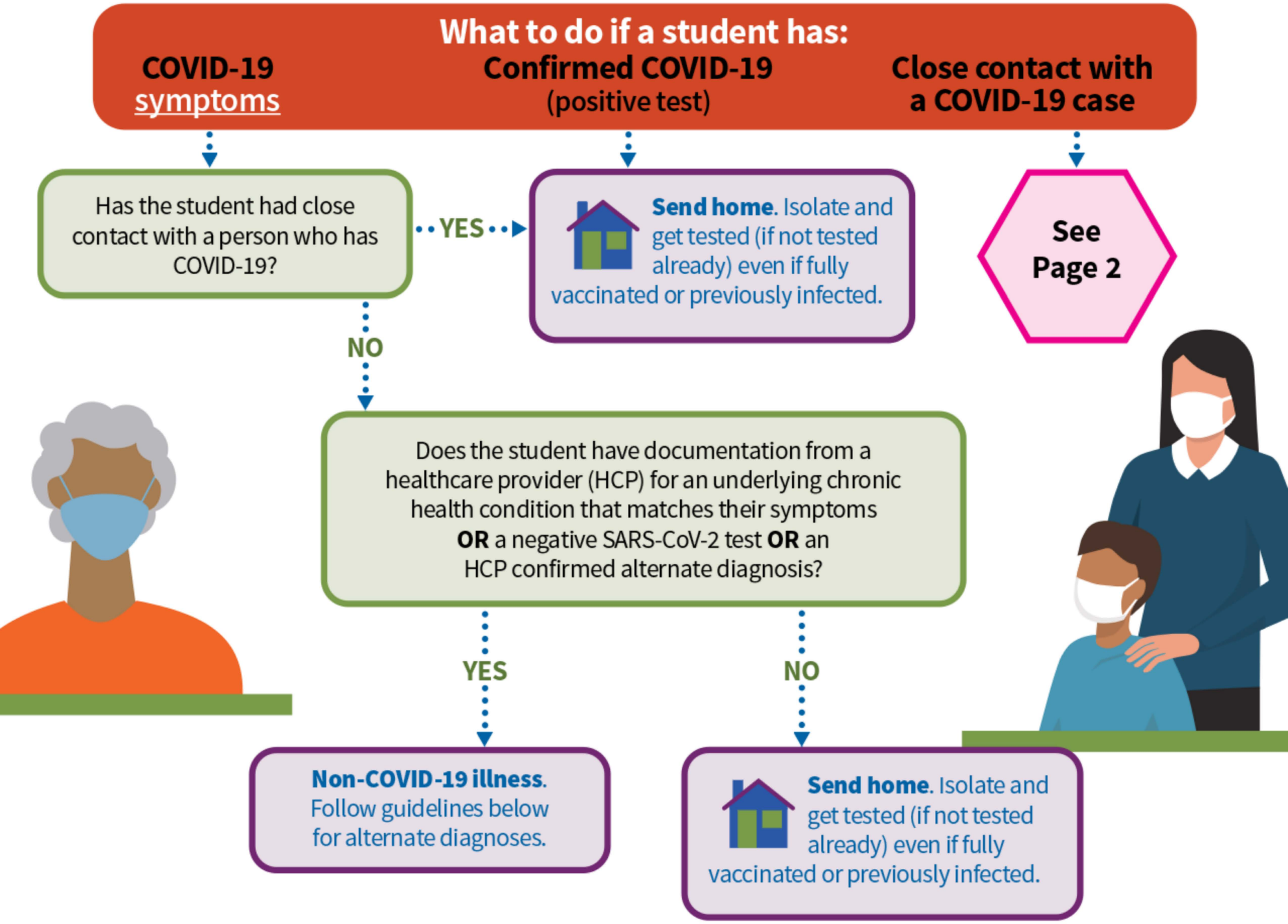
Elizabeth Engelken, Yolo County SELPA



Dr. Scott Turner, East San Gabriel Valley SELPA

Questions?

Managing confirmed or suspected COVID-19 at school*



What to do if a student has:

COVID-19 symptoms

Has the student had close contact with a person who has COVID-19?

YES

Send home. Isolate and get tested (if not tested already) even if fully vaccinated or previously infected.

NO

Does the student have documentation from a healthcare provider (HCP) for an underlying chronic health condition that matches their symptoms **OR** a negative SARS-CoV-2 test **OR** an HCP confirmed alternate diagnosis?

YES

Non-COVID-19 illness. Follow guidelines below for alternate diagnoses.

NO

Send home. Isolate and get tested (if not tested already) even if fully vaccinated or previously infected.

Confirmed COVID-19 (positive test)

Send home. Isolate and get tested (if not tested already) even if fully vaccinated or previously infected.

Close contact with a COVID-19 case

See Page 2

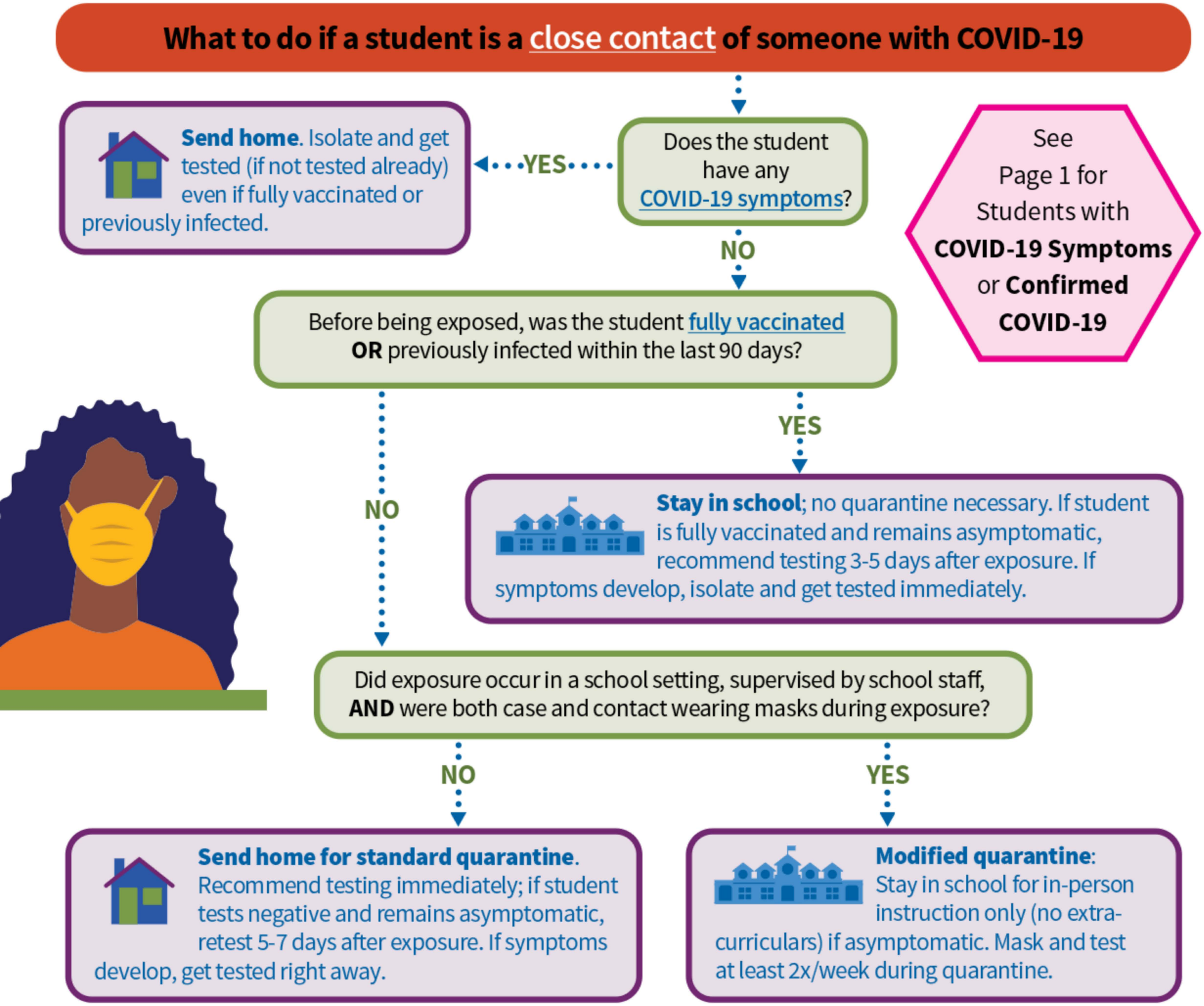
Positive or no test: Stay home in isolation and exclude from in-person instruction for at least 10 days from symptom onset (or from test date if no symptoms). Isolation can end after 10 days **IF** fever-free (without using fever-reducing medication) for at least the previous 24 hours **AND** other symptoms improving.

Negative test or alternate diagnosis (with no previous positive test): May return to in-person instruction if fever-free (without using fever-reducing medication) for at least the previous 24 hours **AND** other symptoms improving.

*For more detailed information and guidelines, see CDPH Schools Guidance and CDPH Isolation & Quarantine Guidance.

Staff and employers are subject to Cal/OSHA COVID-19 ETS or Aerosol Transmissible Diseases standard and should review those requirements.

Managing COVID-19 exposure at school



What to do if a student is a close contact of someone with COVID-19

Does the student have any COVID-19 symptoms?

YES → **Send home.** Isolate and get tested (if not tested already) even if fully vaccinated or previously infected.

See Page 1 for Students with **COVID-19 Symptoms** or **Confirmed COVID-19**

NO → Before being exposed, was the student fully vaccinated **OR** previously infected within the last 90 days?

YES → **Stay in school**; no quarantine necessary. If student is fully vaccinated and remains asymptomatic, recommend testing 3-5 days after exposure. If symptoms develop, isolate and get tested immediately.

NO → Did exposure occur in a school setting, supervised by school staff, **AND** were both case and contact wearing masks during exposure?

NO → **Send home for standard quarantine.** Recommend testing immediately; if student tests negative and remains asymptomatic, retest 5-7 days after exposure. If symptoms develop, get tested right away.

YES → **Modified quarantine**: Stay in school for in-person instruction only (no extra-curriculars) if asymptomatic. Mask and test at least 2x/week during quarantine.

Positive test: Stay home in isolation and exclude from in-person instruction for at least 10 days from symptom onset (or from test date if no symptoms). Isolation can end after 10 days **IF** fever-free (without using fever-reducing medication) for at least the previous 24 hours **AND** other symptoms improving.

Negative or no test: Standard or modified quarantine can end after day 10 following last exposure if student remains asymptomatic.* Quarantine can end after day 7 following last exposure if the student remains asymptomatic and tests negative on day 5 or later.*

*Continue monitoring for symptoms and following all recommended preventative measures through day 14 (masking, hand washing, avoiding crowds, etc). Isolate and get tested if symptoms develop.

Staff and employers are subject to Cal/OSHA COVID-19 ETS or Aerosol Transmissible Diseases standard and should review those requirements.

California Department of Education
Special Education Division

(Revised September 2021)

Alternative Dispute Resolution Allocation Plan

Fiscal Year 2021–22

Due Date: **October 1, 2021**

As a condition of receiving these funds, the special education local plan areas shall, on or before October 1, 2021, develop and submit a plan to the Superintendent of Public Instruction detailing how they will support their member local educational agencies in conducting dispute prevention and voluntary alternative dispute resolution activities, including:

- detailed proposed expenditure information broken down by eligible activity;
- the number, disabilities;
- and demographics of pupils proposed to be served.

SELPA Information

SELPA Name: **Desert/Mountain SELPA**

SELPA Code: 3601

Plan Description

Impacted Areas	Plans by the SELPA and LEA to Conduct Dispute Prevention and Voluntary Alternative Dispute Resolution to Prevent and Resolve Special Education Disputes	Students Served by Proposed Plan
Early intervention to promote collaboration and positive relationships between families and schools and to prevent disputes through proactive communication, collaborative problem solving, and parent support activities.	Integrate outreach activities with existing parent advisory/action groups: SSC, ELAC, DLAC, PTA, CAC, parent resource centers, community liaisons, other. Provide training in cultural diversity, empathy, how to diffuse conflict, and promote "the best interest of the child"	TK-12 students with learning disabilities, English learners at risk of not graduating or reclassifying, students identifying as African American, students with Autism, students on the CDE Dashboard.
Parent education regarding special education processes and rights under the federal Individuals with Disabilities Education Act	Develop parent education modules: RTI, sped continuum, home supports, parent IEP role, advocacy, dispute resolution, transition, mental health, trauma other.	TK-12 students with learning disabilities, Autism, English learners at risk of not graduating or reclassifying, Af Am. students, students on CDE Dashboard.
Parent peer support	Implement local LEA CAC for parents of special needs students to develop parent peer support, connect to resources and provide information.	TK-12 students with learning disabilities and students subject to "Child-find" regulations.

Impacted Areas	Plans by the SELPA and LEA to Conduct Dispute Prevention and Voluntary Alternative Dispute Resolution to Prevent and Resolve Special Education Disputes	Students Served by Proposed Plan
Language access provided as a supplement pursuant to state and federal law	Increase translation staff, translate all information docs to align with the LEA-ELL population, purchase translation equipment, train staff, plan for literacy needs of parents.	All English language learners identified with disabilities, who are at risk of not reclassifying or not graduating.
Collaboration with family empowerment centers and other family support organizations.	Connect liaisons to CAC, P&I, Celebrate Families; parent education and experiential learning; work with IRC, Rockin' Our Disabilities, CAPTAIN, Moses Ministry, other.	Students with Autism and other disabilities, those subject to "Child-find", identified in dispro data, ELL, African Am. students and with chronic absenteeism.
Conduct voluntary alternative dispute resolution activities, including offering voluntary alternative dispute resolution for issues that are not resolved through the individualized education program process.	Promote SELPA and LEA ADR services, support resolution skills with training and coaching, develop internal systems of ADR procedures, increase staff for ADR services, train stake holders in IDEA, provide educational materials.	Students with disabilities, students with Autism, and those subject to "Child-find". Students identified in dispro data, students with Autism, ELL students, and students identifying as African American.
Partnership with family empowerment centers or other family support organizations, including by providing support to those organizations to assist in the activities specified in this subdivision to prevent and resolve disputes in a pupil-centered, collaborative, and equitable manner.	Create outreach teams, develop local parent centers and hire staff; build relationships and partner with local parent support groups: IRC, IEHP, Autism Society, CAPTAIN, Moses Ministries and other regional parent resource groups. Provide training: IDEA rights, collaboration, building positive relationships. Provide child-care and vary the time of activities.	Students with disabilities including Autism and those subject to "Child-find". Students identified in dispro. data, ELL students, students identifying as African American and LGBTQ.
Identify, and conduct outreach to, families who face language barriers and other challenges to participation in the special education process, and whose pupils have experienced significant disruption to their education as a result of the COVID-19 pandemic	Campaign with through multiple communication channels: social-media, video recordings, print, other. Provide transportation, incentives, food and other for activities to draw in parents. Create welcoming schools with empathy where parents are heard; staff is accessible.	Students with disabilities, with Autism, and those subject to "Child-find". Students identified in dispro. data, with Autism, ELL students, students identifying as African American, students, students with mental health needs and chronic absenteeism.
Other impacted areas (Identify the impacted area and the plan for using the funds)	Missing or late IEPs, assessments, supports services: provide additional staff, interns, coaches, lead teachers, subs, NPA staff, tutoring agencies, additional hours, other.	Students with outdated IEPs and assessments; students with need of make-up services, students not making progress towards goals.

Proposed Expenditures

Object Codes	ADR Allocation Funds (Expenditures)	Itemized Description and Justification
1. 1000–Certified Salaries	$800,000.00	Salary for certificated staff providing services directly related to LEA dispute prevention and resolution plans.
2. 2000–Classified Salaries	$65,000.00	Salary for clerical staff providing support to staff carrying out dispute prevention and resolution plans.
3. 3000–Employee Benefits	$318,512.00	Benefits for certificated and support staff.
4. 4000–Materials and Supplies (cannot exceed 10%)	$101,234.00	Office supplies and materials for trainings, staff meetings, and parent engagement activities.
5. 5000–Services and other operating costs	$400,000.00	Consultants, LEA participant stipends, and other services related to community outreach and the promotion of parent engagement.
6. Total Direct Costs (Total of 1 through 5)	**$1,684,746.00**	
7. 6000–Capital Outlay (cannot exceed 10% of allocation or $10,000 per purchase)	$0.00	
8. 7300–Indirect Costs CDE approved rate: 0.0785 (Enter 7.5% as 0.075)	$132,252.00	CDE approved 2021/22 indirect cost rate for San Bernardino County Superintendent of Schools.
9. Total Grant Budget (Total 6 through 8)	**$1,816,998.00**	

California Department of Education
Special Education Division

(Revised September 2021)

Learning Recovery Plan

Fiscal Year 2021–22

Due Date: **October 1, 2021**

As a condition of receiving funding, the special education local plan area shall, on or before October 1, 2021, work with its member local educational agencies to develop and submit a plan to the Superintendent of Public Instruction.

The requirement states the plan must include:

- how the special education local plan area and its member local educational agencies will implement the requirements;
- detailed proposed expenditure information broken down by eligible activity;
- the number, disabilities, and demographics of pupils proposed to be served.

If the SELPA has LEAs that are using their allocations in different ways due to the unique needs of the LEA, the SELPA submits a separate plan for LEAs that addresses their intent to use funds under one SELPA submission.

SELPA Information

SELPA Name: **Desert Mountain SELPA**

SELPA Code: 3601

Plan Description

Applicable LEAs for this Plan **Academy for Academic Excellence, Adelanto Elementary SD, Apple Valley USD, Baker Valley USD, Barstow USD, Bear Valley USD,**

Impacted Areas	Learning Recovery Services for Pupils with Disabilities Related to Impacts of Learning Resulting from COVID-19 School Disruptions (Including Objectives and Metrics that will be used to measure success)	Students Served by Proposed Plan
Additional Support and Services Needed to Address Identified Learning Needs	Transportation services before school, after school, and summer camps outside of ESY to get students to campuses for additional supports and services.	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard
Positive Behavior Supports	ABA or Psych led social skills groups offered before school, after school, Saturdays, or summer camps outside of ESY designated time	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard

Impacted Areas	Learning Recovery Services for Pupils with Disabilities Related to Impacts of Learning Resulting from COVID-19 School Disruptions (Including Objectives and Metrics that will be used to measure success)	Students Served by Proposed Plan
Assessing Learning and Academic Needs of Students	Hiring additional staff: TOSA(s), academic coach(es), interns, lead teachers, and tutoring agencies. Purchase iReady program for Math & ELA to target gaps in learning ⊞	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard subcategories ⊞
Social Emotional Needs	Hiring additional staff: school counselors, social workers, mental health clinicians - services, school psychologists, Tiered supports through MTSS framework Training: Trauma-Invested Practices, Youth Mental Health First Aid, Restorative ⊞	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard subcategories
High Quality and Instruction	UDL Training, Implementation, & Coaching Training on Evidence Based Practices, Implementation, and Coaching Expand training for early education teachers and paraeducators Orton Gillingham (ELA) and Singapore Math ⊞	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard subcategories
Supporting Students Return to In-Person Instruction	Family events at the district or site level - nights and weekends Parent training through parent support centers Hiring Community Outreach Liaison ⊞	TK - 12 students with disabilities, English learners, Homeless youth, Foster youth, and other California dashboard subcategories ⊞
Child Find	Parent training/education Hiring a Community Outreach Liaison Response to Intervention (RtI) Programs developed and implemented Multi-tiered Systems of Support (MTSS) ⊞	TK - 12 students with learning disabilities and general education students subject to "Child Find" regulations in order to meet Federal requirements of Free Appropriate Public ⊞
Assessing Students who are Waiting of Initial IEPs	Hiring additional qualified staff or contracting qualified personnel to provide psycho-education assessments and observations. Paying staff additional hours or contracted days outside their contract to hold IEPs, write IEPs/Psych reports, or assess ⊞	TK - 12 students with learning disabilities and general education students subject to "Child Find" regulations in order to meet Federal requirements of Free Appropriate Public ⊞
Complete Overdue IEPs	Hiring additional qualified staff or contracting qualified personnel to provide psycho-education assessments and observations. Paying staff additional hours or contracted days outside their contract to hold IEPs, write IEPs/Psych ⊞	TK - 12 students with learning disabilities and general education students subject to "Child Find" regulations in order to meet Federal requirements of Free Appropriate Public ⊞
Other Impacted Areas (Identify the impacted Area and the plan for using the funds)	Secondary Transition and graduation planning for students with disabilities age 15 to 22. Work-Based Learning(WBL) Placements Establish additional workability partners for students with disabilities transitioning out of ⊞	Students with disabilities ages 15 - 22 transitioning from high school to adulthood to provide supports and services through their transition and meeting the Federal requirement of Free ⊞

Implementation Timeline of Proposed Plan or Activities

Please describe your plan for implementation, including a timeline and milestones

It may take several years for full recovery of learning losses due to extended, repeated school closures, and traumatic events faced by students. The timeline will begin in September 2021 and will continue through September 2023. LEAs will address the following four (4) domains as we move through and address learning recovery. These domains may intertwine at times based on the need of each student. Domain 1: Leadership for rapid improvement; Prioritize improvement, Monitor goals, Customize supports. Domain 2: Talent management; Recruit, retain, and sustain talent, Target professional learning opportunities, Set performance expectations. Domain 3: Instructional Transformation; Diagnose student needs, Provide rigorous instruction, Remove barriers and provide access. Domain 4: Culture and Climate

Proposed Expenditures

Object Codes	Learning Recovery Funds (Expenditures)	Itemized Description and Justification
1. 1000–Certificated Salaries	$4,600,000.00	Salary for certificated staff providing services directly related to LEA dispute prevention and resolution plans.
2. 2000–Classified Salaries	$195,000.00	Salary for clerical staff providing support to staff carrying out dispute prevention and resolution plans.
3. 3000–Employee Benefits	$1,731,916.00	Benefits for certificated and support staff.
4. 4000–Materials and Supplies (cannot exceed 10%)	$300,000.00	Office supplies and materials for trainings, staff meetings, and parent engagement activities.
5. 5000–Services and other operating costs	$754,439.00	Consultants, LEA participant stipends, and other services related to community outreach and the promotion of parent engagement.
6. Total Direct Costs (Total of 1 through 5)	**$7,581,355.00**	
7. 6000–Capital Outlay (cannot exceed 10% of allocation or $10,000 per purchase)	$0.00	
8. 7300–Indirect Costs CDE approved rate: 0.0785 (Enter 7.5% as 0.075)	$595,136.00	CDE approved 2021/22 indirect cost rate for San Bernardino County Superintendent of Schools.
9. Total Grant Budget (Total 6 through 8)	**$8,176,491.00**	

Assurance of Matching Funds

I am providing assurances that this plan will meet the grant cash match requirement required by Learning Recovery Plan Grant. To meet the cash match requirement, the SELPA will create a SELPA-level grant match. For multi-district SELPA’s, the SELPA will collect/receive and review the grant match expenditure report for each member LEA.

These expenditure reports will be on file at the SELPA and will be made available upon CDE request. The grant match expenditure report will require the following items:

- Amount of grant allocation
- Amount of cash match
- List of expenditures for the amount (i.e. Purchase Order, Invoice, Payment Voucher, Journal Entry, Labor Report, etc.)
- Attestation or declaration that the amount qualified as a match for the purposes of the grant
- Agreement that the expenditures are subject to review

SELPA Name

SELPA Director Name

Date

Dispute Prevention and Dispute Resolution	
Total Allocation Resource 6536	1,816,998
Desert/Mountain SELPA Allocation	363,400
LEA Allocation	1,453,598

	Pupil Count	Percentage of Count	Allocated Amount
Academy for Academic Excellence	132	1%	13,139
Adelanto Elementary	1112	8%	110,690
Apple Valley Unified	1515	10%	150,805
Baker Valley Unified	16	0%	1,593
Barstow Unified	904	6%	89,985
Bear Valley Unified	308	2%	30,659
Excelsior Charter	236	2%	23,492
Excelsior Charter School Corona-Norco	6	0%	597
Health Sciences High and Middle College	98	1%	9,755
Helendale Elementary	134	1%	13,339
Hesperia Unified	2860	20%	284,687
Lucerne Valley Unified	129	1%	12,841
Needles Unified	121	1%	12,044
Norton Science and Language Academy	94	1%	9,357
Oro Grande	349	2%	34,740
San Bernardino County Office of Education	2204	15%	219,388
Silver Valley Unified	385	3%	38,323
Snowline Joint Unified	1055	7%	105,016
Trona Joint Unified	47	0%	4,678
Victor Elementary	1513	10%	150,606
Victor Valley Union High	1385	9%	137,864
	14603	100%	1,453,598

Dispute Prevention and Dispute Resolution	
Total Allocation Resource 6536	8,176,491
Desert/Mountain SELPA Allocation	1,635,298
LEA Allocation	6,541,193

	Pupil Count	Percentage of Count	Allocated Amount
Academy for Academic Excellence	132	1%	59,127
Adelanto Elementary	1112	8%	498,104
Apple Valley Unified	1515	10%	678,621
Baker Valley Unified	16	0%	7,167
Barstow Unified	904	6%	404,933
Bear Valley Unified	308	2%	137,964
Excelsior Charter	236	2%	105,713
Excelsior Charter School Corona-Norco	6	0%	2,688
Health Sciences High and Middle College	98	1%	43,898
Helendale Elementary	134	1%	60,023
Hesperia Unified	2860	20%	1,281,094
Lucerne Valley Unified	129	1%	57,784
Needles Unified	121	1%	54,200
Norton Science and Language Academy	94	1%	42,106
Oro Grande	349	2%	156,329
San Bernardino County Office of Education	2204	15%	987,248
Silver Valley Unified	385	3%	172,455
Snowline Joint Unified	1055	7%	472,571
Trona Joint Unified	47	0%	21,053
Victor Elementary	1513	10%	677,725
Victor Valley Union High	1385	9%	620,390
	14603	100%	6,541,193

Marina Gallegos

Subject: RE: ADR/SpEd Learning Recovery Grants

From: SELPA Mail-Q: Anjanette Pelletier <system@listserv.cc>
Sent: Friday, September 17, 2021 11:34 AM
To: Heidi Chavez <Heidi.Chavez@cahelp.org>
Subject: Fw: ADR/SpEd Learning Recovery Grants

CAUTION: This email originated from outside of the organization. Please do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello all

We have received a couple of really good questions, and for those who were confused, otherwise overwhelmed or not in attendance, Anthony and I thought this would be a good FAQ to share.

- During the school disruptions, LEAs used other funding sources (example general fund, other funds) to pay for supplemental activities. Can LEAs use these new funding to retroactively offset the supplemental costs that they incurred in the prior year (starting March 2020)?
-
- Is there a start date for spending these funds? I think the confusion is not having a start date on the grant.

Yes - you CAN use the funds for retroactive activities.

For SpEd Learning, as long as you are spending those dollars on new, supplemental programs and services, you can retroactively pay yourself back as long as the expense occurred during that March, 2020-September 1, 2021 window outlined. An example that came up during the meeting was an intersession or an added ESY program. Because intersessions and extra ESY (not the standard ESY) are supplemental, those would be eligible.

We are unclear, just yet, exactly how you will show your supplemental expenditures, but the intent is definitely there that you could claim those activities and expenditures if they meet the criteria as listed in the plans. Since we were told the match is the funds we received (and everyone seems to have received 100% of their funds, not 50% as we had anticipated) are matching funds to supplemental services/resources, and the expenditure reporting won't be until September 2023, then LEAs would merely have to show evidence that shows they were entitled to and used all of the received funds for services. They should not have to do anything to books or new year balances - but we will ask SSC to double check this and clarify.

Note: LEAs are saying their can adjust their books (adjustment to beginning balance or credit to revenue) if the State allowed them to use these new funds on prior year expenses.

We do want to make sure that every SELPA and LEA is doing a hard alignment to Equity considerations. Although some may have sufficient prior year expenditures to use up all or most of their funds, we really encourage everyone to consider future facing activities or supports that can also improve capacity, access, communication and outcomes for SWDs.

A lot of us had supplemental things that impacted very few students last year - but with these new funds we might be able to really make a difference in the future as well.

This Equity poster was shared with us - we recommend sharing with your LEAs as they think of equity focused activities they can consider as well.

Re: Start Date -

We believe you can start spending those dollars as soon as you have them and have agreed (locally) about how you are spending them…aligned to your plans of course. CDE will be looking to make sure that your expenses align with the action you have outlined your plan.

The validation tables for the new Resource Codes 6536 (dispute prevention) and 6537 (Learning Recovery) will go live on September 24. For many regions, this means that they cannot enter expenditures until the SACS software is updated - it could generate an error code if entered prior to that date. However, there are others who are willing to make a leap of faith in CDE and they are already allocating funds out to LEAs with a placeholder code that can be updated after September 24.

Expenditure matching to Service can go back to March 14 2020 through Sept 1, 2021 - the period of COVID impact outlined in the appropriation notification.

Hope that helps.

Anjanette and Anthony

SAN MATEO
COUNTY
SELPA

San Mateo County Office of Education

Anjanette Pelletier

Associate Superintendent

San Mateo County SELPA

650.802.5465-Phone

510.909.7373 - Cell

apelletier@smcoe.org

101 Twin Dolphin Drive

Redwood City, CA 94065

DMCC
Desert / Mountain Children's Center

Desert / Mountain Children's Center
17800 Highway 18
Apple Valley, CA 92307-1219

P 760-552-6700
F 760-946-0819
W www.dmchildrenscenter.org

MEMORANDUM

DATE: September 22, 2021

TO: Special Education Directors

FROM: Linda Llamas, Director

SUBJECT: Desert/Mountain Children's Center Client Reports

Attached are the opened and closed cases for the following services:

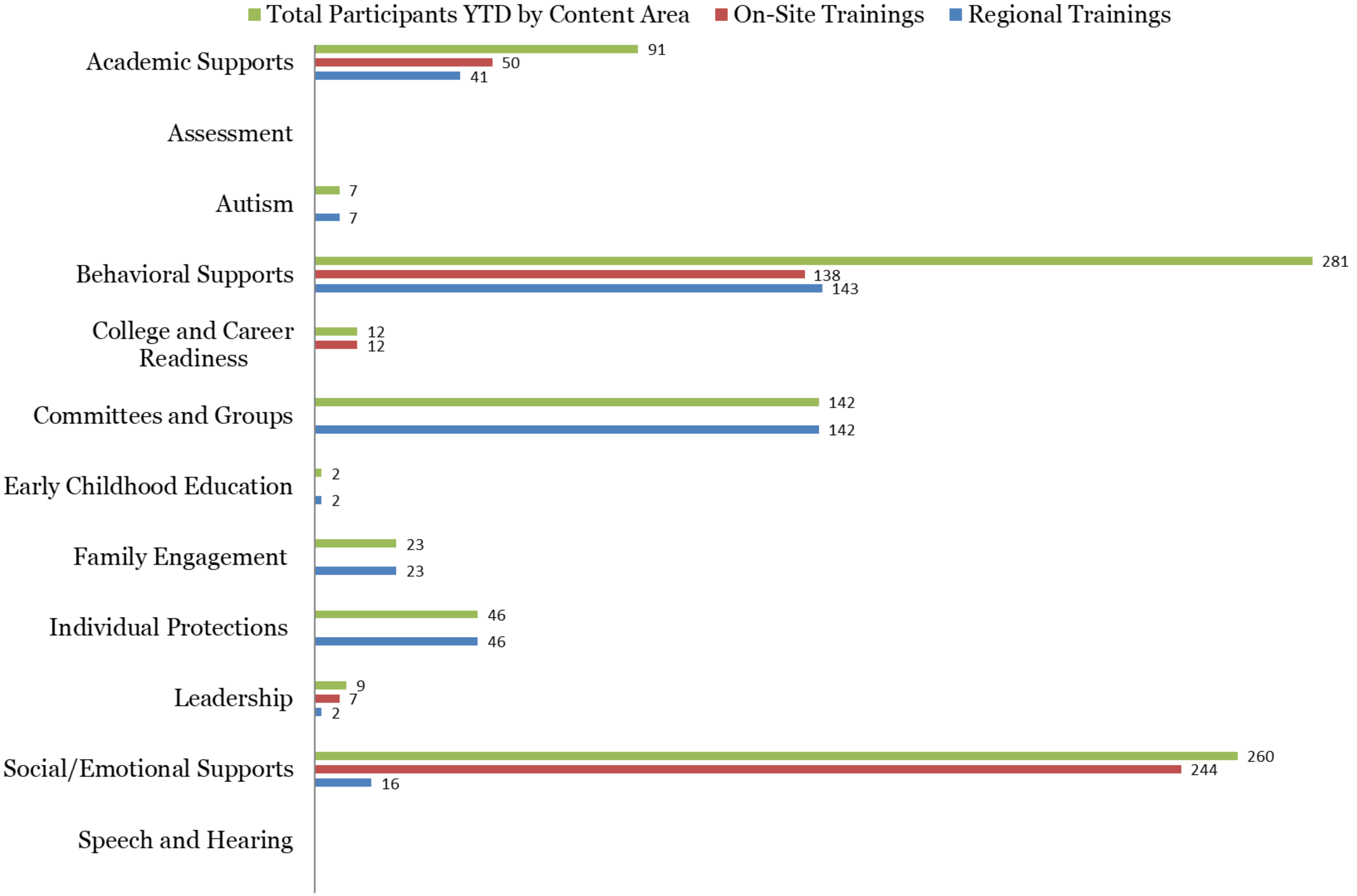
- Screening, Assessment, Referral and Treatment (SART)
- Early Identification Intervention Services (EIIS)
- School-Age Treatment Services (SATS)
- Student Assistance Program (SAP)
- Speech and occupational therapy

If you should have any questions, please contact me at (760) 955-3606 or by email at linda.llamas@cahelp.org

D/M SELPA PROFESSIONAL LEARNING PARTICIPATION SUMMARY

JULY & AUGUST 2021 - 873 PARTICIPANTS

873 YEAR-TO-DATE PARTICIPANTS



Desert/Mountain SELPA
Due Process Summary
July 1, 2021 - September 24, 2021

DISTRICT													CASE ACTIVITY FOR CURRENT YEAR				
	11/12	12/13	13/14	14/15	15/16	16/17	17/18	18/19	19/20	20/21	21-22	Total		D /W	Resolution	Mediation	Settled	Hearing
Adelanto SD	0	3	6	5.5	2.5	5	3	3.5	3	3.5	0	35		0	0	0	0	0
Apple Valley USD	0	0	2	1	1.5	1.5	0	3.5	10	5	1	25.5		1	0	0	0	0
Baker USD	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0
Barstow USD	0	0	0	0	1	3.5	0	2	0	1	0	7.5		0	0	0	0	0
Bear Valley USD	1	0	0	0	0	1	2	0	0	1	0	5		0	0	0	0	0
Helendale SD	0	0	0	0	0	0	1	0	0	0	0	1		0	0	0	0	0
Hesperia USD	5.5	4	3	5	7.5	7	6	7	17.5	7	2	71.5		0	0	1	1	0
Lucerne Valley USD	0	1	2	1	1	2	0	1.5	0	0	0	8.5		0	0	0	0	0
Needles USD	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0
Oro Grande SD	0	0	0	0	0	0	0	0	2	0	0	2		0	0	0	0	0
Silver Valley USD	1	0	0	0	0	0	0	0	0	0	0	1		0	0	0	0	0
Snowline USD	2	1	1	5	4.5	6.5	2	8.5	7	2	0	39.5		0	0	0	0	0
Trona USD	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0
Victor Elementary SD	1	1	4.33	3.33	1.83	2.5	6.5	0	7	1	1	29.49		0	0	0	1	0
Victor Valley Union High SD	2	4	3.33	4.3	7.83	4	4	8.5	6.5	10	1	55.46		0	1	0	0	0
Academy for Academic Excellenc	0	0	4	2	0	1	2	1	1	1	0	12		0	0	0	0	0
CA Charter Academy	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0
Desert/Mountain OPS	0.5	1	1.33	0.83	4.33	3	1.5	3	2	1	0	18.49		0	0	0	0	0
Excelsior Education Center	0	0	0	0	0	0	0	0.5	2	0	0	2.5		0	0	0	0	0
Health Sciences HS & MS	0	0	0	0	0	0	0	1	1	0	0	2		0	0	0	0	0
SELPA-WIDE TOTALS	**13**	**15**	**26.99**	**27.96**	**31.99**	**37**	**28**	**40**	**59**	**32.5**	**5**	**316.44**		**1**	**1**	**1**	**2**	**0**

Districts showing a value of .50 above indicates that the district is a co-respondent with another district.

*Number accounts for High Tech High but has exited from CAHELP. Actual count for 2019-20 is 67.

Desert/Mountain SELPA
Due Process Activity Summary
July 1, 2021–September 24, 2021

LEA Case Number	Issue(s)	Date Filed	Resolution Scheduled	Mediation Scheduled	Pre-Hearing Conference	Due Process Hearing	Status
1. VVUHSD Case No. 2021070206	LEA filed on parent for permission to assess, pursuant to assessment plan of 3-19-21	7/7/21	7/26/21		~~7/26/2021~~ 9/13/21	~~08/03 - 05/21~~ 9/21-23/21	Filing was necessary because the parent filing of 10/20 was withdrwan and left with open IEP's and lack of student attendance. 7/26/21 Continuance granted for parent to obtain attorney.
2. Victor Elem SD Case No. 2021070710	Failure to provide FAPE 1. Program 2. Speech/Lang. 3. Appropriate Assessment	7/21/2021	8/6/2021	~~9/7/2021~~	~~10/29/2021~~	~~9/14-16/21~~	**Mediation - Settlement Agreement** 1. IEE - (Sp & Lang and Psycho ed) 2. SP & Lang (2W x 20 min) individual therapy added to IEP 3. Comp Ed (academic, SP/Lang, OT contingent on results) 4. 1:1 until assessments completed not stay put **Settlement Agreement** **CLOSED**
3. Hesperia USD Case No. 2021070965	Failure to provide FAPE 1. Communication 2. Academics 3. Behavioral management	7/29/2021	8/5/2021			~~9/21-23/21~~	**Full execution of settlement agreement on 8/11/2021 -** 1. Conduct Assessments: Suppleemntal Speech and Central Auditory Processing. 2. 1:1 instructional assistance through 12/17/2021 until TISA is reviewed. 3. Amend IEP: Speech 4M/30 min group and 4M/30 min individual. 4. Comp Ed (Speech and Lang). 5. Reimburse parents for intensive reading services. **Settlement Agreement** **CLOSED**

Desert/Mountain SELPA
Due Process Activity Summary
July 1, 2021–September 24, 2021

4. Hesperia USD Case No. 2021080484	Denial of FAPE 1. Student not making progress. 2. Failed to provide appropriate program.	8/17/2021	8/30/2021		10/4/2021	10/12 - 10/14, 2021	Resolution Negotiations in Progress.
5. Apple Valley USD Case No. 2021090257	AVUSD filed to defend placement.	9/9/2021					Parent moved and withdrew complaint. **CLOSED**

Desert /Mountain SELPA
Legal Expense Summary
As Reported at Steering September 24, 2021

2000-2001	$39,301.51
2001-2002	$97,094.90
2002-2003	$37,695.13
2003-2004	$100,013.02
2004-2005	$136,514.09
2005-2006	$191,605.08
2006-2007	$140,793.00
2007-2008	$171,614.04
2008-2009	$263,390.71
2009-2010	$114,076.96
2010-2011	$293,578.50
2011-2012	$567,958.10
2012-2013	$321,646.04
2013-2014	$250,372.65
2014-2015	$297,277.76
2015-2016	$204,756.26
2016-2017	$233,130.03
2017-2018	$247,459.52
2018-2019	$314,479.71
2019-2020	$475,930.79
2020-2021	$354,582.16
2021-2022	$17,446.66

TRIAGE COLLABORATION MEETING

AUGUST 6TH, 2021

UCLA Evaluation Team and County Partners

MHSOAC
Mental Health Services
Oversight & Accountability Commission

UCLA Semel Institute for Neuroscience & Human Behavior
Health Services and Society

UCLA TEAM AND PARTNERS

Bonnie Zima, MD, MPH
Principal Investigator

Roya Ijadi-Maghsoodi, MD, MSHPM
Co-Investigator

Corey O'Malley, PhD
Co-Investigator

Lily Zhang, MS
Statistician

Elizabeth Bromley, MD, PhD
Co-Investigator

Elyse Tascione, MA
Project Manager

Alanna Montero, BS
Research Associate

Jet DeKruse, LMFT
Senior Program Manager

Kenneth Wells, MD, MPH
Co-Investigator

DEDICATION

Richard Van Horn (9/24/39 - 6/15/21)

- Revolutionized the nation’s and California’s approach to mental health.
- Helped develop the Mental Health Services Act.
- Key stakeholder and policy advisor for the SB-82/833 evaluation.

CHILD/YOUTH & SCHOOL-COUNTY FORMATIVE EVALUATION

Formative Evaluation

Process

Stakeholder perception

Community Partnered Approach

Stakeholder Advisory Board

Early interviews and meetings with program leads

Mixed Methods Design

Qualitative Interviews
- Stakeholder groups in each program
- Every 6 months starting in 2019

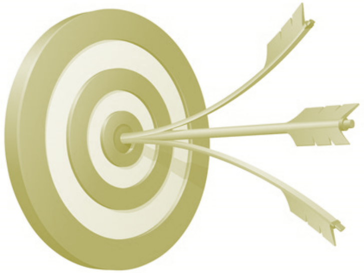
Quantitative Surveys
- Services delivered
- Clients served
- Program implementation

SPECIFIC AIMS

1. **To describe and assess selected program implementation activities, processes, and outcomes across program phases.**

   - Subaim 1a. To examine variation in implementation by program type, region, new or augmenting, urban or rural, and relevant sociodemographics and contextual factors.

   - Subaim 1b. To understand the ongoing influence of the COVID-19 pandemic on implementation.

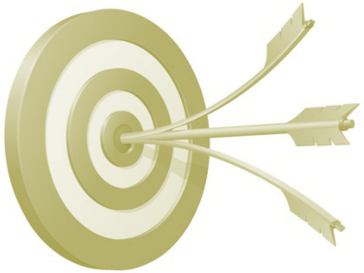


SPECIFIC AIMS

2. **Identify facilitators and barriers to program implementation across program phases.**

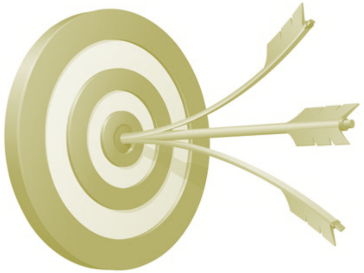
    - Subaim 2a. Examine variation in facilitators and barriers to implementation by program type and context.

    - Subaim 2b. Understand influences of COVID-19 on existing facilitators and barriers to implementation.



SPECIFIC AIMS

3. **Provide lessons learned and evidence-based recommendations for future program implementation based on analyses for Aims 1 and 2.**



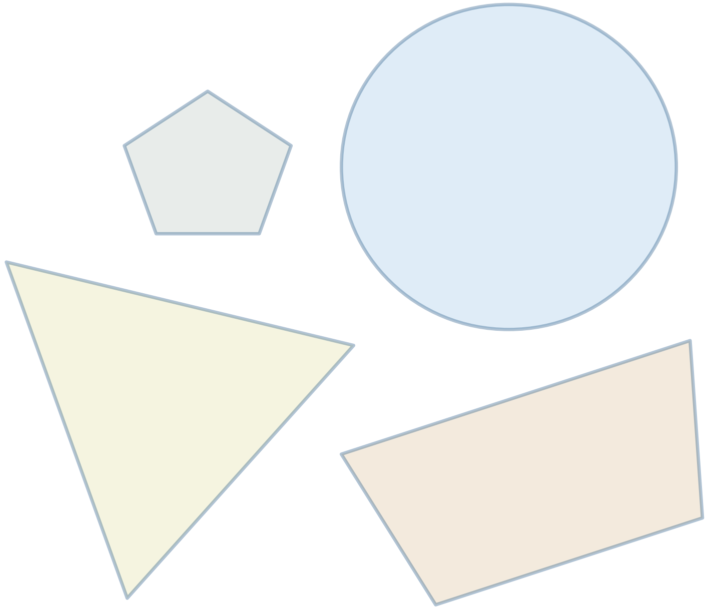
PRELIMINARY FINDINGS

DATA SOURCES

- First four rounds of stakeholder **interviews** with Phase 1 programs
- Early returns from **program surveys**
- Data and insights from **stakeholder engagement activities**

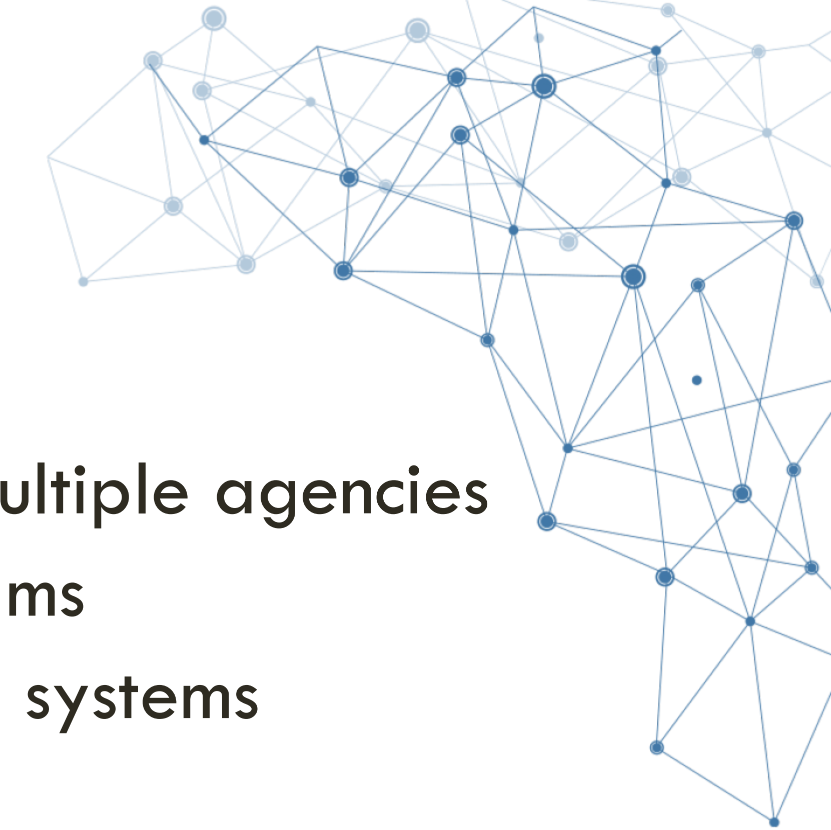
PROGRAM FEATURES

Heterogeneity



Care process target areas:

- health prevention (n=6; 43%)
- early intervention (n=6; 43%)
- crisis services (n=14; 100%)
- treatment (n=6; 50%)
- referral (n=11; 86%)
- care coordination (n=9; 71%)
- community outreach (n=6; 50%)



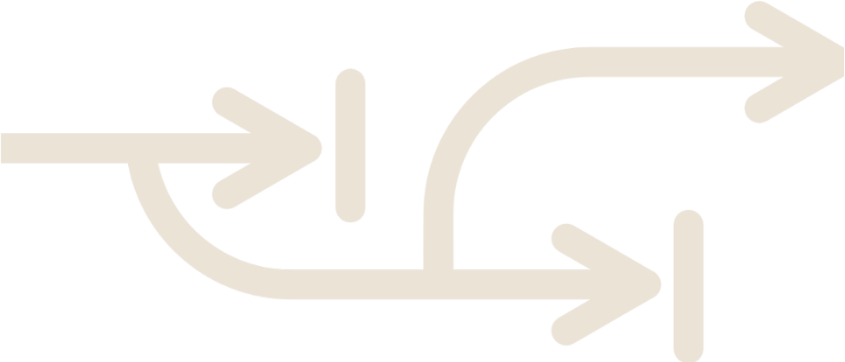
PROGRAM FEATURES

Complexity

- Partnerships with multiple agencies
- Several units or teams
- Multiple regulatory systems

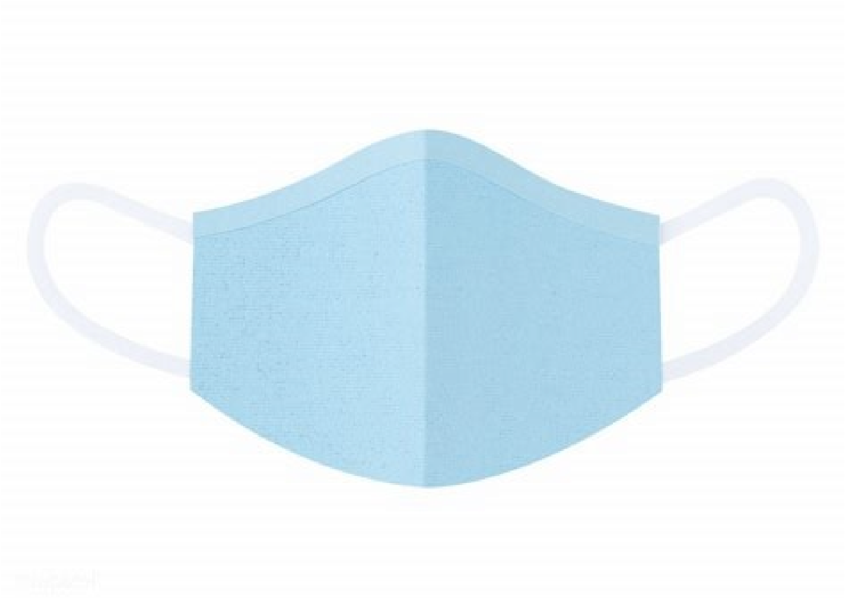
Adaptability

- Allowed most programs to be executed as broadly intended
- All but 2 program leads agreed their programs had been carried out as intended and described in their proposal (n=12; 86%)



FACTORS AFFECTING IMPLEMENTATION

COVID-19 Pandemic



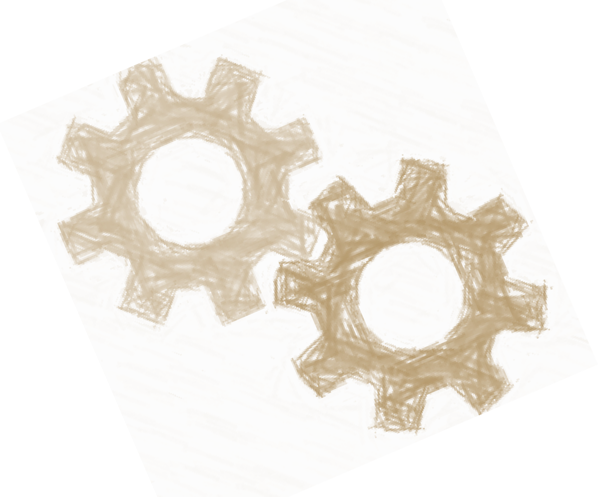
- Changes in demand and acuity
- Refocus on basic and social needs, equity
- Constant innovation:
  - Rapid but mixed uptake of telehealth
  - New engagement strategies
  - New methods for detecting need

FACTORS AFFECTING IMPLEMENTATION

Staff and Leadership Engagement

- Positive attitudes about programs, passion and enthusiasm for their work, many go above and beyond
- Leads in all (n=14) programs agreed that their program was actively supported by their organization’s leadership.
- Programs housed in external organizations have varying experiences with prioritization and leadership engagement.

FACTORS AFFECTING IMPLEMENTATION



Staff Turnover

Impacts

- Change in the range or quality of services (n=6; 43%)
- Increase in staff case load (n=4; 28.6%)
- Reduction in staff morale (n=4; 28.6%)
- Loss of professional expertise (n=4; 28.6%)
- Loss of institutional knowledge (n=4; 28.6%)

Contributors

- Stresses of crisis work
- Compensation
- Structure and workload of some roles

Recruitment Challenges

- Particularly for smaller, rural, and partnered programs

FACTORS AFFECTING IMPLEMENTATION

Resources

- Variation in amount of Triage Grant funding, adaptation to budget cuts

- “Patchworking” to combine multiple funding and revenue sources

- Variable access to critical community resources for youth mental health

FACTORS AFFECTING IMPLEMENTATION

Sustainability

Planning

- 9 of 14 programs have a sustainability plan in place.

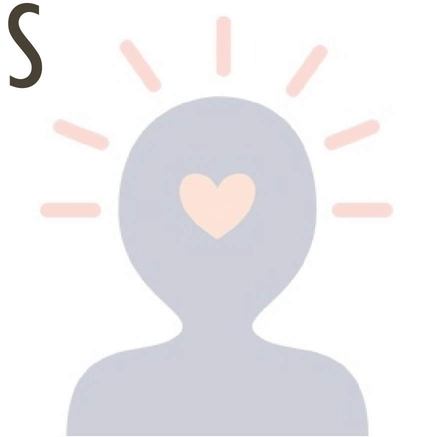
Major Sources Considered

- Medi-Cal (n=11)
- MHSA funds (n=8)
- County funds (n=5)
- School district funds (n=5)

Challenges

- Medi-Cal not suitable for all care processes, penetration varies
- Many options not predictable or long-term

ADDRESSING TRIAGE GRANT PROGRAM GOALS



Expand crisis prevention and treatment services

Interviews

- Filling gaps in service systems and settings
- Identifying and responding to unmet community needs
- Engaging in partnerships for improved linkage and utilization

Program Lead Survey

- Most program leads agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Increase client and student wellness

Interviews

- Providing crisis services that are targeted to the specific mental health needs of their communities

Program Lead Survey

- Most program leads agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Decrease unnecessary hospitalizations and associated costs
(Child/Youth Grant Goal)

Interviews

- Providing preventative care
- Providing early intervention services
- Providing crisis services that improve quality of crisis response to de-escalate
- Addressing unnecessary use of emergency departments for mental health crises

Program Lead Survey

- Most program leads agreed that their program is suitable for and effective at this goal

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Reduce unnecessary law enforcement involvement and costs
(Child/Youth Grant Goal)

Interviews

- Preventing need for law enforcement involvement
- Providing alternatives to law enforcement involvement
- Improving law enforcement's understanding of mental health
- Providing options for co-response with law enforcement to encourage de-escalation

Program Lead Survey

- Most program leads agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Increase access to a continuum of mental health services and supports through school-community partnerships (School-County Grant Goal)

Interviews

- Providing services that did not previously exist in schools
- Increasing reach and intensity of existing services at schools
- Utilizing a partnered approach to offer greater depth of care

Program Lead Survey

- All School-County program leads (n=4; 100%) agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Develop coordinated and effective crisis response systems on school campuses when mental health crises arise (School-County Grant Goal)

Interviews

- Supporting development of new referral and tracking systems
- Ensuring existing systems are used appropriately and effectively
- Using referral systems to ensure major crises in schools are addressed in a timely and appropriate manner

Program Lead Survey

- All School-County program leads (n=4; 100%) agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Engage parents and caregivers in supporting their child's social-emotional development and building family resilience
(School-County Grant Goal)

Interviews

- Providing outreach, training, support, and resources to parents/caregivers beyond immediate interactions during discrete crises

Program Lead Survey

- All School-County program leads (n=4; 100%) agreed that their program is suitable for and effective at this goal.

ADDRESSING TRIAGE GRANT PROGRAM GOALS

Reduce the number of children placed in special education for emotional disturbance or removed from school and community due to their mental health needs (School-County Grant Goal)

Interviews

- Tracking special education utilization and school discipline
- Working with school staff in special education to improve knowledge and access to resources
- Working with school staff to improve systems and cultures in school discipline

Program Lead Survey

- Some School-County program leads agreed that their program is suitable for and effective at this goal

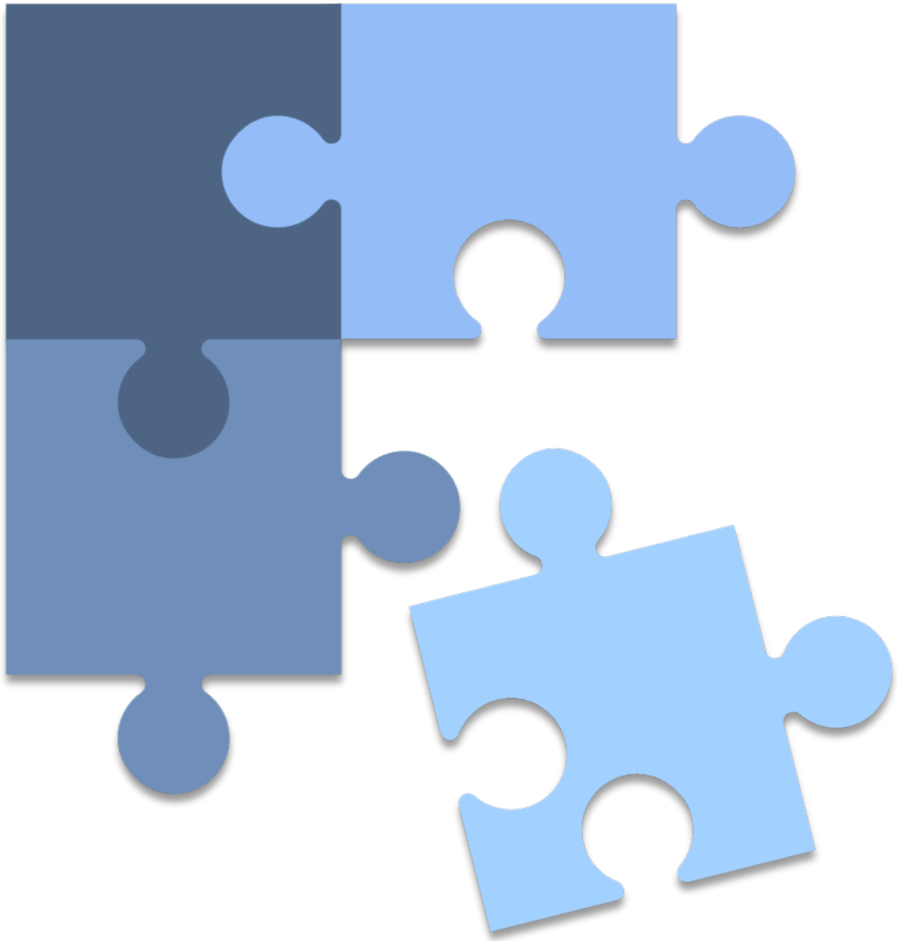
EARLY LESSONS LEARNED

1. Programs make unique contributions to youth mental health services in their counties and communities, aimed at:
   - **increasing access** by filling gaps and building partnerships within and between sectors.
   - **improving quality** by providing age-appropriate triage services delivered by specialists.
   - **expanding services** in schools by introducing new services and integrating mental health into the school culture.
2. These same contributions can also make them challenging to deliver, especially for programs delivering many types of services, organized into multiple teams, or partnered with organizations across sectors.

EARLY LESSONS LEARNED

3. Programs demonstrate that **adaptability** and **innovation** are critical to executing programs despite these challenges.
4. Programs may also benefit from **support** that targets their unique contributions and addresses challenges in delivering crisis services, such as support for:
   - building and sustaining **partnerships**, especially across sectors.
   - mitigating **staff turnover.**
   - securing necessary **funding and resources.**

THANK YOU FOR YOUR CONTINUED PARTNERSHIP!



Professional Learning Opportunity | CAHELP

Transition Partnership Program (TPP) Beginning of the Year

At the TPP Beginning-of-the-Year Meeting, the Desert/ Mountain SELPA Career Technical Education Team invites Teri Black, a special education teacher from Adelanto High School, and Thomas McMullen, a representative from Nepris, to present instruction that might be considered a substitute for Academic Innovations.

Ms. Black's presentation will introduce participants to digitalized transition activities by using an electronic portfolio. The lessons will guide participants through career exploration and employment activities tailored to each student's specific needs in a structured but versatile setting.

Mr. McMullen, a representative from Nepris, will connect educators and learners with a network of industry professionals virtually, bringing real-world relevance and career exposure to all students. Nepris also provides a skills-based volunteering platform for organizations to extend education outreach and build their brand among the future workforce.

Contract goals will be reviewed with TPP and WAI staff, and participants will have an opportunity to discuss workshops and paid work experience opportunities for the 2021/22 school year.

Presented By

Adrienne Shepherd, Program Manager

Date

September 28, 2021

Time

8:30 a.m - 1:00 p.m

Location

Virtual training, a link will be sent to each participant prior to the training date. **This training may be recorded.**

Audience

Transition case technicians, job developers, TPP teachers, TPP instructional assistants, rehabilitation counselors, TPP job coaches, and secondary special education teachers.

Cost

There is no fee for this training.

Registration

Please register online at:
https://sbcss.k12oms.org/52-200289

Special Accommodations

Please submit any special accommodation requests at least fifteen working days prior to the training by notating your request when registering.

8.9 Compliance Update

Verbal report, no materials

8.10 Nonpublic School/Nonpublic Agency Update

Verbal report, no materials

DMSELPA

Desert/Mountain Special Education Local Plan Area
17800 Highway 18
Apple Valley, CA 92307-1219

P 760-552-6700
F 760-242-5363
W www.dmselpa.org

MEMORANDUM

Date September 14, 2021

To: Directors of Special Education

From: Peggy Dunn, Program Manager

Subject: **Occupational and Physical Therapy Reports**

Attached are the occupational and physical therapy Referral Status, and Current Students Direct Services reports by district.

If you have any questions concerning either report, please contact me at (760) 955-3568 at peggy.dunn@cahelp.org

Desert Mountain SELPA

2021-2022 Non-Public School Placement Report

	July				August				September				October				November				December			
	District Placed	Residential Placed	LCI/Foster Placed	TOTAL	District Placed	Residential Placed	LCI/Foster Placed	TOTAL	District Placed	Residential Placed	LCI/Foster Placed	TOTAL	District Placed	Residential Placed	LCI/Foster Placed	TOTAL	District Placed	Residential Placed	LCI/Foster Placed	TOTAL	District Placed	Residential Placed	LCI/Foster Placed	TOTAL
Adelanto	3			3	3			3	2			2												
Apple Valley	17	1	5	23	17	1	5	23	20	1	7	28												
Baker																								
Barstow	5	1		6	5	1		6	5	1		6												
Bear Valley																								
Helendale																								
Hesperia	17			17	17			17	15			15												
High Tech High																								
Lucerne Valley									1			1												
Needles																								
Oro Grande																								
Silver Valley																								
Snowline	11	1		12	11	1		12	11			11												
Trona																								
Victor Elem	8		1	9	8		1	9	6		1	7												
VVUHSD	22	1	2	25	21	1	2	24	20	2	2	24												
TOTALS	**83**	**4**	**8**	**95**	**82**	**4**	**8**	**94**	**80**	**4**	**10**	**94**												
2020-21 Totals	78	6	16	100	69	6	15	90	81	4	18	103	80	4	18	102	80	4	17	101	83	4	17	104
2019-20 Totals	80	11	19	110	74	11	16	101	73	8	17	98	74	8	19	101	75	8	19	102	75	8	19	102
2018-19 Totals	56	18	10	84	63	15	10	88	66	15	13	94	76	13	15	103	81	12	17	110	82	12	17	111
2017-18 Totals	32	17	5	54	30	16	5	51	33	16	6	55	30	17	5	51	21	17	6	44	23	17	5	45
2016-17 Totals	88	21	15	124	79	20	13	112	79	17	14	110	87	17	14	118	90	19	14	123	90	21	14	125

California Association of Health and Education Linked Professions

Upcoming Trainings

Date/Time	Event	Location
10/27/2021 1:00 PM - 3:30 PM	RESTORATIVE PRACTICES OVERVIEW	VIRTUAL
10/27/2021 2:30 PM - 4:30 PM	STRUCTURED LITERACY WITH ORTON-GILLINGHAM: FOUNDATIONAL	VIRTUAL
10/29/2021 2:00 PM - 3:00 PM	FAMILY FUN DAYS	VIRTUAL/DMESC
11/1/2021 -	Forms and Facts 101 (Self-paced course)	Virtual/self-paced
11/1/2021 -	Legally Compliant IEP present levels of performance (plops), goals, and educational benefit (self-paced course)	Virtual/self-paced
11/1/2021 -	Prior written notice (self-paced course)	Virtual/self-paced
11/2/2021 2:00 PM - 4:00 PM	THE WHAT, WHY, AND HOW OF IEP MEETING NOTES	VIRTUAL
11/3/2021 2:30 PM - 4:30 PM	AUTISM INTRODUCTION AND CONNECTION TO OUR PRACTICES	VIRTUAL
11/4/2021 2:30 PM - 4:00 PM	CRISIS PREVENTION INSTITUTE (CPI) FLEX-BLENDED LEARNING	VIRTUAL
11/9/2021 8:00 AM - 10:00 A	FOLLOW UP TO THE TPP BEGINNING OF THE YEAR MEETING	VIRTUAL

Upcoming Trainings

Date/Time	Event	Location
11/9/2021 2:00 PM - 4:00 PM	THE ART OF FACILITATING IEP MEETINGS	VIRTUAL
11/9/2021 9:00 AM - 10:30 A	WEBIEP AM QUESTION AND ANSWER SESSION	VIRTUAL
11/10/2021 2:00 PM - 3:30 PM	LIFE AND WORK BALANCE: CARING, CONNECTING, AND CELEBRATING	VIRTUAL
11/10/2021 2:30 PM - 4:30 PM	STRUCTURED LITERACY WITH ORTON-GILLINGHAM: ADVANCED	VIRTUAL
11/10/2021 2:00 PM - 3:30 PM	WEBIEP PM QUESTION AND ANSWER SESSION	VIRTUAL
11/10/2021 8:00 AM - 2:00 PM	YOUTH MENTAL HEALTH FIRST AID	VIRTUAL
11/17/2021 10:00 A - 11:30 A	REAL TALK…PARENT-TO-PARENT GROUP CHATS	VIRTUAL/DMESC
11/17/2021 12:30 PM - 4:00 PM	UNDERSTANDING GRIEF AND LOSS WITH CHILDREN AND ADOLESCENCE	DMESC
11/19/2021 2:00 PM - 3:00 PM	FAMILY FUN DAYS	VIRTUAL/DMESC
11/30/2021 1:30 PM - 4:00 PM	TISA: DETERMINING THE NEED AND WORKING EFFECTIVELY WITH INTENSIVE SUPPORTS	ONLINE

Date/Time	Event	Location
12/1/2021 -	Forms and Facts 101 (self-paced course)	Virtual/self-paced
12/1/2021 -	Legally Compliant IEP present levels of performance (plops), goals, and educational benefit (self-paced course)	Virtual/self-paced
12/1/2021 -	Prior written notice (self-paced course)	Virtual/self-paced
12/2/2021 9:00 AM - 10:30 A	WEBIEP AM QUESTION AND ANSWER SESSION	VIRTUAL
12/2/2021 2:00 PM - 3:30 PM	WEBIEP PM QUESTION AND ANSWER SESSION	VIRTUAL
12/7/2021 1:00 PM - 4:00 PM	UNIVERSAL SCREENER OVERVIEW	VIRTUAL
12/7/2021 2:00 PM - 3:30 PM	WEBEIP PM QUESTION AND ANSWER SESSION	VIRTUAL
12/8/2021 8:30 AM - 12:30 PM	BASIC RESTORATIVE PRACTICES AND USING CIRCLES EFFECTIVELY	VIRTUAL
12/8/2021 2:30 PM - 4:30 PM	ORTON-GILLINGHAM APPLICATION CHECK-IN	VIRTUAL
12/8/2021 8:00 AM - 2:00 PM	YOUTH MENTAL HEALTH FIRST AID	VIRTUAL

Date/Time	Event	Location
12/17/2021 2:00 PM - 3:00 PM	FAMILY FUN DAYS	VIRTUAL/DMESC

Professional Learning Opportunity | CAHELP

A new collaborative group!

All You Need Is Love: The Behavioral Collaborative

Presented By

Renee Garcia, Program Specialist
and Derek Hale, School Psychologist

Date

October 6, 2021
December 8, 2021
March 16, 2022

Time

3:00 - 4:00 p.m.

Cost

Free

Description

The Behavioral Collaborative group will meet three times per year virtually to develop skills and interventions for students with behavioral concerns across all tiers. Come network with other teachers and paras to develop strategies for challenging behaviors of students with varying disabilities.

Registration

Please register online at:

10/06/21
https://sbcss.k12oms.org/52-209399

12/08/21
https://sbcss.k12oms.org/52-209400

03/16/22
https://sbcss.k12oms.org/52-209401

Audience

General education teachers, special education teachers, and paraprofessionals.

Special Accommodation

Please submit any special accommodation requests at least fifteen working days prior to the training by notating your request when registering.

Location

Virtual training, a link will be sent to each participant prior to the training date.

Get in **Touch**

Address : 17800 Highway 18, Apple Valley, CA 92307
Phone : (760) 955-3573
Email : judith.loera@cahelp.org
Website : www.cahelp.org

Professional
Learning Opportunity | CAHELP

De-Escalation Strategies for Educators

Presented By

Danielle Cote,
Program Specialist

Date

October 12, 2021

Time

2:30 - 4:00 p.m.

Description

This course stresses the importance of focusing on prevention and early recognition of factors that may lead to escalation of student behavior. Topics will include self-care, precipitating factors, rational detachment, values of staff members and organizations, non-verbal communication, para-verbal communication, verbal communication, crisis development and the verbal de-escalation continuum.

Location

Virtual, a link will be sent to each participant prior to the training.

Audience

Special education teachers, paraprofessionals, site administrators, school psychologists, and general education teachers.

Cost

Desert/Mountain SELPA and Charter SELPA Members $0.00
Non-member participants $25.00

Special Accommodation

Please submit any special accommodation requests at least fifteen working days prior to the training by notating your request when registering.

Registration

Please register online at:
https://sbcss.k12oms.org/52-203209

Get in **Touch**

Address : 17800 Highway 18, Apple Valley, CA 92307
Phone : (760) 955-3559
Email : Jennifer.Holbrook@cahelp.org
Website : www.cahelp.org