SOUTHWEST
HEALTH & HUMAN
SERVICES

Southwest Health and Human Services
Board Agenda
Wednesday, June 15, 2016
Public Health Conference Rooms
Government Center, 2nd Floor
Marshall
9:00 a.m.

HUMAN SERVICES

A. Call to order

B. Pledge of Allegiance

C. Consent Agenda
   1. Amend/Approval of Agenda
   2. Identification of Conflict of Interest
   3. Approval of 05/18/16 board minutes

D. Financial

E. Caseload

	05/16	04/16	03/16
Social Service	3,680	3,697	3,647
Licensing	471	483	483
Out-of-Home Placements	171	173	169
Income Maintenance	12,447	12,503	12,527
Child Support Cases	3,356	3,360	3,329
Child Support Collections	$869,242	$892,307	$927,144
Non IV-D Collections	$38,367	$75,071	$92,083

F. Decision Items
   1.

G. Discussion/Information
   1. Success story – Mariah McCloud, Social Worker (CPS)

COMMUNITY HEALTH

H. Call to order

I. Consent Agenda
   1. Amend/Approval of Agenda
   2. Identification of Conflict of Interest
   3. Approval of 05/18/16 board minutes

J. Financial

K. Caseload

	05/16	04/16	03/16
WIC		2315	2324
Family Home Visiting	52	48	47
PCA Assessments	28	20	21
Managed Care	284	274	262
Dental Varnishing	107	97	126
Refugee Health	5	1	7
Latent TB Medication Distribution	30	27	24

L. Decision Items
   1.

M. Discussion/Information
   1. PHEP update – Anna Snyder
   2. HIPAA – Carol Biren
   3. Murray County Tobacco Ordinance/CIA Ordinance

GOVERNING BOARD

N. Call to order

0. Consent Agenda
   1. Amend/Approval of Agenda
   2. Identification of Conflict of Interest
   3. Approval of 05/18/16 board minutes

P. Financial

Q. Employee Recognition
   - Mariah McCloud, 1 year, Social Worker (CPS), Marshall
   - Diana Meaden, 1 year, Social Worker, Slayton
   - Jill Toering, 1 year, Social Worker, Luverne
   - Connie Seaman, 1 year, Accounting Technician, Marshall
   - Josh Varpness, 1 year, Child Support Officer, Marshall
   - Anna Snyder, 1 year, Public Health Educator, Luverne
   - Marge Pankonen, 25 years, Child Support Officer, Pipestone
   - Marie Meyers, 30 years, Nursing Supervisor, Redwood Falls

GOVERNING BOARD (cont.)

R. Decision Items

1. Arnold Siyapche, Information Technology Specialist, completion of 12 month probationary period, 1% salary increase, effective 07/06/16
2. Lisa Luckhardt, Social Worker, completion of 12 month probationary period, 1% salary increase, effective 07/06/16
3. Justine Heinis, Social Worker (CPS), probationary appointment (12 months), $40,660.00 annual, effective 05/31/16
4. Nicole Berry, Social Worker (CPS), probationary appointment (12 months), $40,660.00 annual, effective 06/06/16
5. Angela Frisk, Social Worker, probationary appointment (12 months), $42,500.00 annual, effective 07/11/16
6. Kami Parker, promotional appointment – Office Support Specialist to Child Support Officer, $17.36 per hour, effective 06/06/16
7. Alyssa Sorensen, promotional appointment – Office Support Specialist to Eligibility Worker, $17.14 per hour, effective 06/27/16
8. Sarah Kirchner, promotional appointment – Collections Officer to Fiscal Manager, $55,500.00 annual, effective 05/31/16
9. Tammy Groen, Social Worker (CPS), resignation, effective 06/24/16
10. Clara Sik, Eligibility Worker, retirement, effective 06/30/16
11. Amy Herigon, leave without pay request
12. Request for Case Aide
13. Request for Sanitarian
14. Personnel Policy Number 22 – Social Media Policy
15. Administrative Policy Number 8 – Disaster Recovery Plan
16. Administrative Policy Number 9 – Physical and Technical Safeguards
17. Administrative Policy Number 10 – LAN, E-Mail, Internet Access, and Personal Computing Equipment
18. Administrative Policy Number 14 – Health Care Insurance Portability & Accountability Act (HIPAA)
19. Administrative Policy Number 18 – Passwords
20. Administrative Policy Number 24 – Equipment Disposal Policy
21. Civil Rights Plan
22. Contracts

S. Discussion/Information

1. Strategic Plan – August 30th & 31st
2. Executive Committee meeting – 2017 budget
3. Site updates

T. Adjournment

Next Meeting Dates:

- **Wednesday, July 20, 2016 – Marshall**
- **Wednesday, August 17, 2016 – Marshall**
- **Wednesday, September 21, 2016 – Marshall**

SOUTHWEST HEALTH & HUMAN SERVICES

Ivanhoe, Marshall, Slayton, Pipestone, Redwood and Luverne Offices

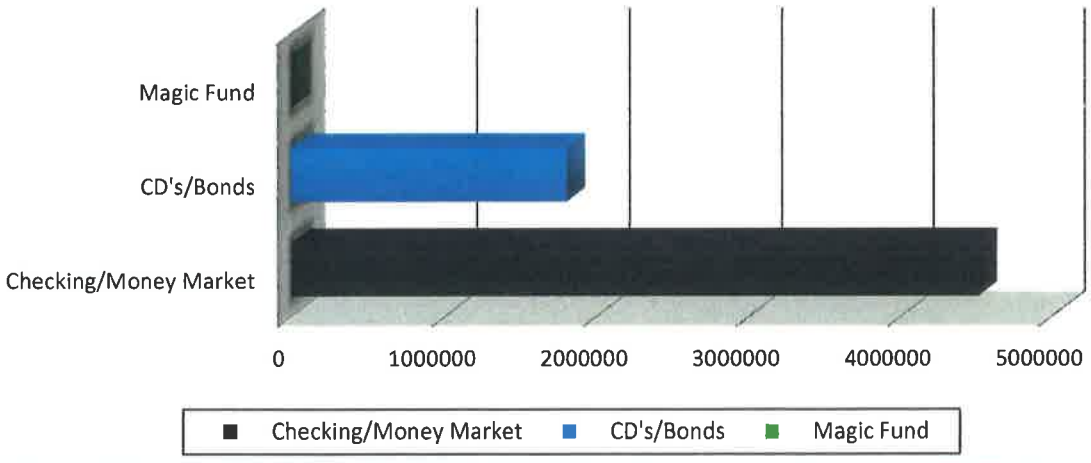
SUMMARY OF FINANCIAL ACCOUNTS REPORT For the Month Ending: **May 31, 2016**

* Income Maintenance * Social Services * Information Technology * Health *

Description	Month	Running Balance
BEGINNING BALANCE		**$826,629**
RECEIPTS		
Monthly Receipts	2,167,513	
County Contribution	1,609,582	
Interest on Investments	781	
TOTAL MONTHLY RECEIPTS		3,777,876
DISBURSEMENTS		
Monthly Disbursements	3,009,587	
TOTAL MONTHLY DISBURSEMENTS		3,009,587
ENDING BALANCE		**$1,594,918**

REVENUE			
Checking/Money Market	***$1,594,918***		**Average Balance last two years $3,707,033**
CD's/Bonds	***$1,800,000***		
Magic Fund	*$0*		
ENDING BALANCE		**$3,394,918**	

REVENUE DESIGNATION



Southwest Health and Human Services

Treasurer's Cash Trial Balance

As of 05/2016

Fund		Beginning Balance	This Month	YTD	Current Balance
1	Health Services Fund				
		1,436,504.12			
	Receipts		236,197.79	1,476,475.75	
	Disbursements		103,651.54-	353,404.80-	
	Payroll		207,946.85-	1,100,045.92-	
	Fund Total		75,400.60-	23,025.03	1,459,529.15
5	Human Services Fund 410		General Administration		
		352,118.99			
	Receipts		50,471.35	244,619.15	
	Disbursements		12,597.85-	219,696.74-	
	Payroll		13,956.35-	76,171.38-	
	Dept Total		23,917.15	51,248.97-	300,870.02
5	Human Services Fund 420		Income Maintenance		
		3,696,135.62-			
	Receipts		841,648.26	2,484,049.67	
	Disbursements		362,305.88-	1,404,873.11-	
	Payroll		350,053.52-	1,890,244.20-	
	Dept Total		129,288.86	811,067.64-	4,507,203.26-
5	Human Services Fund 431		Social Services		
		8,365,424.02			
	Receipts		2,383,247.49	5,073,289.20	
	Disbursements		180,100.38-	797,096.44-	
	SSIS		1,003,935.26-	3,322,284.71-	
	Payroll		606,092.04-	3,156,601.17-	
	Dept Total		593,119.81	2,202,693.12-	6,162,730.90
5	Human Services Fund 461		Information Systems		
		2,035,385.63-			
	Receipts		3,734.50	10,543.00	
	Disbursements		846.51-	4,966.18-	
	Payroll		22,499.41-	135,248.74-	
	Dept Total		19,611.42-	129,671.92-	2,165,057.55-

Southwest Health and Human Services

Treasurer's Cash Trial Balance

Fund		Beginning Balance		This Month	YTD	Current Balance
5	Human Services Fund		471	LCTS Collaborative Agency		
		0.00				
	Receipts			45,810.00	85,634.00	
	Journal Entries			45,810.00-	85,634.00-	
	Dept Total			0.00	0.00	0.00
	Fund Total	2,986,021.76		726,714.40	3,194,681.65-	208,659.89-
61	Agency Health Insurance					
		0.00				
	Receipts			216,765.84	1,203,696.46	
	Disbursements			145,451.53-	992,910.10-	
	Fund Total			71,314.31	210,786.36	210,786.36
71	LCTS Lyon Murray Collaborative Fund		471	LCTS Collaborative Agency		
		28,987.61				
	Disbursements			0.00	31,225.50-	
	Journal Entries			19,458.00	34,850.00	
	Dept Total			19,458.00	3,624.50	32,612.11
	Fund Total	28,987.61		19,458.00	3,624.50	32,612.11
73	LCTS Rock Pipestone Collaborative Fund		471	LCTS Collaborative Agency		
		35,699.21				
	Receipts			0.00	650.00	
	Disbursements			0.00	4,473.00-	
	Journal Entries			9,011.00	16,054.00	
	Dept Total			9,011.00	12,231.00	47,930.21
	Fund Total	35,699.21		9,011.00	12,231.00	47,930.21
75	Redwood LCTS Collaborative		471	LCTS Collaborative Agency		
		22,416.99				
	Disbursements			0.00	5,742.00-	
	Journal Entries			17,341.00	34,730.00	

Southwest Health and Human Services

Treasurer's Cash Trial Balance

Fund		Beginning Balance	This Month	YTD	Current Balance
	Dept Total		17,341.00	28,988.00	51,404.99
	Fund Total	22,416.99	17,341.00	28,988.00	51,404.99
77	Local Advisory Council		477 Local Advisory Council		
		1,622.38			
	Disbursements		150.00-	308.00-	
	Dept Total		150.00-	308.00-	1,314.38
	Fund Total	1,622.38	150.00-	308.00-	1,314.38
All Funds		4,511,252.07			
	Receipts		3,777,875.23	10,578,957.23	
	Disbursements		805,103.69-	3,814,695.87-	
	SSIS		1,003,935.26-	3,322,284.71-	
	Payroll		1,200,548.17-	6,358,311.41-	
	Total		768,288.11	2,916,334.76-	1,594,917.31

Southwest Health and Human Services

Trial Balance
As of 05/2016
Report Basis: Cash

1 Health Services Fund

Account		Beginning Balance	Actual This- Month	Actual Year- To- Date	Current Balance
	----------Assets----------				
1001	Cash in Bank - Checking	1,436,504.12	75,400.60-	23,025.03	1,459,529.15
1090	Investments	320,000.00	0.00	0.00	320,000.00
	Total Assets	1,756,504.12	75,400.60-	23,025.03	1,779,529.15
	---Liabilities and Balance-----				
	Liabilities				
	Total Liabilities	0.00	0.00	0.00	0.00
	Fund Balance				
2881	Unassigned Fund Balance	1,799,880.68-	0.00	0.00	1,799,880.68-
2885	Revenue Control	0.00	236,147.61-	1,475,868.14-	1,475,868.14-
2887	Expenditure Control	0.00	311,548.21	1,452,843.11	1,452,843.11
	Total Fund Balance	1,799,880.68-	75,400.60	23,025.03-	1,822,905.71-
	Total Liabilities and Balance	1,799,880.68-	75,400.60	23,025.03-	1,822,905.71-
410	General Administration				
	----------Assets----------				
1265	Due From Other Funds (Proprietary)	43,376.56	0.00	0.00	43,376.56
	Total Assets	43,376.56	0.00	0.00	43,376.56
	---Liabilities and Balance-----				
	Liabilities				
	Total Liabilities	0.00	0.00	0.00	0.00
	Total Liabilities and Balance	0.00	0.00	0.00	0.00
1	Health Services Fund	0.00	0.00	0.00	0.00

Southwest Health and Human Services

Trial Balance
As of 05/2016 Report Basis: Cash

5 Human Services Fund

Account		Beginning Balance	Actual This- Month	Actual Year- To- Date	Current Balance
410	General Administration				
	----------Assets----------				
1001	Cash In Bank - Checking	352,118.99	23,917.15	51,248.97-	300,870.02
1265	Due From Other Funds (Proprietary)	245,800.53	0.00	0.00	245,800.53
	Total Assets	597,919.52	23,917.15	51,248.97-	546,670.55
	---Liabilities and Balance-----				
	Liabilities				
2090	Due To Flexible Plan Employees	1,599.96	18,098.00-	18,098.02-	16,498.06-
	Total Liabilities	1,599.96	18,098.00-	18,098.02-	16,498.06-
	Fund Balance				
2881	Unassigned Fund Balance	599,519.48-	0.00	0.00	599,519.48-
2887	Expenditure Control	0.00	5,819.15-	69,346.99	69,346.99
	Total Fund Balance	599,519.48-	5,819.15-	69,346.99	530,172.49-
	Total Liabilities and Balance	597,919.52-	23,917.15-	51,248.97	546,670.55-
420	Income Maintenance				
	----------Assets----------				
1001	Cash In Bank - Checking	3,696,135.62-	129,288.86	811,067.64-	4,507,203.26-
1090	Investments	592,000.00	0.00	0.00	592,000.00
	Total Assets	3,104,135.62-	129,288.86	811,067.64-	3,915,203.26-
	---Liabilities and Balance-----				
	Liabilities				
	Total Liabilities	0.00	0.00	0.00	0.00
	Fund Balance				
2881	Unassigned Fund Balance	3,104,135.62	0.00	0.00	3,104,135.62
2885	Revenue Control	0.00	840,771.36-	2,480,108.17-	2,480,108.17-
2887	Expenditure Control	0.00	711,482.50	3,291,175.81	3,291,175.81
	Total Fund Balance	3,104,135.62	129,288.86-	811,067.64	3,915,203.26
	Total Liabilities and Balance	3,104,135.62	129,288.86-	811,067.64	3,915,203.26
431	Social Services				
	----------Assets----------				

Southwest Health and Human Services

Trial Balance
As of 05/2016

Report Basis: Cash

5 Human Services Fund

Account		Beginning Balance	Actual This- Month	Actual Year- To- Date	Current Balance
1001	Cash In Bank - Checking	8,365,424.02	593,119.81	2,202,693.12-	6,162,730.90
1090	Investments	888,000.00	0.00	0.00	888,000.00
1205	County Advances - MFIP (Chippewa Cty)	80,749.47	0.00	0.00	80,749.47
	Total Assets	9,334,173.49	593,119.81	2,202,693.12-	7,131,480.37
	---Liabilities and Balance-----				
	Liabilities				
	Total Liabilities	0.00	0.00	0.00	0.00
	Fund Balance				
2881	Unassigned Fund Balance	9,334,173.49-	0.00	0.00	9,334,173.49-
2885	Revenue Control	0.00	2,378,918.51-	4,973,271.40-	4,973,271.40-
2887	Expenditure Control	0.00	1,785,798.70	7,175,964.52	7,175,964.52
	Total Fund Balance	9,334,173.49-	593,119.81-	2,202,693.12	7,131,480.37-
	Total Liabilities and Balance	9,334,173.49-	593,119.81-	2,202,693.12	7,131,480.37-
461	Information Systems				
	----------Assets----------				
1001	Cash In Bank - Checking	2,035,385.63-	19,611.42-	129,671.92-	2,165,057.55-
	Total Assets	2,035,385.63-	19,611.42-	129,671.92-	2,165,057.55-
	---Liabilities and Balance-----				
	Liabilities				
	Total Liabilities	0.00	0.00	0.00	0.00
	Fund Balance				
2881	Unassigned Fund Balance	2,035,385.63	0.00	0.00	2,035,385.63
2885	Revenue Control	0.00	3,734.50-	10,543.00-	10,543.00-
2887	Expenditure Control	0.00	23,345.92	140,214.92	140,214.92
	Total Fund Balance	2,035,385.63	19,611.42	129,671.92	2,165,057.55
	Total Liabilities and Balance	2,035,385.63	19,611.42	129,671.92	2,165,057.55
471	LCTS Collaborative Agency				
	----------Assets----------				
	Total Assets	0.00	0.00	0.00	0.00
	---Liabilities and Balance-----				
	Liabilities				

Southwest Health and Human Services

RM- Stmt of Revenues & Expenditures

As Of 05/2016 Report Basis: Cash

DESCRIPTION	CURRENT MONTH	YEAR TO- DATE	2016 BUDGET	% OF BUDG	% OF YEAR
FUND 1 HEALTH SERVICES FUND					
REVENUES					
CONTRIBUTIONS FROM COUNTIES	0.00	391,199.00-	782,398.00-	50	42
INTERGOVERNMENTAL REVENUES	1,734.00-	108,607.14-	327,100.00-	33	42
STATE REVENUES	55,139.15-	324,290.61-	921,568.00-	35	42
FEDERAL REVENUES	142,642.37-	454,749.22-	1,124,712.00-	40	42
FEES	36,287.33-	193,736.52-	448,995.00-	43	42
EARNINGS ON INVESTMENTS	124.88-	2,159.09-	3,000.00-	72	42
MISCELLANEOUS REVENUES	219.88-	1,126.56-	0.00	0	42
TOTAL REVENUES	236,147.61-	1,475,868.14-	3,607,773.00-	41	42
EXPENDITURES					
PROGRAM EXPENDITURES	0.00	0.00	0.00	0	42
PAYROLL AND BENEFITS	207,946.85	1,100,045.92	2,862,402.00	38	42
OTHER EXPENDITURES	103,601.36	352,797.19	745,371.00	47	42
TOTAL EXPENDITURES	311,548.21	1,452,843.11	3,607,773.00	40	42

Southwest Health and Human Services

RM- Stmt of Revenues & Expenditures

As Of 05/2016 Report Basis: Cash

DESCRIPTION	CURRENT MONTH	YEAR TO- DATE	2016 BUDGET	% OF BUDG	% OF YEAR
FUND 5 HUMAN SERVICES FUND					
REVENUES					
CONTRIBUTIONS FROM COUNTIES	1,609,582.02-	1,827,577.21-	9,546,442.00-	19	42
INTERGOVERNMENTAL REVENUES	4,886.32-	17,166.33-	10,000.00-	172	42
STATE REVENUES	565,738.66-	1,475,283.91-	4,712,344.00-	31	42
FEDERAL REVENUES	834,363.78-	2,827,409.48-	7,305,662.00-	39	42
FEES	171,807.18-	804,892.43-	1,916,800.00-	42	42
EARNINGS ON INVESTMENTS	655.63-	11,335.12-	27,000.00-	42	42
MISCELLANEOUS REVENUES	36,390.78-	500,258.09-	1,333,500.00-	38	42
TOTAL REVENUES	3,223,424.37-	7,463,922.57-	24,851,748.00-	30	42
EXPENDITURES					
PROGRAM EXPENDITURES	1,204,739.42	4,285,998.58	9,238,507.00	46	42
PAYROLL AND BENEFITS	972,595.22	5,249,886.48	13,012,977.00	40	42
OTHER EXPENDITURES	337,473.33	1,140,817.18	2,600,264.00	44	42
TOTAL EXPENDITURES	2,514,807.97	10,676,702.24	24,851,748.00	43	42

Southwest Health and Human Services

Revenues & Expend by Prog,Dept,Fund

Report Basis: Cash

Element	Description	Account Number		Current Month	Year- To- Date	Budget	% of Bdgt	% of Year
530 PROGRAM	Clearway Grant		Revenue	0.00	74,952.00-	149,000.00-	50	42
			Expend.	12,336.82	46,451.60	133,677.00	35	42
			Net	12,336.82	28,500.40-	15,323.00-	186	42
900 PROGRAM	Emergency Preparedness		Revenue	20,640.91-	55,409.10-	117,300.00-	47	42
			Expend.	11,589.12	41,989.95	130,861.00	32	42
			Net	9,051.79-	13,419.15-	13,561.00	99-	42
901 PROGRAM	Med Reserve Corps		Revenue	0.00	0.00	3,500.00-	0	42
			Expend.	830.06	919.28	1,733.00	53	42
			Net	830.06	919.28	1,767.00-	52-	42
483 DEPT	Health Education	Totals:	Revenue	40,723.11-	274,325.00-	522,900.00-	52	42
			Expend.	44,219.02	194,664.48	566,820.00	34	42
			Net	3,495.91	79,660.52-	43,920.00	181-	42
485 DEPT	Environmental Health							
800 PROGRAM	Environmental		Revenue	8,432.97-	46,055.73-	234,400.00-	20	42
			Expend.	16,142.38	70,780.77	234,336.00	30	42
			Net	7,709.41	24,725.04	64.00-	38,633-	42
820 PROGRAM	Healthy Homes Grant		Revenue	4,858.60-	10,285.80-	40,000.00-	26	42
			Expend.	1,101.07	14,785.17	23,101.00	64	42
			Net	3,757.53-	4,499.37	16,899.00-	27-	42
485 DEPT	Environmental Health	Totals:	Revenue	13,291.57-	56,341.53-	274,400.00-	21	42
			Expend.	17,243.45	85,565.94	257,437.00	33	42
			Net	3,951.88	29,224.41	16,963.00-	172-	42
1 FUND	Health Services Fund	Totals:	Revenue	236,147.61-	1,475,868.14-	3,607,773.00-	41	42
			Expend.	311,548.21	1,452,843.11	3,607,773.00	40	42
			Net	75,400.60	23,025.03-	0.00	0	42

Southwest Health and Human Services

Revenues & Expend by Prog,Dept,Fund

Report Basis: Cash

Element	Description	Account Number		Current Month	Year- To- Date	Budget	% of Bdgt	% of Year
742 PROGRAM	Mental Health/Children Only		Revenue	93,190.55-	439,229.02-	957,137.00-	46	42
			Expend.	169,166.30	714,529.28	1,467,408.00	49	42
			Net	75,975.75	275,300.26	510,271.00	54	42
750 PROGRAM	Developmental Disabilities		Revenue	91,805.94-	274,263.47-	792,617.00-	35	42
			Expend.	28,255.65	148,207.13	417,435.00	36	42
			Net	63,550.29-	126,056.34-	375,182.00-	34	42
760 PROGRAM	Adult Services		Revenue	111,094.53-	491,523.75-	1,090,000.00-	45	42
			Expend.	8,122.74	37,891.92	110,500.00	34	42
			Net	102,971.79-	453,631.83-	979,500.00-	46	42
765 PROGRAM	Adults Waivers		Revenue	66,264.91-	202,622.94-	484,000.00-	42	42
			Expend.	1,590.54	22,211.58	17,000.00	131	42
			Net	64,674.37-	180,411.36-	467,000.00-	39	42
431 DEPT	Social Services	Totals:	Revenue	2,378,918.51-	4,973,271.40-	15,505,393.00-	32	42
			Expend.	1,785,798.70	7,175,964.52	16,106,612.00	45	42
			Net	593,119.81-	2,202,693.12	601,219.00	366	42
461 DEPT	Information Systems							
0 PROGRAM	...		Revenue	3,734.50-	10,543.00-	28,500.00-	37	42
			Expend.	23,345.92	140,214.92	348,907.00	40	42
			Net	19,611.42	129,671.92	320,407.00	40	42
461 DEPT	Information Systems	Totals:	Revenue	3,734.50-	10,543.00-	28,500.00-	37	42
			Expend.	23,345.92	140,214.92	348,907.00	40	42
			Net	19,611.42	129,671.92	320,407.00	40	42
5 FUND	Human Services Fund	Totals:	Revenue	3,223,424.37-	7,463,922.57-	24,851,748.00-	30	42
			Expend.	2,514,807.97	10,676,702.24	24,851,748.00	43	42
			Net	708,616.40-	3,212,779.67	0.00	0	42
FINAL TOTALS	977 Accounts		Revenue	3,459,571.98-	8,939,790.71-	28,459,521.00-	31	42
			Expend.	2,826,356.18	12,129,545.35	28,459,521.00	43	42
			Net	633,215.80-	3,189,754.64	0.00	0	42

SOUTHWEST HEALTH AND HUMAN SERVICES CHECK REGISTER

MAY 2016

DATE	RECEIPT or CHECK #	DESCRIPTION	+ DEPOSITS	-DISBURSEMENTS	BALANCE
	BALANCE FORWARD				826,629.20
5/2/16	67464-67488	Disb		9,466.51	817,162.69
5/2/16	67489-67591	Disb		218,950.71	598,211.98
5/2/16	1521-1537 ACH	Disb		989.53	597,222.45
5/2/16	9418	Disb		15,879.27	581,343.18
5/3/16	18130-18163,18165,18167	Dep	69,168.44		650,511.62
5/2/16	23718	Interest	706.63		651,218.25
5/2/16	23723	Interest	73.88		651,292.13
5/9/16	67592-67669	Disb		8,237.29	643,054.84
5/9/16	67670-67820	Disb		230,559.28	412,495.56
5/9/16	1538-1565 ACH	Disb		3,040.87	409,454.69
5/6/16	18164,18166,18168-18255	Dep	1,421,484.81		1,830,939.50
5/9/16	9419	Disb		27,666.46	1,803,273.04
5/11/16	18256-18307	Dep	166,824.71		1,970,097.75
5/12/16	9420	Disb		53,713.17	1,916,384.58
5/13/16	7302-7319	PAYROLL		136,751.96	1,779,632.62
5/13/16	37334-37578 ACH	PAYROLL		463,894.80	1,315,737.82
5/13/16	18308-18335	Dep	169,430.32		1,485,168.14
5/16/16	67821-67855	Disb		7,135.00	1,478,033.14
5/16/16	1566-1566	Disb		150.00	1,477,883.14
5/16/16	67856-67975	Disb		339,351.08	1,138,532.06
5/16/16	1567-1585 ACH	Disb		2,422.33	1,136,109.73
5/16/16	9421	Disb		8,483.40	1,127,626.33
5/17/16	18336-18369	Dep	238,157.72		1,365,784.05
5/18/16	37579-37582 ACH	PAYROLL		2,273.17	1,363,510.88
5/18/16	9422	Disb		8,852.42	1,354,658.46
5/18/16	67976-68064	Disb		10,348.80	1,344,309.66
5/18/16	68065-68267	Disb		93,416.12	1,250,893.54
5/18/16	1586-1588 ACH	Disb		876.40	1,250,017.14
5/20/16	18370-18421	Dep	682,283.72		1,932,300.86
5/20/16	9423	Disb		7,978.48	1,924,322.38
5/23/16	68268-68320	Disb		7,762.30	1,916,560.08
5/23/16	68321-68432	Disb		544,175.03	1,372,385.05
5/23/16	1589-1599 ACH	Disb		710.52	1,371,674.53
5/23/16	9424	Disb		10,081.57	1,361,592.96
5/24/16	18422-18462	Dep	182,388.70		1,543,981.66
5/24/16	9425	Dep	699.00		1,544,680.66
5/24/16	9426	Disb		912.45	1,543,768.21
5/27/16	7320-7346	PAYROLL		136,569.41	1,407,198.80
5/27/16	37583-37834 ACH	PAYROLL		461,058.83	946,139.97
5/27/16	18463-18498	Dep	838,234.19		1,784,374.16
5/31/16	68433-68468	Disb		15,197.50	1,769,176.66
5/31/16	68469-68580	Disb		152,623.32	1,616,553.34
5/31/16	1600-1604 ACH	Disb		525.46	1,616,027.88
5/31/16	9427	Disb		29,533.68	1,586,494.20
5/31/16	18499-18509	Dep	8,423.11		1,594,917.31
					1,594,917.31
					1,594,917.31
					1,594,917.31
					1,594,917.31
					1,594,917.31
	Balanced jvp 6/2/16	TOTALS	3,777,875.23	3,009,587.12	

Adult - Social Services Caseload

Average	Adult Brain Injury (BI)	Adult Community Alternative Care (CAC)	Adult Community Access for Disability Inclusion (CADI)	Adult Essential Community Supports	Adult Mental Health (AMH)	Adult Protective Services (APS)	Adult Services (AS)	Alternative Care (AC)	Chemical Dependency (CD)	Developmental Disabilities (DD)	Elderly Waiver (EW)	Total Programs
2014	14	242	14		331	37	842	28	484	464	334	2789
2015	12	227	13		306	34	817	23	403	460	352	2652
2016	13	240	12	0	297	48	823	18	394	452	363	2660
2017												

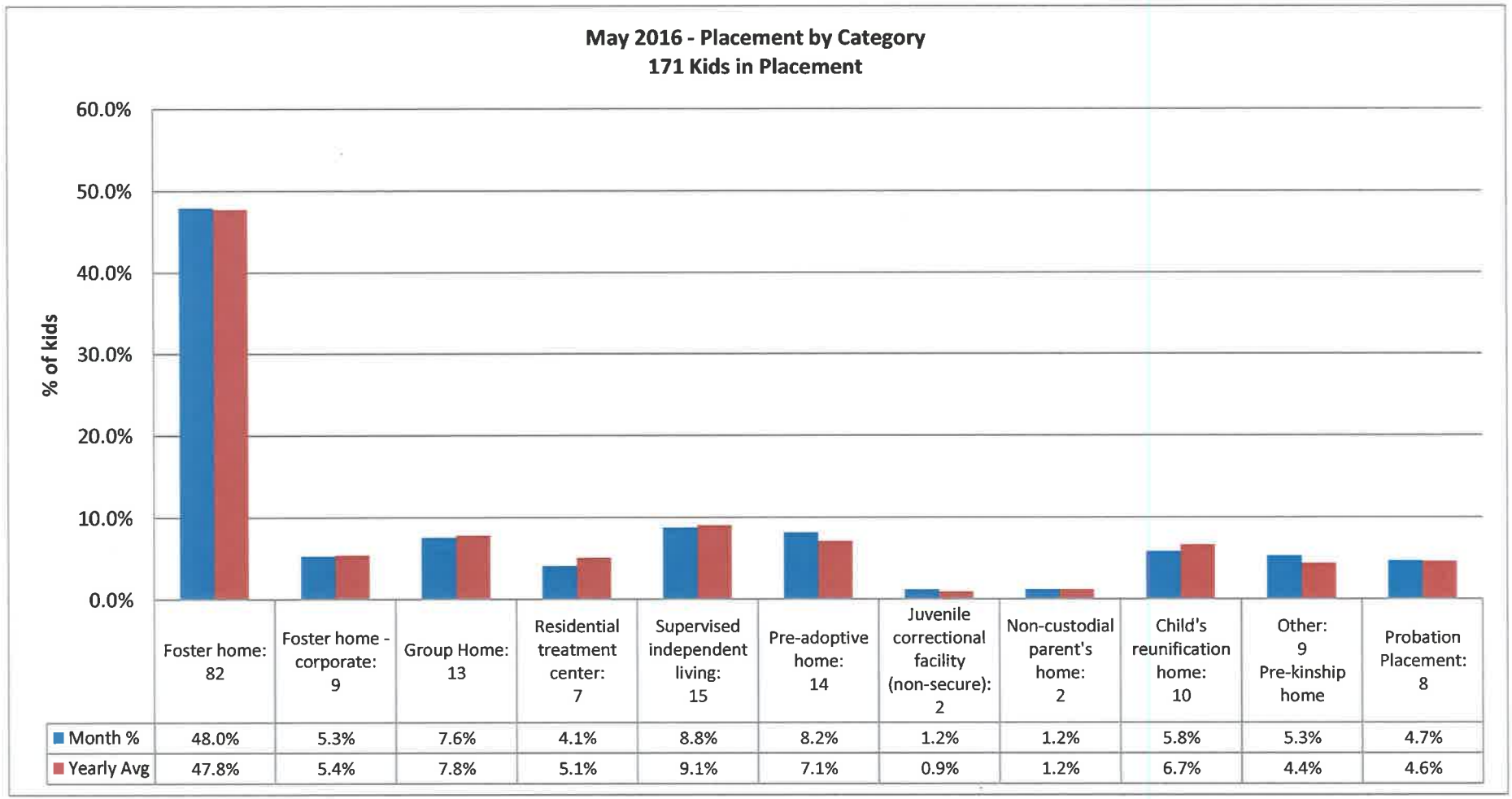
*Note: CADI name change and there is a new category (Adult Essential Community Supports)

2016	Adult Brain Injury (BI)	Adult Community Access for Disability Inclusion (CADI)	Adult Community Alternative Care (CAC)	Adult Essential Community Supports	Adult Mental Health (AMH)	Adult Protective Services (APS)	Adult Services (AS)	Alternative Care (AC)	Chemical Dependency (CD)	Developmental Disabilities (DD)	Elderly Waiver (EW)	Total Programs
January	13	237	12	0	297	40	815	19	367	452	358	2610
February	13	238	12	0	297	42	827	19	412	453	361	2674
March	13	243	12	0	293	44	835	17	370	452	366	2645
April	13	240	12	0	294	55	822	17	403	451	362	2669
May	13	241	12	0	303	59	818	17	417	453	367	2700
June												
July												
August												
September												
October												
November												
December												
	13	**240**	**12**	**0**	**297**	**48**	**823**	**18**	**394**	**452**	**363**	**2660**

Children's - Social Services Caseload

Average	Adolescent Independent Living (ALS)	Adoption	Child Brain Injury (BI)	Child Community Alternative Care (CAC)	Child Community Alternatives for Disabled Individuals (CADI)	Child Protection (CP)	Child Welfare (CW)	Children's Mental Health (CMH)	Early Inter vention: Infants & Toddlers with Disabilities	Minor Parents (MP)	Parent Support Outreach Program (PSOP)	Total Programs
2014	42	18	0	4	31	127	104	106	0	1	16	449
2015	38	15	1	3	30	153	127	96	0	1	18	482
2016	40	17	2	4	35	179	147	86	0	0	13	524
2017												

2016	Adolescent Independent Living (ALS)	Adoption	Child Brain Injury (BI)	Child Community Alternative Care (CAC)	Child Community Alternatives for Disabled Individuals (CADI)	Child Protection (CP)	Child Welfare (CW)	Children's Mental Health (CMH)	Early Inter vention: Infants & Toddlers with Disabilities	Minor Parents (MP)	Parent Support Outreach Program (PSOP)	Total Programs
January	40	15	2	4	35	179	138	87	0	0	13	513
February	39	15	2	4	34	180	154	85	0	0	13	526
March	39	17	2	4	33	186	145	88	0	0	11	525
April	43	17	1	5	35	193	151	85	0	0	15	545
May	41	19	1	5	36	157	148	87	0	1	14	509
June												
July												
August												
September												
October												
November												
December												
	40	**17**	**2**	**4**	**35**	**179**	**147**	**86**	**0**	**0**	**13**	**524**



	Foster home: 82	Foster home - corporate: 9	Group Home: 13	Residential treatment center: 7	Supervised independent living: 15	Pre-adoptive home: 14	Juvenile correctional facility (non-secure): 2	Non-custodial parent's home: 2	Child's reunification home: 10	Other: 9 Pre-kinship home	Probation Placement: 8
Month %	48.0%	5.3%	7.6%	4.1%	8.8%	8.2%	1.2%	1.2%	5.8%	5.3%	4.7%
Yearly Avg	47.8%	5.4%	7.8%	5.1%	9.1%	7.1%	0.9%	1.2%	6.7%	4.4%	4.6%

2016 KIDS IN OUT OF HOME PLACEMENT - BY COUNTY

	Jan-16	Feb-16	Mar-16	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	YTD Average	2015 Average
Lincoln	12	11	13	11	11								12	8
Lyon	55	54	46	44	45								49	50
Murray	4	6	4	6	5								5	5
Pipestone	19	21	22	20	19								20	22
Redwood	74	73	70	79	77								75	59
Rock	14	13	14	13	14								14	13
Monthly Totals	**178**	**178**	**169**	**173**	**171**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		

June 2016: Total kids in placement = 171

Total of 3 Children entered placement

1	Lyon	Foster Care
1	Redwood	Residential Treatment Facility
1	Rock	Juvenile Correctional Facility

Total of 5 Children were discharged from placement (discharges from previous month)

1	Murray	Correctional Facility
1	Pipestone	Group Home
1	Redwood	Probation
1	Redwood	Supervised Independent Living
1	Redwood	Foster Home

NON IVD COLLECTIONS

MAY 2016

PROGRAM	ACCOUNT	TOTAL
MSA/GRH	05-420-605.5802	50
TANF (MFIP/DWP/AFDC)	05-420-610.5803	585
GA	05-420-620.5803	454
FS	05-420-630.5803	229
CS (PI Fee, App Fee, etc)	05-420-640.5501	1,978
MA Recoveries & Estate Collections (25% retained by agency)	05-420-650.5803	13,412
REFUGEE	05-420-680.5803	100
CHILDRENS		
Parental Fees, Holds	05-431-710.5501	6,637
OOH/FC Recovery	05-431-710.5803	8,434
CHILDCARE		
Licensing	05-431-720.5502	1,950
Corp FC Licensing	05-431-710.5505	600
Over Payments	05-431-721&722.5803	0
CHEMICAL DEPENDENCY		
CD Assessments	05-431-730.5519	3,108
Detox Fees	05-431-730.5520	813
MENTAL HEALTH		
Insurance Copay	05-431-740.5803	6
Over Payments	05-431-741 or 742.5803	0
DEVELOPMENTAL DISABILITIES		
Insurance Copay/Overpayments	05-431-750.5803	6
ADULT		
Insurance Copay/Overpayments	05-431-760.5803	6
TOTAL NON-IVD COLLECTIONS		**38,367**

SOUTHWEST HEALTH AND HUMAN SERVICES
PERSONNEL POLICY NUMBER 22

EFFECTIVE DATE: 01/21/15
REVISION DATE: 06/15/16
AUTHORITY: Southwest Health and Human Services Joint Governing Board

----SOCIAL MEDIA POLICY----

Section 1 - Policy Statement

a. Southwest Health and Human Services (SWHHS) understands that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media while at work or when work related information is disclosed on social media, we have established these guidelines for appropriate use of social media.

Section 2 – Guidelines

a. In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with SWHHS, as well as any other form of electronic communication. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members, customers, vendors, people who work on behalf of SWHHS or SWHHS legitimate business interests may result in disciplinary action up to and including termination.

b. ~~Carefully read these policies; Administrative Policy #1 - Data Privacy and Procedures, Administrative Policy #10 - LAN Email Internet Access, Administrate Policy #13 - Equal Opportunity and Affirmative Action, Administrative Policy #14 - HIPAA , Personnel Policy #11 - Code of Ethics, and Personnel Policy #15 - Respectful Workplace and ensure your postings are consistent with these policies.~~ Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

c. Always be fair and courteous to fellow associates, customers, members, suppliers or people who work on behalf of SWHHS. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or by utilizing our open door policy than by posting complaints to a social media outlet.

d. Post only appropriate and respectful content

- Maintain the confidentiality of SWHHS private or confidential information. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

- Do not create a link from your blog, website or other social networking site to a SWHHS website without identifying yourself as a SWHHS employee.

- Express only your personal opinions. Never represent yourself as a spokesperson for SWHHS. If SWHHS is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of SWHHS, fellow associates, members, customers, suppliers or people working on behalf of SWHHS. If you do publish a blog or post online related to the work you do or subjects associated with SWHHS, make it clear that you are not speaking on behalf of SWHHS. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of SWHHS."

e. Using social media at work

- Refrain from using social media while on work time unless it is work-related as authorized by your manager ~~or consistent with Administrative Policy #10 - LAN Email Internet Access~~. Do not use SWHHS' email addresses to register on social networks, blogs or other online tools utilized for personal use.

f. Other general guidelines

- SWHHS strongly discourages "friending" of consumers/patients on social media websites. Staff generally should not initiate or accept friend requests except in unusual circumstances such as the situation where an in-person friendship pre-dates the professional relationship.

Section 3 – Use of SWHHS Social Media Sites

a. This section establishes guidelines for the establishment and use by SWHHS of social media sites (including but not limited to Facebook and Twitter) as a means of conveying SWHHS information to its citizens. The intended purpose behind establishing SWHHS social media sites is to disseminate information from the agency, about the agency, to its constituents. SWHHS has an overriding interest and expectation in deciding what is "spoken" on behalf of SWHHS on agency social media sites. Examples of social media include Facebook, blogs, MySpace, RSS, YouTube, Second Life, Twitter, LinkedIn, Delicious, and Flicker.

b. General Policy

- The establishment and use by any SWHHS social media sites are subject to approval by the Director or his/her designees. All SWHHS social media sites shall be administered by SWHHS Information Technology ("IT") staff.
- SWHHS social media sites should make clear that they are maintained by SWHHS and that they follow the agency's Social Media Policy.
- Wherever possible, agency social media sites should link back to the official SWHHS website for forms, documents, online services and other information necessary to conduct business with SWHHS.
- The Director and Management Information Supervisor or designee will monitor content on SWHHS's social media sites to ensure adherence to both SWHHS Social Media Policy and the interest and goals of SWHHS.
- SWHHS reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy or any applicable law. Any content removed based on these guidelines must be retained by the Data Privacy Officer for a reasonable period of time, including the time, date and identity of the poster, when available.
- These guidelines must be displayed to users or made available by hyperlink.
- SWHHS's website at www.swmhhs.com will remain the agency's primary internet presence.
- All agency social media sites shall adhere to applicable federal, state and local laws, regulations and policies.
- Comments on topics or issues not within the jurisdictional purview of SWHHS may be removed.
- Employees representing the agency via agency social media sites must conduct themselves at all times as a representative of the agency and in accordance with all agency policies.

c. Comment Policy

- As a public entity the agency must abide by certain standards to serve all its constituents in a civil and unbiased manner.

- Comments containing any of the following inappropriate forms of content shall not be permitted on SWHHS social media sites and are subject to removal and/or restriction by the Director or his/her designees:
    - Comments not related to the original topic, including random or unintelligible comments;
        1. Profane, obscene, violent, or pornographic content and/or language;
        2. Content that promotes, fosters or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, or national origin;
        3. Defamatory or personal attacks;
        4. Threats to any person or organization.

- Information that may tend to compromise the safety or security of the public or public systems.

- SWHHS reserves the right to deny access to SWHHS social media sites for any individual, who violates the SWHHS's Social Media Policy, at any time and without prior notice.

- Departments shall monitor their social media sites for comments requesting responses from the agency and for comments in violation of this policy.

- When a SWHHS employee responds to a comment, in his/her capacity as a SWHHS employee, the employee's name and title should be made available.

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 8

EFFECTIVE DATE: 01/01/11
REVISION DATE: 12/18/13, 06/15/16
AUTHORITY: Southwest Health and Human Services Joint Governing Board

----DISASTER RECOVERY PLAN----

Section 1 - Purpose

a. The purpose of this policy is to detail the disaster recovery procedures for Southwest Health and Human Services. This policy identifies the following:
   - Current physical equipment that requires a "plan" for disaster recovery
   - Current backup systems for data
   - Hot sites and contracted or other agreements for alternate sites and replacement equipment.
   - I.T., management, and user personnel involved in plan and recovery
   - Recovery procedures after an actual disaster
   - Testing of Disaster Recovery Plan(DRP)

Section 2 - Current Servers

a. Critical Servers:
   - LLMHS01 Human Services Data Server containing day to day documents, etc.
   - SWMAIL01Human Services and Lyon County Exchange/Email Server
   - SWHHS14Human Services Terminal Server (used by telecommuters for access to SWHHS data and e-mail services)
   - IBM I Series Server, contains LLMHS and Lyon County accounting software and associated dataSWHHS06 Pipestone (on their premesis)
   - PHFILE server Redwood (on their premesis)
   - SWHHS06 Rock (on their premises)
   - SWMSHLDC Entire Active Directory

b. Non-Critical Servers:
   - LLMHS10 and LLMHS12 (these are antivirus and Windows software updates servers).
   - State Firewall Routers are installed in all county government centers, and provide wide data/internet access to other county and state government systems.

Section 3 - Current Backup Systems

a. I series full system tape backups, which includes all software and user Id's. The operating system is completed on a quarterly basis. Copies of this are kept off site.

b. I series daily tape backups of all accounting and associated changing data are completed daily, with weekly off site copies.

c. Email/Exchange Server tape backups are completed daily, with weekly off site copies.

d. Staff data/documents tape backups are completed daily with weekly off site copies.

e. SSIS server tape backups are completed daily, with weekly off site copies.

Section 4 - Hot Sites and Contracted or Other Agreements for Alternate Sites, and Replacement Equipment

a. State router replacement would be the complete responsibility of the State of MN. These are in place and usable at any county location in the State of MN.

b. Current "Hot" servers at the Lincoln (Ivanhoe),Murray (Slayton), Redwood (Redwood Falls), Pipestone (Pipestone) and Rock (Luverne) sites are already in place and functional on the same domain as the central site in Lyon (Marshall). Copies of current off-site backups would be restored to one of these selected sites to make all data available to system users.

c. I series equipment replacement will be available through an Emergency Hardware Replacement Contract with our IBM solutions vendor CPS Technology Solutions, Inc.(signed 04/27/09). All off site backups can be restored to this replacement system which could be delivered to our site or alternate site within the time period specified in the contract (2 working days).

d. Other systems such as Maxis, MMIS, and Prism are all through the Internet and are maintained at the State of MN site by them. These are available to end users from any county location in the State of MN. Nightingale Notes is maintained by Champ.

e. The SSIS server would be replaced by the State of MN.

f. Other servers would have to be secured through a vendor.

Section 5 - I.T., Management, and User Personnel Involved in Plan and Recovery

a. Personnel involved in a DRP (Disaster Recovery Plan) recovery situation would include but may not be limited to the following:

- ~~Christopher Sorensen,~~ -Director
- ~~Karri Harvey,~~ Management Information Supervisor
- ~~Nancy Walker,~~ Deputy Director
- ~~Kathy Herding,~~ Financial Assistance Supervisor
- ~~Cindy Nelson,~~ SS and PH Division Directors
- ~~Loren Stromberg,~~ Lyon County Administrator
- ~~Ron Krause,~~ Lyon County Facilities Manager

b. Based on the level of disaster, the members present, and availability of resources job responsibilities will be assigned accordingly.

c. Duties

IT Personnel

- Provide technical support for hardware removal
- Cleanup wiring
- Replace physical equipment
- Test repairs

Director and County Administrator

- Declare level of disaster
- Initial notification of disaster team
- Assist with assessment of the extent of damage
- Authorize purchases and required disbursements
- Oversee recovery status

DRP team

- Determine relocation site and required equipment
- Assign personnel to alternate if needed
- Provide support in the cleanup of the data center or alternate site
- Test repairs

I.T. Supervisor

- Determine which equipment is destroyed
- Review with DRP team
- Contact contracted vendors for replacements
- Provide support in the cleanup of the date center or alternate site
- Test repairs

Materials List

- Telephone sets
- Personal computers
- Network cables
- Server hardware
- Blank computer tapes
- Desks
- Chairs
- Non-computer equipment

Vendor List

- Frontier Phone Company (Slayton and Ivanhoe) 507-372-2266
- Trimin Government Solutions (IFS accounting software) 320-259-5007
- Computer Professional Unlimited (CPU) (Payroll and Lyon County phone system) 320-589-2110
- Fran's Communication (General telephone wiring and Lyon County phone system) 507-532-6467
- CPS Technology Solutions (IBM I-series hardware maintenance contract holder) 800-438-7761
- Office of the Enterprise Technology (OET) (State of MN DHS systems, phone lines, data lines, Maxis, MMIS, and Prism)
- The Computer Man, Inc. (Computer hardware supplier and software maintenance engineer on CISCO equipment) 507-532-7562
- IBM (I-series hardware maintenance) 800-426-7378

Section 6 - Recovery procedures after disaster

a. Assemble technical and management team

b. Determine level of disaster

c. Assemble clean up or technical team and repair existing site or prepare alternate site

d. Establish communications links-phone and data

e. Environment; heat, a/c, power, furniture

f. Begin hardware replacement or salvage current equipment

g. Reassemble and review requirements and prepare additional needs list for vendors

h. Acquire backup copies of necessary data and backup tapes

i. Inform all personnel of the public of recovery place with short and long term expectations

j. Acquire backup copies of necessary data and backup tapes

k. Contact State of MN to reroute email etc. to alternate site

Section 7 - Testing of DRP

a. ~~Initial tests of entire shutdown at Lyon County site with Murray and Lincoln as alternate sites were conducted in August of 2008.~~ The State of MN does tests of SSIS restores and other State systems on a regular basis. Monthly system soft tests are performed during regular updates and the rebooting of each of the servers.

b. Making of alternate sites into a primary site in case of physical disaster may mean adding some hard drive space for long term (over 30 days) to restore non-essential data from offsite backup tapes. Tape drives or other form of backup media would need to be acquired from a vendor to restore tapes, and to perform on-going backups, as these servers do not currently have a tape drive.

Section 8 – Contract with other Entities

a. Each county is responsible for their own DRP. SWHHS is responsible to maintain systems and get them back up and online in accordance to their policy. All critical servers will be back online and restored dependent on the type of disaster and equipment needed.

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 9

EFFECTIVE DATE: 01/01/11
REVISION DATE: ~~11/18/15~~, 06/15/16
AUTHORITY: Southwest Health and Human Services Joint Governing Board

~~---RISK MANAGEMENT AND ASSSEMENT PLAN~~PHYSICAL AND TECHNICAL SAFEGUARDS----

Section 1 - Purpose

a. The purpose of this policy is to detail the ~~risk management and assessment procedures~~Physical and Technical Safeguards for Southwest Health and Human Services. This policy identifies the following:

- Tape Backups
- Workstation Security
- ~~Passwords~~
- Security of Data Center~~computer are~~
- Firewalls, Virus Software, and Spam/Internet Filters
- Battery power and generators
- Access to computer systems
- ~~Staff Expectations~~
- Assessment of Controls
- Contingency Plan~~ and Risks~~
- Device and Media Accountability, Backup and storage, Disposal and Reuse
- Technical Safeguards

Section 2 - Tape Backups

a. All servers are backed up to synology data stor. The Friday tape is stored off site in a fireproof safe. Month end tapes are saved for 12 months. Year end tapes are saved permanently. This function is performed by Information Technology Specialist.

~~Section 3 – Passwords~~

~~a. All systems 15 character passwords which require changing every 30 days. Passwords must be unique and cannot be reused for 6 months. Server passwords require alphabetic numeric and special characters. Only IT personnel have access to the server (administrator) passwords.~~

Section 34 – Workstation Security

a. Workstations are secured in the following ways:
- Hard drive encryption
- Unique usernames
- Passwords that adhere to the password policy, 15 character alpha number.
- Locking of computer when not in use or stepping away from workstation
- Limited access, shutting office doors, making sure monitors are not easily seen and if they are in the direction of a walkway have the appropriate privacy screen filters installed and used.

Section 4 - Security of ~~Computer Area~~Data Center

a. The doors to the ~~computer room~~Data Center are locked at all times. Only authorized personnel have access to the ~~computer room~~Data Center and work area. Internal video surveillance is installed and monitored. Recorded data can be reviewed if necessary.

Section 5 - Firewalls, Virus Software, and Spam/Internet Filters

a. There is a Cisco firewall in place to restrict outside intrusion of the network. Anti-Virus software is in place and updated daily on all personal computers and servers. There is a spam filter in place to monitor and filter all incoming mail. There is an anti-malware and anti-exploit software installed and updated daily.

Section 6 - Battery Power and Generators

a. All servers are powered by uninterruptable power supply batteries, which in turn are backed up by a fuel powered generator.

Section 7 - Access to computer systems

a. Access to the various computer systems functions are restricted to specific employees depending on their job requirements. Supervisors determine the access needed by their staff. ~~This access is reviewed at least annually.~~

~~Section 8 - Staff Expectations~~

~~a. Staff are expected to safeguard data and their access to computer systems at all times. Passwords are not to be shared. Staff is expected to lock their computer when leaving their office or workstation. Monitors are not to be facing clients when accessing data. Staff only have access to data they need in order to~~

~~perform the duties of their position. Supervisors are expected to monitor staff activities and direct staff to make changes when risks are identified. Each year staff will sign the Employee Responsibilities: Data Privacy form attached with their performance evaluation. Supervisors will routinely and at least annually discuss data privacy with staff at a department staff meeting.~~

Section ~~9~~8 - Assessment of Controls

a. Each location has unique security dependent on building controls. All servers and switches are behind locked doors with limited access.

- **Marshall:** Building security is controlled by Lyon County, there are security devices that allow for after-hours access to the building via employee badges. Doors to both Human Services and Public health offices have key pad entries and the code is changed when there is a change in staffing. IT has a separate area that houses the data center and IT staff, there is a separate keypad entry with code as well as key locks only available to IT staff and janitorial staff. The front desk staff is protected by safety glass.
- **Redwood:** Building security is maintained by Redwood County. Physical access to the building is controlled by key lock and monitored by surveillance cameras. There is a key fob door control to employee office area both for Human Services, Public Health and Eligibility worker area. IT equipment is in the janitorial room with a locked cage securely housing the switches. The service is located in the courthouse with Redwood County's IT secure data center that is controlled with limited access by their IT staff with key. The front desk staff is protected by safety glass. Child support in the court house has keyed lock.
- **Slayton:** Building security is maintained by Murray County, physical access is granted by key. Employee office area for both Human Services and Public health is accessed by keypad entry. IT equipment is in the janitorial room with limited access by key. The front desk staff is protected by safety glass.
- **Luverne:** Physical security is maintained by Rock County. Physical access to the building is by key lock. There is a keypad that grants access to the human services and public health area. The front desk staff is protected by safety glass. Switches are located in a wiring closet with limited key access. The server is located in the Rock County Courthouse that is in their data center controlled by limited locked access. The front desk staff is protected by safety glass.
- **Ivanhoe:** Building security is maintained by Lincoln County. Physical access is granted by key. Human Services and Public Health have separate keyed entrances. Human Services is in multiple areas within the lower level of the courthouse. IT equipment is located in a secure locked

cage with limited access.

- **Pipestone:** Has keyed external lock and keyed internal lock. Switches are located in locked wiring closet, server is located in locked are in Courthouse with Pipestone County Servers. Front desk staff is protected by glass.

b. ~~It is expected that Supervision will consider risk assessment in business decisions.~~ Supervisors are expected to report any concerns with ~~risk management~~physical or technical security to the Director immediately. ~~Annually all supervisors will review staff access. The IT Manager will assess at least semi-annually, computer safeguards required to ensure security and minimize risk.~~

c. Defining access control and validation. Southwest Health and Human Services maintains access to physical locations determined by job specificity. IT staff that have proper BCA clearance are allowed in the data center or secure areas. Janitorial staff also have a proper BCA background check and clearance. Staff are given access to working areas using the keypad or key fob systems in each location. Areas controlled by keys are determined by supervisors and job descriptions.

d. Maintenance records. A signature log is created at the front desk area of all vendors including maintenance repair that would access secure areas. The only exception is in Marshall where the data center is located in a different area of the building. IT maintains a written log of outside professionals who have access for maintenance to buildings or structure.

Section ~~10~~9 – Contingency Plan

a. This policy defines how the physical spaces are protected when emergency mode operations are put into effect. Logging of authorized personnel will be maintained of all law enforcement, IT, Directors, Vendors, or designated staff that will need access to the area. Those that don't have security clearance will be accompanied by a member of the staff at all times. If the security of the physical area is compromised during an emergency, we will restore systems at one of our other 5 locations to maintain the integrity of our data. Any hardware that is in a compromised area will be removed and stored securely.

Section ~~11~~10 - Device and Media Accountability, Backup and Storage, Disposal and Reuse

a. Laptops, Desktops, Servers and mobile devices are used by staff according to their job description. A working inventory is used and updated routinely by IT staff. All items contain a barcode that has data linked including the serial

number, purchase date, warranty and employee that it was distributed to.

b. Once an employee leaves, equipment is returned to IT staff and securely stored until re-issuance. Prior to re-issuing equipment laptops, desktops, and/or mobile devices are wiped and reloaded so previously stored data is not compromised. Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.
~~1. Once an employee leaves equipment is returned to IT staff and securely stored until re-issuance. Prior to re-issuing equipment laptops, desktops, and/or mobile devices are wiped and reloaded so previously stored data is not compromised. Any equipment or storage media that contains confidential, critical, internal use only, and/or private information will be erased by appropriate means or destroyed by the Security Officer or his/her appointed designee before the equipment/media is reused.~~

c. Disposal: All electronic protected health information (e~~E~~PHI) on decommissioned devices and storage media must be irretrievably destroyed, in order to protect the confidentiality of the data contained. If the device or media contains e~~E~~PHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data. If the device or media contains the only copy of e~~E~~PHI that is required or needed, a retrievable copy of the e~~E~~PHI must be made prior to disposal.

d. Removable magnetic "disks" (floppies, ZIP disks, and the like) and magnetic tapes (reels, cartridges) can be "degaussed" by an appropriately-sized and -powered degasser or physically destroyed.

e. Fixed internal magnetic storage (such as computer hard drives), as well as removable storage, can be cleansed by a re-writing process. Software is used to over-write all the usable storage locations of a medium. The simplest method is a single over-write; additional security is provided by multiple over-writes with variations of all 0s, all 1s, complements (opposite of recorded character), and/or random characters.

f. A few kinds of "write-many" optical media (such as CD-RWs) can be processed via an over-write method. This is not the case for the vast majority of "write-once" optical media in use (notably the CD-R). Because such media are optical rather than magnetic, they cannot be degaussed. For the write-once variety, only physical destruction will do.

g. Removable "solid state" storage devices are also now available. These "flash memory" devices are solid state and are non-volatile (the memory maintains data even after all power sources have been disconnected). Examples include CompactFlash, Memory Stick, Secure Digital, Smart Media and other types of plug-ins, and a range of "mini-" and "micro-drive" flash devices that use USB or FireWire ports. Secure overwrites (following manufacturer specifications) are possible for these media as well. Neither degaussing nor over-writing offers absolute guarantees. Unless, of course, one is willing to disintegrate, incinerate, pulverize, shred, or smelt. As with paper, the method of disposal depends on the perceived risks of discovery, and estimates of the type of threat.

h. Paper containing sensitive information should be shredded. Strip cut shredders (also called straight cut or spaghetti cut) render paper into thin, long strips.

i. End of life for equipment: Once equipment reaches its usable expectancy, hardware is properly disposed of. Hard drives are erased using Kill disk with DDOS level (U.S. Department of Defense level) features. After hard drives have been Killdisked, they are stored in the data center until they can be taken to DHS MN.IT Services, 444 Lafayette Road N, St. Paul, MN 55101, where they are shredded. (This includes all tapes, disks, storage devices) PC's, laptops, servers, printers are all recycled through local resources in a manner that is environmentally friendly.

~~a) Removable magnetic "disks" (floppies, ZIP disks, and the like) and magnetic tapes (reels, cartridges) can be "degaussed" by an appropriately-sized and -powered degasser or physically destroyed.~~

~~b) Fixed internal magnetic storage (such as computer hard drives), as well as removable storage, can be cleansed by a re-writing process. Software is used to over-write all the usable storage locations of a medium. The simplest method is a single over-write; additional security is provided by multiple over-writes with variations of all 0s, all 1s, complements (opposite of recorded character), and/or random characters.~~

~~c) A few kinds of "write-many" optical media (such as CD-RWs) can be processed via an over-write method. This is not the case for the vast majority of "write-once" optical media in use (notably the CD-R). Because such media are optical rather than magnetic, they cannot be degaussed. For the write-once variety, only physical destruction will do.~~

~~d) Removable "solid state" storage devices are also now available. These "flash memory" devices are solid state and are non-volatile (the memory maintains data even after all power sources have been disconnected). Examples include CompactFlash, Memory Stick, Secure Digital, Smart Media and other types of plug-ins, and a range of "mini-" and "micro-drive" flash devices that use USB or FireWire ports. Secure overwrites (following manufacturer specifications) are possible for these media as well.~~

~~Neither degaussing nor over-writing offers absolute guarantees. Unless, of course, one is willing to disintegrate, incinerate, pulverize, shred, or smelt. As with paper, the method of disposal depends on the perceived risks of discovery, and estimates of the type of threat.~~

~~e) Paper containing sensitive information should be shredded. Strip cut shredders (also called straight cut or spaghetti cut) render paper into thin, long strips. Cross-cut shredders (also~~
~~Policy: HIPAA Device and Media Control 3~~

~~End of life for equipment: Once equipment reaches its usable expectancy, hardware is properly disposed of. Hard drives are erased using Kill disk with DDOS level (U.S. Department of Defense level) features. After hard drives have been Killdisked, they are stored in the data center until they can be taken to DHS MN.IT Services, 444 Lafayette Road N, St. Paul, MN 55101, where they are shredded. (This includes all tapes, disks, storage devices) PC's, laptops, servers, printers are all recycled through local resources in a manner that is environmentally friendly.~~

Section ~~12~~1 - Technical Safeguards

a. Unique User Identification:
- Southwest Health and Human Services IT staff will assign a unique name and/or number for identifying and tracking user identity.

b. Emergency Access Procedures:
- Emergency Access will be established by the Security Officer and as directed in Admin Policy #8 - Disaster Recovery Plan.
- When leaving workstation area, staff must log off their workstation.

c. Encryption and Decryption of PHI:
- All hard drives are encrypted using HP Protect tools or Bitlocker Drive Encryption. Decryption is performed only during times of repair or if data becomes corrupt. The Decryption key is located in the Data Center which has limited access. Email is encrypted by ZIX mail, it is automatic and works with minimal effort from the sender, "Securemail" is to be used as part of the subject line.

d. Audit Controls:
- Audit Controls in place such as user account controls which lock an end-user out of their account after 3 attempted log in failures. Log reports are gathered through Kiwi syslogger for VPN access. Log files are gathered through Appxtender to be reviewed as necessary.

- Southwest users seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.
- Southwest users are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.
- A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting EPHI.

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 10

EFFECTIVE DATE: 01/19/11
REVISION DATE: 12/17/14, 06/15/16
AUTHORITY: Southwest Health and Human Services Joint Governing Board

--- LAN, E-MAIL, INTERNET ACCESS, AND PERSONAL COMPUTING EQUIPMENT ---

Section 1 - Introduction

a. This policy has been prepared to serve as a guide for the effective and efficient use and operation of Southwest Health and Human Service Local Area Network (LAN). Hereinafter, Southwest Health and Human Services will be referred to as Agency. It is also to provide guidance on use of e-mail and Internet access associated with the Agency LAN.

b. The LAN is to be used for conducting Agency business. Any information created or stored on the Agency LAN is the property of the Agency. The Agency reserves the right to monitor LAN usage to determine compliance with this policy.

c. Any deviation from the established policy of operation and use will be recognized only on the authority of the Southwest Health and Human Services Governing Board or its designee.

Section 2 - Definitions

a. Local Area Network (LAN): That system comprised of all equipment associated with a computer network including, but not necessarily limited to, Agency provided computer, monitor, keyboard, mouse, printer/s, servers, and software.

b. Electronic Mail (e-mail): Text based, electronic communications distributed via a communications network. This can include documents, memos, data, or other electronically transmitted communications. It is Agency property and intended for Agency business. All data and other electronic messages within this system are the property of the Agency.

c. Internet Access: Access via Agency network connection to the Internet.

Section 3 - System Security

a. Password Protection - Access to the LAN system will be password protected. Do not share your password with other employees and especially non-Agency personnel. If non-Agency personnel need access to the LAN, the department head should contact the ~~data processing~~IT department.

b. Software - As viruses and security are of major concern, the only software to be used on the LAN system is that which is provided by the Agency. Employees will not be allowed to add software to their PC or introduce information or data from outside the Agency without permission from their supervisor and the ~~data processing~~IT department.

Only ~~A~~agency standard software is allowed. Any other software must be approved by ~~data processing~~IT prior to purchasing and installation on any PC or the LAN.

It is understood that there may be occasions when it is necessary to introduce data from outside the Agency LAN. All data must be screened for viruses prior to introduction into the LAN system.

~~c. Screen Lock - Employee work stations will automatically lock off after 5 minutes of inactivity. Staff shall lock their work station if leaving their desk.~~

Section 4 - Hardware/Personal Computing Equipment

a. Only ~~A~~agency supplied computer hardware and associated peripherals are allowed to be used. Personally supplied devices may not be connected to ~~A~~agency equipment, unless required and authorized by ~~data processing~~IT for specific business reasons.

Section 5 - Electronic Mail

a. Purpose - The Agency supports utilizing e-mail to increase timely and effective business communications throughout the Agency. The purpose of this policy is to encourage appropriate use of e-mail as an effective and efficient business communications tool.

b. Access - All employees of the Agency will have access to e-mail.

c. Security and Administration - Individual e-mail access will be password protected. While this security measure is beyond the usual measure taken to protect access to paper records and telephones, it should be recognized that no system of communication is completely secure, including e-mail.

An employee's e-mail address is owned by the Agency. When an individual's employment with the Agency is terminated, the e-mail administrator may either remove that individual's e-mail address or redirect their e-mail to another employee.

Problems or issues regarding e-mail should be directed to the ~~data processing~~IT unit. Guest e-mail accounts for individuals not employed by the Agency may be allowed in appropriate circumstances and will always be password protected.

d. Appropriate E-mail Usage and Guidelines - The e-mail system is provided by the Agency for your use as an employee of the Agency. Access to e-mail is a privilege not a prerogative and certain responsibilities accompany that privilege. Users of e-mail are expected to be ethical and responsible in their use. E-mail is subject to all of the same laws, policies, and practices that apply to the use of other forms of communications such as telephones and paper records.

Incidental or occasional personal use may be permitted subject to the limitations of this policy and provided such personal use: (1) does not interfere with the employee's or any other employee's job duties or routine business activities; (2) does not result in additional expense to the agency; (3) does not require modification to software or other system components; (4) is not for political, religious, unlawful or illegal practices, personal financial profit, or other promotional activities; (5) does not result in the consumption of Aagency resources; (6) does not contain or imply threatening, obscene, or abusive language; and (7) does not contain or imply harassing, demeaning, or sexually explicit statements or materials.

Employees are not permitted to use or access pop up or chat mail unless authorized or pre-installed by IT. The only e-mail that may be used on agency computers is Microsoft Outlook, which is on the Agency LAN.

e. Inappropriate Uses of Agency Computer Systems - It is a violation of policy for any employee, including supervisors, to use the computer systems for the purposes of satisfying idle curiosity about the affairs of others, with no work related purpose for obtaining access to the files, data, or communications of others.

It is also a violation for employees to intentionally intercept, eavesdrop, record, alter, read, or receive other employee's e-mail without proper authorization.

Other violations of this e-mail policy that WILL NOT be tolerated include, but are not limited to:

- illegal activities
- wagering or betting activities
- harassment of any kind
- solicitation, except for Agency-sanctioned activities
- commercial activities
- promotion of political or religious positions or activities
- other unethical activities

f. E-mail Review - The Agency, at its discretion, may also use computer programs that monitor e-mail messages electronically, checking for particular words or patterns of activity, for purposes of assuring system security and compliance with policies.

Supervisors have the right to review the contents of employees' e-mail communications.

~~g. Passwords - Passwords shall be periodically changed to ensure security of the LAN. Users should not share their passwords with anyone except their supervisor.~~

~~Supervisors or management may access an employee's e-mail if employees are on leave of absence, vacation, or are transferred from one department to another department or~~

~~it is necessary for Agency business purposes.~~

~~g~~h. Retention of E-mail - Generally, e-mail messages are temporary communications which are non-vital and may be discarded on a routine basis. However, depending on the content of the e-mail message, it may be considered a more formal record and should be printed and retained pursuant to a department's record retention schedules. Examples of messages of this nature are: policy, decision making connected to specific case files, contract related or otherwise an essential part of a larger record, or other memorandum of significant public business. As such, e-mail messages are similar to printed communication and should be written with the same care.

Employees should be aware that when they have deleted a message from their mailbox it may not have been deleted from the e-mail system. The message may be residing in the recipient's mailbox or forwarded to other recipients. Furthermore, the message may be stored on the LAN server's backup system.

Section 6 - Internet Access

a. Purpose - Internet access provides the Agency with significant access and dissemination of information to individuals outside the Agency. The use of the Internet access is intended to serve Agency business. Like all e-mail messages, messages sent through the Internet are capable of being forwarded without the express permission of the original author. Therefore, users must use caution in the transmission and dissemination of messages outside of the Agency LAN, and must comply with all state and federal laws.

The use of Internet access is intended to serve Agency business. Incidental or occasional personal use may be permitted subject to the limitations of this policy and specifically, subject to the same limitations stated in this policy's section on the personal use of e-mail. The Agency, at its discretion, under the direction of the LAN Administrator, may use computer programs to monitor Internet use electronically for the purpose of assuring system security and compliance with policies.
~~e-mail. The Agency, at its discretion, under the direction of the LAN Administrator, may~~

~~use computer programs to monitor Internet use electronically for the purpose of assuring system security and compliance with policies~~.

b. Web Radio - Internet Web sites that use streaming video or audio, such as radio stations, are not allowed, except for training or specific business purposes!

c. **Caution!!** Computer viruses can enter our computer system through the Internet. To prevent this **do not** download any software, files, or screen savers from the Internet without authorization from your supervisor and assistance from ~~Data Processing~~IT.

Section 7 - Applicability

a. This policy applies to all individuals who are provided access to the LAN, Internet, and e-mail systems.

~~**Section 8 - Penalties**~~

~~a. As per Agency policies, the misuse of the LAN, Internet access, or e-mail system privileges shall be grounds for discipline up to and including dismissal. In addition, violations of this policy or misuse of the system may be referred for criminal prosecution.~~

ADMINISTRATIVE POLICY NUMBER 14 – HIPAA

Due to the extensive changes, the current HIPAA policy will be deleted in its entirety and will be replaced with the attached document.

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 14

EFFECTIVE DATE: 02/15/12
REVISION DATE: 12/17/14, 06/15/16
AUTHORITY: Southwest Health and Human Services
(SWHHS) Joint Governing Board

---HEALTH CARE INSURANCE PORTABILITY & ACCOUNTABILTY ACT (HIPAA)---

Table of Contents

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 14

Section 1 – Definitions

Access: Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Agent: An agent of the Agency is determined in accordance with federal common law of agency. The Agency is liable for the acts of its agents. An agency relationship exists if the Agency has the right or authority of the Agency to control the agent's conduct in the course of performing a service on behalf of the Agency (i.e. give interim instructions, direct the performance of the service).

Agency: For the purposes of this policy, the term "Agency" shall mean SWHHS to which the policy and breach notification apply.

Audit: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing. Audit activities shall also take into consideration SWHHS' information system Risk Assessment results.

Audit Controls: Technical mechanisms that track and record computer/system activities.

Audit Logs: Records of activity maintained by the system which provide: 1) date and time of significant activity; 2) origin of significant activity; 3) identification of user performing significant activity; and 4) description of attempted or completed significant activity.

Audit Trail: Means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events (audit logs) that relate to an operating system, an application, or user activities. Audit trails provide:

- Individual accountability for activities such as an unauthorized access of ePHI;
- Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information; and
- Problem analysis such as an investigation into a slowdown in a system's performance.

An audit trail identifies who (login) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time).

Breach: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Breach excludes:

- Any unintentional acquisition, access or use of PHI by an employee or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate (BA): Under the HIPAA Privacy and Security Rules, a person (or entity) who is not a member of the covered entity's workforce and who performs any function or activity involving the use or disclosure of individually identifiable health information or who provides services to a covered entity that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc.

Business Associate Agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by a covered entity and business associate that establishes permitted and required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Covered Entity (CE): A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

Designated Record Set (DRS): For the Agency's purposes, the following is defined as a designated record set. A group of records maintained by the Agency that is;

- The medical records and billing records about individuals,
- The enrollment, payment, claims adjudication, and case management record systems

maintained by the agency,
- Used, in whole or in part, by or for the Agency to make decisions about individuals.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Health Care Operations: Health care operations mean the legitimate business activities of our practice. These activities may include quality assessment and improvement activities; fraud & abuse compliance; business planning & development; and business management & general administrative activities. These can also include agency telephoning an individual to remind an individual of appointments, or using a translation service if there is a need to communicate with an individual in person, or on the telephone, in a language other than English.

HIPAA Privacy and Security Risk Management Team: Individuals who are knowledgeable about the Organization's HIPAA Privacy and Security policies, procedures, training, computer system set up, and technical security controls, and who are responsible for the Risk Management process and procedures outlined in this policy. This team is comprised of the Security Officer, Privacy Officers, Director, Deputy Director, Social Services Division Director and other team members as needed.

Individually Identifiable Health Information: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Need to Know: Employees will only be given information that the employee needs to have in order to accomplish a given function and only for proper administration of an appropriate health-related program and HIPAA.

Payment: Payment means our activities to obtain reimbursement for the medical services provided to an individual, including billing, claims management, and collection activities. Payment also may include an individual's insurance carrier's efforts in determining eligibility, claims processing, assessing medical necessity, and utilization review. Payment may also include activities carried out on our behalf by one or more of our collection agencies or agents in order to secure payment on delinquent bills.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the Agency, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Privacy Regulation: Policies and procedures required by HIPAA Standards for Privacy of PHI.

Record: Means any item, collection, or grouping of information that includes PHI data and is maintained, collected, used or disseminated by the Agency.

Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

Risk Assessment: (Referred to as *Risk Analysis* in the HIPAA Security Rule); the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place. The Risk Assessment includes administrative, physical, technical and organizational safeguards that enable and govern ePHI that is received, created, maintained or transmitted;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: Within this policy, it refers to two major process components: Risk Assessment and Risk Mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only.

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks

determined in the Risk Assessment process to satisfactory levels within the Agency given its mission and available resources.

Tennessen Warning: The government must give individuals notice when collecting private or confidential information from them. This is referred to as a "Tennessen warning notice." Government may also call it a "privacy notice," a "notice of collection of private/confidential data," or something similar. The purpose of the notice is to enable people to make informed decisions about whether to give information about themselves to the government.

Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-employees, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Threat Action: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Threat Source: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the Agency's ability to protect ePHI.

Treatment: Treatment means the provision, coordination, or management of an individual's health care and related services by health care providers involved in an individual's care. Students may be a member of the health care team. It includes the coordination or management of health care by a provider with a third party insurance carrier, communication with lab or imaging providers for test results, consultation between agency clinical staff and other health care providers relating to an individual's care, or agency referral of an individual to a specialist physician or facility. Agency treatment includes collaboration with other community agencies to address an individual's health needs, including schools, community action agencies, food shelves, transportation providers who are not typically considered "health care" providers.

Trigger Event: Activities that may be indicative of a security breach that require further investigation.

Unsecured Protected Health Information: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

- Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
    - Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission).
- The media on which the PHI is stored or recorded has been destroyed in the following ways:
    - Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Workforce: Workforce means employees, Board members, volunteers, trainees, students and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

Section 2 – Purpose

a. The Federal Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. HIPAA responds to concerns from citizens, the health care industry and government agencies for enhanced security and privacy of individual health information. In passing HIPAA, Congress intended to:
    - Improve the portability and continuity of health insurance coverage for consumers;
    - Combat waste, fraud, and abuse in health insurance and health care delivery;
    - Standardize electronic data interchanges between health care organizations;
    - Protect the security, privacy, and availability of individual health information.

Section 3 - Privacy Officers and Security Officer

a. Dale Hiland, Social Services Supervisor and Carol Biren, Public Health Director are the designated Privacy Officers and Karri Harvey, Management Information Supervisor is the Security Officer for HIPAA purposes. These people are responsible for the development and implementation of the policies and procedures required by HIPAA Standards for Privacy of Individuals Identifiable Health Information (IIHI) or Electronic Individuals Identifiable Health Information (eIIHI), hereafter referred to as Protected Health Information (PHI) and the privacy regulation. The Privacy Officers also serve as the people to receive complaints and who should provide further information about matters covered by the privacy notice. The Privacy Officers need to be familiar with the privacy regulation. Delegation of some of these duties may be given to other employees of the agency. Responsibilities of the Privacy Officers and Security Officer will include:

- Building a strategic and comprehensive privacy program that defines, develops, maintains and implements policies and procedures that enable consistent, effective privacy and security practices which minimize risk and ensure the confidentiality of PHI, paper and/or electronic, across all media types. Ensures privacy forms, policies, standards, and procedures are up-to-date.
- Serves in a leadership role for privacy compliance.
- Privacy Officers collaborate with the Security Officer to ensure alignment between security and privacy compliance programs including policies, practices, investigations, and acts as a liaison to the IT department.
- Privacy Officers establishes, with the Security Officer, an ongoing process to track, investigate and report inappropriate access and disclosure of PHI. Monitor patterns of inappropriate access and/or disclosure of PHI.
- Performs or oversees initial and periodic HIPAA Privacy and Security Risk Assessment and Risk Mitigation Plans.
- Facilitates audits to validate Security compliance efforts throughout the Agency.
- Takes a lead role, to ensure the Agency has and maintains appropriate privacy and confidentiality consents, authorization forms and information notices and materials reflecting current Agency and legal practices and requirements.
- Oversees, develops and delivers initial and ongoing privacy and security training to the workforce.
- Participates in the development, implementation, and ongoing compliance monitoring of all business associates and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
- Works cooperatively with Public Health and other applicable Agency units in overseeing patient rights to inspect, amend, and restrict access to PHI when appropriate.
- Manages all required breach determination and notification processes under HIPAA and applicable State breach rules and requirements.

- Establishes and administers a process for investigating and acting on privacy and security complaints.
- Performs required breach investigations, documentation, and mitigation. Works with Human Resources to ensure consistent application of sanctions for privacy and security violations.
- Initiates, facilitates and promotes activities to foster information privacy and security awareness within the Agency and related entities.
- Maintains current knowledge of applicable federal and state privacy laws and accreditation standards.
- Works with Agency administration, legal counsel, and other related parties to represent the Agency's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.
- Cooperates with the U.S. Department of Health and Human Service's Office for Civil Rights, State regulators and/or other legal entities in any compliance reviews or investigations.
- Serves as information privacy resource to the Agency regarding release of information and to all departments for all privacy related issues.

Section 4 - Use and Disclosure

a. **Uses and Disclosures** - For appropriate uses, the Agency is permitted to use and disclose PHI as follows:
   - To the individual who is the subject of the data.
   - Those persons or entities that are authorized by the client to receive their PHI.
   - Those entities that are required or allowed by the privacy regulations and state law.
   - Those employees on a need to know basis. Employees will only be given information that the employee needs to have in order to accomplish a given function.

b. **Disclosure of Information**
   - Requests for copies of PHI in the DRS shall be managed by the Privacy Officers.
   - Employees will not release PHI without approval of Privacy Officers.
   - Please refer to the Request for PHI (section 5) for specific practice.
   - All clients will be required to sign the Notice of Privacy and the Authorization for Release of Information or the Tennessen Warning at the time of the initial visit and annually thereafter for the release/Tennessen, which will include the statement for disclosure of PHI for the purposes of treatment, payment, and healthcare operations.

- Two attempts will be made to obtain signature on above documents. If unable to obtain required signatures, the notice and release will be provided by mail. This will be documented in the client's file.

c. **Confirmation of a Valid Authorization**

- A valid authorization consists of a written request that includes:
  - Name of client
  - Who is disclosing the information
  - Who is receiving the information
  - Description of information being disclosed
  - Purpose of disclosure
  - Signature and date
  - Effective / Expiration date
  - Statement of right to revoke
  - Statement of condition of treatment, payment, and healthcare operations
  - Potential for redisclosure
- If any pieces of the authorization above are missing, the requestor will be contacted and requested to properly complete a disclosure for PHI.
- If the patient is a minor, the parent and/or guardian is responsible for the signature on the authorization. SWHHS will provide verification that the individual is the responsible party for the patient.

d. **Routine and Non-Routine Disclosures** will be individually evaluated and processed per request. The Agency will ensure that only the minimum amount of information is disclosed to satisfy the request.

e. **Limit Use Disclosures to Those Authorized by the Client**

PHI will be provided to the individual and to the Office of Civil Rights. Disclosure of PHI will be allowed under the following circumstances:

- If the client has authorized a use or disclosure;
- If the disclosure is for health care operations, payment or treatment and the client has signed a consent form for the Agency, or a consent form is not required;
- If the client has agreed to the disclosure for a facility directory or to an individual necessary for the care of the individual; or
- If the disclosure is one of the social responsibility disclosures and all conditions for such disclosure are met. Social responsibility disclosures include:
  - Uses and disclosures required by law;
  - Use and disclosures for public health activities;
  - Disclosures about victims of abuse, neglect or domestic violence;

- Uses and disclosures for health oversight activities;
- Disclosures for judicial and administrative hearings;
- Disclosures for law enforcement purposes;
- Uses and disclosures about decedents;
- Uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- Uses and disclosures to avert a serious threat to health or safety;
- Uses and disclosures for specialized government functions; and
- Disclosures for workers' compensation.

f. **Limit Request to Minimum Necessary**

The Agency will limit its requests for disclosure of PHI to the amount necessary to accomplish the purpose for which the request is made. Only individuals with a legitimate need to know may use or disclose PHI. Each individual may only use or disclose the minimum information necessary to perform their designated role regardless of the extent of access provided to them.

g. **Ability to Rely on Request for Minimum Necessary**

The Agency may rely on a reasonable request as the minimum necessary for the stated purpose(s) when:

- The disclosure is to a public official as allowed in the social responsibility reporting.
- The information is requested by another covered entity.
- The information is requested by an employee or business associate of the agency.

h. **Verification Policies**

Before disclosing PHI, the Agency will verify the identity of the person requesting the PHI and the authority of that person to have access. The Agency may rely on written statements, if such reliance is reasonable. For public officials, the Agency may rely on an identification badge or a letter written on government letterhead.

For requests by phone, the Agency will obtain a number to return the call, establish the legitimacy of the number provided, call the person back at the verified number, and confirm that the person is who he or she claims to be. The Agency will treat a personal representative as the individual for purposes of the privacy regulations:

- A personal representative is someone who has, under applicable law, the authority to act on behalf of an individual in making decisions related to health care.
- The Agency will abide by special provisions for un-emancipated minors, deceased individuals, and abuse-neglect and endangerment situations.

i. **Uses and Disclosures of PHI Permitted or Required by Law**

In some circumstances, SWHHS may be legally bound to use or disclose an individual's PHI without an individual's consent or authorization. State and federal privacy law permits or requires such use or disclosures regardless of an individual's consent or authorization in certain situations, including, but not limited to:

- **Emergencies:** If an individual is incapacitated and requires emergency medical treatment, the Agency will use and disclose PHI to ensure the necessary medical services are received. The Agency will attempt to obtain consent as soon as practical following treatment.
- **Others involved in an individual's Healthcare:** Upon an individual's verbal authorization, the Agency may disclose, to a family member, close friend or other person an individual designates, only that PHI that directly relates to that individual's involvement in an individual's healthcare and treatment. The Agency may also need to use PHI to notify a family member, personal representative or someone else responsible for an individual's care of an individual's location and general condition.
- **Communication barriers:** If the Agency tries but cannot obtain an individual's consent to use or disclose an individual's PHI because of substantial communication barriers and an individual's physician, using his or her professional judgment, infers that an individual consents to the use or disclosure, or the physician determines that a limited disclosure is in the individual's best interests, the Agency may permit the use or disclosure.
- **Required by Law:** The Agency may disclose PHI to the extent that its use or disclosure is required by law. This disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law.
- **Regulatory Activities:** The Agency may disclose PHI to an authorized public health authority to prevent or control disease, injury, or disability or to comply with state child or adult abuse or neglect law. The Agency is obligated to report suspicion of abuse and neglect to the appropriate regulatory agency.
- **Food and Drug Administration:** The Agency may disclose PHI to a person or company as required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations as well as to track product usage, enable product recalls, make repairs or replacements or to conduct post-marketing surveillance.
- **Health oversight activities:** The Agency may disclose an individual's PHI to a health oversight agency for audits, investigations, inspections, and other activities necessary for the appropriate oversight of the health care system and government benefit programs such as Medicare and Medicaid.
- **Judicial and administrative proceedings:** The Agency may only disclose an individual's PHI in the course of any judicial or administrative proceeding in response to a court order expressly directing disclosure, or in accordance with

specific statutory obligation compelling us to do so, or with individual's permission.

- **Law enforcement activities:** The Agency may not disclose an individual's PHI to a law enforcement officer for law enforcement purposes without court order, statutory obligation or patient authorization.
- **Coroners, medical examiners, funeral directors and organ donation organizations:** The Agency may disclose an individual's PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other lawful duties. The Agency also may disclose an individual's PHI to enable a funeral director to carry out his or her lawful duties. PHI may also be disclosed to organ banks for cadaveric organ, eye, bone, tissue and other donation purposes.
- **Serious threats to health or safety:** The Agency may disclose an individual's PHI to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
- **Military activity & national security:** The Agency may disclose the PHI of members of the armed forces for activities deemed necessary by appropriate military command authorities to assure proper execution of the military mission. The Agency also may disclose an individual's PHI to certain federal officials for lawful intelligence and other national security activities.
- **Worker's Compensation:** The Agency may disclose an individual's PHI as authorized to comply with worker's compensation law.
- **U.S. Department of Health and Human Services:** The Agency must disclose an individual's PHI to that individual upon request and to the Secretary of the United States Department of Health & Human Services to investigate or determine the Agency's compliance with the privacy laws.
- **Disaster Relief Activities:** The Agency may disclose an individual's PHI to local, state or federal agencies engaged in disaster relief and to private disaster relief assistance organizations (such as the Red Cross if authorized to assist in disaster relief efforts).

Section 5 - HIPAA Patient Rights

a. **Individual Rights**

Individuals have a right to access any PHI that is used to make decisions about the individual subject of the data, including information used to make health care decisions or information used to determine whether a claim will be paid. The individual has a right to access their designated record set. The right of access also applies to health care clearinghouses; health care providers that create or receive PHI other than as a business associate of the Agency.

b. **Request for PHI**

An individual may request that the Agency release PHI. The agency will require that the request be in writing and clearly identify the information requested. It will be the responsibility of the Privacy Officers to review the request, determine its legitimacy, review and approve the data requested prior to release, advise the requester if the data cannot be released and why, and ensure the request is logged appropriately. All requests for PHI data should be sent to the Privacy Officers, SWHHS, 607 West Main Street, Suite 100, Marshall, Minnesota 56258.

c. **Request for PHI Approved**

If the Agency approves the request for release of PHI, the Agency will:

- Make copies of the requested PHI;
- Inform the individual of the approval for release and determine a method for delivering the information to the individual;
- Document the release of PHI

d. **Request for PHI Denied**

The Agency will permit any individual to request access to inspect or copy the designated record set for as long as it is maintained by the Agency with the following exceptions:

- Information compiled in reasonable anticipation of a civil, criminal or administrative action or proceeding.
- Any data determined by Minnesota State Law to be determined to be "confidential," or "private" i.e.,
    - medical or psychological information stamped confidential
    - names of reporters
    - adoption records
    - chemical dependency records (per MN Statute Chapter 254A; section 09.)

e. **Accounting of Disclosures**

The Agency will obtain from the Master HIPAA Request Log and provide, upon request, a 6-year accounting of disclosures made of the individual's PHI , except for disclosures:

- To carry out treatment, payment or health care operations.
- To the individual data subject (i.e., requests the individual made about his/her own information).
- To facility directories or to person's involved in the individual's care or other notification purposes.
- For national security or intelligence purposes.
- To corrections officials or law enforcement personnel when the individual is in custody.

- Which were made before the compliance date.
- To a record locator service, unless the individual has elected to be excluded from the service.

In certain circumstances involving health oversight agencies or law enforcement agencies, the Agency may temporarily suspend the individual's right to receive an accounting of disclosures.

Information that must be must be maintained (tracked) and included in an accounting:

- Date of disclosure.
- Name of individual or entity who received the information and their address, if known.
- Brief description of the protected health information disclosed.
- Brief statement of the purpose of the disclosure or a copy of the individual's written request for disclosure.

f. **Amendment Requests**

- The Agency will permit an individual to request that the Agency amend PHI. The Agency will require that the request be in writing, clearly identify the information to be amended, and that a reason be stated for the amendment. The Agency will so inform any individual of this expectation. All requests to amend PHI data should be sent to the Privacy Officers, SWHHS, 607 West Main Street, Suite 100, Marshall, Minnesota 56258.
- The Agency will have up to 60 days to act on the request. One 30 day extension is allowed. The subject of the data's written request will become a part of any case file maintained on the subject. The document will be retained for 6 years.

g. **Accepting an Amendment**

If the Agency decides to accept an amendment, the Agency will:

- Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. Inform the individual in a timely manner that the amendment has been accepted. The Agency will obtain agreement from the individual to allow the Agency to share the amendment with individuals or entities identified by the individual and the Agency.
- Make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - persons identified by the individual as having received PHI about the individual and needing the amendment; and

- persons, including business associates, that the Agency knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeable rely, on such information to the detriment of the individual.

h. **Denying an Amendment**

Requests for amendment may be denied if the information to be amended:

- If the Agency was not the originator of the information, unless the originator is no longer available to amend the request.
- Is not part of the designated record set.
- Is not accessible to the individual because federal or state law does not permit it.
- Is accurate and complete as determined by the Agency upon review.

If the Agency denies all or a part of the requested amendment, the Agency will:

- Provide the individual with a timely, written denial. The denial will use plain language and contain:
  - the basis for the denial;
  - the individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
  - a statement that, if the individual does not submit a statement of disagreement, the individual may request that the Agency provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
  - a description of how the individual may complain to the Agency or make appeal pursuant to Administrative Procedures Act (Minn. Stats. Chapter 14).
- Permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment.
- Prepare a written rebuttal to the individual's statement of disagreement.
- Identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Agency's denial of the request, the individual's statement of disagreement, if any, and the Agency's rebuttal, if any, to the designated record set.
- If the individual has submitted a statement of disagreement, the Agency must include the material appended, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.
- If the individual has not submitted a written statement of disagreement, the Agency will include the individual's request for amendment and its denial, or an

accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

i. **Actions on Notice of an Amendment**
If the Agency is informed by another covered entity of an amendment to an individual's PHI, the Agency will amend the PHI in designated record sets. Amendments will be made in a reasonable time period, as expeditiously as possible.

j. **Documentation**
All requests to amend PHI data should be sent to the Privacy Officers, Southwest Health and Human Services, 607 West Main Street, Suite 100, Marshall, Minnesota 56258. All requests to amend documentation will be retained for 6 years.

k. **Alternative Means of Communication Request**
The Agency will accommodate all reasonable requests from individuals to receive communication of PHI by alternative means or at an alternative location.
The agency will require that the request be in writing and clearly identify the information requested. It will be the responsibility of the Privacy Officers to review the request, determine its legitimacy, review and approve the request prior to release, advise the requester if the data cannot be released or communicated by an alternate means and why, and ensure the request is logged. The outcome of the request will be communicated to the patient upon final determination. All requests should be sent to the Privacy Officers, SWHHS, 607 West Main Street, Suite 100, Marshall, Minnesota 56258.
The Agency will have up to 60 days to act on the request. One 30 day extension is allowed. The subject of the data's written request will become a part of any case file maintained on the subject. The document will be retained for 6 years.

l. **Accepting the Request for Alternative Means of Communication**
If the Agency approves the request, the Agency will:

- Provide the PHI via an alternated means of communication;
- Inform the individual of the approval for the alternate means of communication and determine a method for delivering the information to the individual;
- Document the release of PHI.

m. **Denying the Request for Alternative Means of Communication**
If the Agency denies the request, the Agency will:

- Provide the individual with a timely, written denial. The denial will use plain language and contain the basis for the denial.

n. **Restricted Use Request**

The Agency will allow an individual to request that the Agency restricts its use and disclosure of PHI for treatment, payment or health care operations. The Agency will require that the request be in writing and clearly identify the information requested. It will be the responsibility of the Privacy Officers to review the request, determine its legitimacy, review and approve the request prior to use and disclosure, advise the requester if the data cannot be restricted and why, and ensure the request is logged.

o. **Restriction to a Health Plan Procedure**

- The patient will complete the Request for Restriction of Health Information, and indicate it is a restriction to a health plan.
- The patient must provide payment, in full, to SWHHS prior to the services being conducted.
- The PHI for that specific date of service will be deemed self-pay.
- SWHHS will ensure that the information from that specific date of service is not released to the insurance company.
- If approved, SWHHS will document the restriction within the patient's medical record. When releasing records, the staff will always review the list of restrictions to ensure they are abiding by the approved patient request for that specific date of service.
- The restriction to health information to the health plan specified is only for the specific date of service.
- If denied, SWHHS will inform the patient in writing, including the reason for the denial of the request for restriction of health information.
- All documentation regarding restrictions will be stored in the patient's medical record.

Section 6 – Miscellaneous

a. **Complaints Policy**

The Agency will provide a process for individuals to make complaints to the Agency concerning its HIPAA privacy regulations policies and procedures, its compliance with those policies or procedures or its compliance with the privacy regulations itself. The notice provided to individuals will include a brief description of how individuals may file a complaint, including the title, phone number and address to contact for further information on the policies for filing a complaint. Complaints will be logged appropriately and directed to the Privacy Officers. The Agency will document all complaints received and their disposition.

b. **Anti-Retaliation Policy**

The Agency will not retaliate against any person for exercising a right under the HIPAA privacy regulations, or for filing a complaint, participating in an investigation, or opposing any lawful act in relation to the privacy regulations.

Section 7 – Breach Notification

a. **Purpose**

To provide guidance for breach notification by covered entities when impermissive or unauthorized access, acquisition, use and/or disclosure of the Agency's patient PHI occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH), Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Omnibus Rule), as well as any other federal or state notification law.

b. **Discovery of Breach**

- A breach of PHI shall be treated as discovered as of the first day on which an incident that may have resulted in a breach is known to the Agency, or, by exercising reasonable diligence would have been known to the Agency (includes breaches by the Agency's business associates). The Agency shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a employee or agent (e.g. a business associate acting as an agent of the Agency) of the Agency.

c. **Breach Investigation**

- The HIPAA Privacy and/or HIPAA Security Officer(s) shall serve as the investigators of the breach process. The investigators shall be responsible for the management of the breach investigation, completion of a Risk Assessment, and coordinating with others in the Agency as appropriate (e.g., administration, human resources, HIPAA Privacy and Security Risk Management Team, legal counsel, etc.) The investigators shall be the key facilitators for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the Risk Assessment and notifications made, shall be retained for a minimum of six years.
- The following risk assessment will be completed for each breach investigation:
    - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

- The unauthorized person who used the protected health information or to the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

d. **Documentation**

- The Agency shall document the Risk Assessment as part of the investigation in the incident report form noting the outcome of the Risk Assessment process. The Agency has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the Risk Assessment, the Agency will determine the need to move forward with breach notification. The Agency may make breach notifications without completing a Risk Assessment.

e. **Timeliness of Notification**

- Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 days after the discovery of the breach by the Agency involved or the business associate involved that is acting as the Agency's agent. It is the responsibility of the Agency to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

f. **Delay of Notification Authorized for Law Enforcement Purposes**

- If a law enforcement official states to the Agency that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Agency shall:
  - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
  - If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

g. **Content of the Notice**

- The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured PHI that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the Agency is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

h. **Methods of Notification**

- The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:
  - **Notice to Individual(s)**
    Notice shall be provided promptly and in the following form:
    - Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the Agency knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out. Limited examples:
      - The Agency may send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, if they all reside at a single address and all individuals to which the notice applies are clearly identified on the notice. When a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, however, address a breach notice to the dependent himself or herself
      - In the limited circumstance that an individual affirmatively chooses not to receive communications from the Agency at any written addresses or email addresses *and* has agreed only to receive communications orally or by

telephone, the provider may telephone the individual to request and have the individual pick up their written breach notice from the Agency directly. In cases in which the individual does not agree or wish to travel to the Agency to pick up the written breach notice, the Agency should provide all of the information in the breach notice over the phone to the individual and document that it has been done.

- Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
- In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the Agency's website, or a conspicuous notice in a major print or broadcast media in the Agency's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.
- If the Agency determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

- **Notice to Media**
  - Notice shall be provided to prominent media outlets serving the state and regional area (of the breached patients) when the

breach of unsecured PHI affects 500 or more of the Agency's patients of a State or jurisdiction.

- The Notice shall be provided in the form of a press release.
- What constitutes a prominent media outlet differs depending upon the State or jurisdiction where the Agency's affected patients reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.

- **Notice to Secretary of HHS**
  - Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.
  - For breaches involving 500 or more individuals, the Agency shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
  - For breaches involving less than 500 individual, the Agency will maintain a log of the breaches. The breaches may be reported during the calendar year or no later than 60 days after the end of that calendar year in which the breaches were discovered (e.g., 2012 breaches must be submitted by 3/1/2013 – 60 days). Instructions for submitting the logged breaches are provided at www.hhs.gov.

- **Maintenance of Breach Information/Log**
  - As described above and in addition to the reports created for each incident, the Agency shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
- A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
- A description of the action taken with regard to notification of patients, the media, and the Secretary regarding the breach.
- The results of the breach investigation will be logged appropriately.
- Resolution steps taken to mitigate the breach and prevent future occurrences.

- **Business Associate Responsibilities**

  The business associate (BA) of the Agency that accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, without unreasonable delay and in no case later than 60 days after discovery of a breach, notify the Agency of such breach (when the business associate is an agent of the Agency, this notification must be provided within a shorter timeframe as specified in the Business Associate Agreement policy). Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the Agency with any other available information that the Agency is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the Agency will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is the responsibility of the Covered Entity to document this notification).

Section 8 – Auditing Information System Activity

a. SWHHS shall audit access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards.

b. Violation of this policy and its procedures by employees may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

c. **Purpose**

It is the policy of SWHHS to safeguard the confidentiality, integrity, and availability of patient health information applications, systems, and networks. To ensure that appropriate safeguards are in place and effective. This policy applies to organizational information applications, systems, networks, and any computing devices, regardless of ownership [e.g., owned, leased, contracted, and/or stand-alone).

d. **Scope**

This policy has been developed to address the Agency-wide approach to information system auditing processes. Departments and business units shall work with the Security Officer and/or IT to develop specific procedures based on applications and systems for auditing processes.

e. **Procedures**

- Responsibility for auditing information system access and activity is assigned to SWHHS Security Officer or other designee as determined by SWHHS' administration. The responsible individual shall:
    - Assign the task of generating reports for audit activities to the individual responsible for the application, system, or network.
    - Assign the task of reviewing the audit reports to the individual responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task.

  SWHHS' auditing processes shall address access and activity at the following levels listed below. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
- SWHHS shall determine the systems or activities that will be tracked or audited by:
    - Focusing efforts on areas of greatest risk and vulnerability as identified in the Risk Assessment and ongoing Risk Mitigation Plan.
    - Maintaining confidentiality, integrity, and availability of ePHI applications and systems.
- SWHHS shall identify trigger events or criteria that raise awareness of questionable conditions of viewing of confidential information. The events may

be applied to the entire Agency or may be specific to a department, unit, or application. At a minimum, SWHHS shall provide immediate auditing in response to:

- Patient complaint
- Employee complaint
- Suspected breach of patient confidentiality
- High risk or problem prone event (e.g., VIP admission)
- Any action that causes suspicion or poses a concern

- SWHHS shall determine auditing frequency by reviewing past experience, current and projected future needs, and industry trends and events. SWHHS will determine its ability to generate, review, and respond to audit reports using internal resources. SWHHS may determine that external resources are also appropriate.
- SWHHS' IT Department, Security Officer or designee is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Audit documentation/reporting tools may address the following data elements:
  - Application Audited
  - Date
- The process for review of audit logs, trails, and reports shall include:
  - Description of the activity as well as rationale for performing audit.
  - Identification of which employees or department/unit will be responsible for review (employees shall not review audit logs which pertain to their own system activity).
  - Frequency of the auditing process.
  - Determination of significant events requiring further review and follow-up.
  - Identification of appropriate reporting channels for audit results and required follow-up.
- Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), if publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

f. **Evaluation and Reporting of Audit Findings**

- Audit information that is routinely gathered must be reviewed in a timely manner by the individual/department responsible for the activity/process. The reporting process shall allow for meaningful communication of the audit findings to those departments/units sponsoring the activity.
  - Significant findings shall be reported immediately in a written format. SWHHS' breach form may be utilized to report a single event.

- Reports of audit results shall be limited to internal use on a minimum necessary/ need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
- Security audits constitute an internal, confidential monitoring practice that may be included in SWHHS' performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable patient PHI shall not be included in the reports).
- Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring departments/units.

g. **Auditing Business Associate and/or Vendor Access and Activity**

- We work directly with BA on audits as deemed necessary.

h. **Audit Log Security Controls and Backup**

- Audit logs shall be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident. Generally, system administrators shall not have access to the audit trails or logs created on their systems.
- Audit logs maintained within an application shall be backed-up as part of the application's regular backup procedure.
- SWHHS shall audit internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required. Auditing of data back-up processes shall be carried out:
    - On a periodic basis for established practices and procedures.
    - More often for newly developed practices and procedures (e.g., weekly, monthly, or until satisfactory assurance of reliability and integrity has been established).

i. **Retention of Audit Information**

- Audit logs and trail report information shall be maintained based on organizational needs. Retention of this information shall be based on:
    - Organizational history and experience.
    - Available storage space.
- Logs summarizing audit activities shall be retained for a period of six years.

Section 9 – HIPPA Security Oversights

a. SWHHS Human Resources, Privacy Officers, Security Officer or designee is responsible for facilitating the training and supervision of all employees, investigation and sanctioning of any employee that is in non-compliance with the HIPAA privacy and security regulations.

b. **Employee Training**

- The Agency will train all members of its workforce in the policies and procedures adopted by the Agency necessary to comply with the HIPAA privacy and security regulations. Agency staff will receive training annually. Training will be provided to each new member of the Agency's workforce at the time of hire and as part of new employee orientation.
- Training can be done in a variety of ways, including, but not limited to: speaker, on-line, department meetings, or other.
- Training is mandatory for all employees.
- Human Resources maintains documentation of the training session materials and attendees for a minimum of six years.
- Employees will be trained on the employee responsibility information listed below.

c. **Employee Responsibilities**

- SWHHS will monitor access and activities of employees and will address any discrepancies.
- Workstations may only be used to perform assigned job responsibilities.
- Employees may not download software onto SWHHS' workstations and/or systems without prior approval from the Security Officer or designee.
- Employees are required to report malicious software to the Security Officer or designee immediately.
- Employees are required to report unauthorized attempts, uses of, and theft of SWHHS' systems and/or workstations.
- Employees are required to report unauthorized access to facilities.
- No employee may alter ePHI maintained in any system, even if they have the technical ability to do so without specific authorization.
- Employees will understand that they are responsible for the security of any portable devices that they use. The level of encryption and security must correspond to the most sensitive information stored on the device. Loss or theft must be reported immediately.
- Employees are required to understand their role in SWHHS' contingency plan.
- Employees may not share their user names nor passwords with anyone.

- When a request is made for disclosure of information, employee must determine if PHI is in information to be released and notify the Privacy Officers and receive approval before authorizing the release of information.
- The Security Officer facilitates the timely communication of security updates and reminders to all employees to which it pertains. Examples of security updates and reminders include, but are not limited to:
    - Latest malicious software or virus alerts
    - SWHHS' requirement to report unauthorized attempts to access ePHI
    - Changes in creating or changing passwords
    - Changes in regulatory standards
- Additional training is provided to employees in the information services department. Employees will receive training based on the scope of their job.

d. **Supervisor Responsibilities**

- Although the Security Officer is responsible for implementing and overseeing activities related to compliance to the Security rule, it is the responsibility of all leaders (i.e. Executive Team , Supervisors, Lead Workers) to supervise employees, third party vendors, contractors or other users of SWHHS' systems, applications, servers, workstations, etc. that contain ePHI.
- Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance. Leaders assist the Security Officer to ensure appropriate role-based access is provided to all employees.
- Leaders take reasonable steps to hire, retain, and promote employees and provide access to employees who comply with the Security regulation and SWHHS' security policies and procedures.
- Human Resources gets input from Supervisors who identify appropriate systems access for all new staff. HR provides the information to IT for access.
- When an employee is terminated from SWHHS, the Supervisor completes the appropriate form with last date of employment and routes to IT for terminating access.
- Supervisors are required to report a change in an employee's title, role, department, and/or location.
    - Refer to Admin Policy #9 for Physical and Technical Safeguards.

e. **Non-compliance of SWHHS' policies and procedures**

- All employees and any others with system access report non-compliance of SWHHS' policies and procedures to the Security or Privacy Officer or Human Resource. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

- Investigation/Employee Sanctions: If there is a report of non-compliance or if employees fail to comply with the Agency's privacy and security policies or procedures, the Agency will apply appropriate disciplinary sanctions.
- The Privacy or Security Officer or Human Resources promptly facilitates a thorough investigation of all reported violations of SWHHS' privacy and security policies and procedures. The Privacy or Security Officer or Human Resources may request the assistance from others such as the employee's supervisor, other employees, and/or other vendor/contractors as needed.
    - The Security Officer completes an audit trail/log to identify and verify the violation and sequence of events.
    - Human Resources interviews any individual that may be aware of or involved in the incident.
        - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
        - HR provides individuals suspected of non-compliance of the security rule and/or SWHHS' policies and procedures the opportunity to explain their actions to determine whether it was an unintentional or malicious deviation from established policies and procedures.
    - HR thoroughly documents the investigation in a timely manner.
    - The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
- Violation of any security policy or procedure by employees may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
- HR maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

f. **Dissemination of HIPAA Policies and Procedures**

The Agency will place a copy of its HIPAA Policies and Procedures for the workforce consumption on SharePoint.

Section 10 – Risk Assessment and Risk Mitigation Plan

a. **Purpose**

This policy establishes the scope, objectives, and procedures of SWHHS' HIPAA Privacy and Security Risk Assessment and HIPAA Privacy and Security Risk Mitigation Plan process. The Risk Assessment and Risk Mitigation Plan is intended to support and protect the Agency and its ability to fulfill its mission.

b. **Policy**

It is the policy of SWHHS to conduct HIPAA Privacy and Security Risk Assessments on a regular basis or upon major changes in the technical infrastructure, implementation of a new application with ePHI or upon changes in regulations.

- During the Risk Assessment process, a system identification and characterization will be conducted to determine what systems create, store, maintain, or transmit protected health information.
- All threats and vulnerabilities to the system will be evaluated through reviews of systems.
- Based on threat and vulnerability evaluation as well as evaluation of current controls, SWHHS will evaluate;
    - The likelihood of a threat and/or vulnerability occurring
    - The impact of a threat and/or vulnerability occurring.
- Upon understanding the threat and vulnerabilities of a threat or vulnerability being exploited, a level of risk will be assigned.
- A Risk Assessment Report will be generated at the completion of the Risk Assessment that will define the;
    - Scope of the Risk Assessment
    - Systems evaluated during the Risk Assessment
    - Findings and Risks from the Risk Assessment
    - Recommended mitigations to address/mitigate risks.
- The risks will be evaluated, addressed, and mitigated following the Risk Assessment process using the HIPAA Privacy and Security Risk Mitigation Plan.

c. Maintain documentation of all Risk Assessments, Risk Assessment Reports and Risk Mitigation Plans for a minimum of six years.

Section 11 – Business Associates

a. To establish guidelines for SWHHS to identify those vendor/business relationships which meet the HIPAA definition of a Business Associate (BA) and provide direction in establishing formalized Business Associate Agreements (BAA). SWHHS shall implement

the required procedures and ensure documentation to establish satisfactory assurance of compliance.

b. **Procedures**

The Agency shall determine responsible oversight for the management of business associate relationships and agreements.

Responsibility may be delegated to Privacy Officer or other designated employee.

- The Agency's department units are responsible for facilitating the assessment of both existing and future vendor/business relationships to determine whether the relationship meets the criteria for a HIPAA BAA. The following criteria define a BA under HIPAA:
    - The vendor/business' staff members are not members of the Agency's workforce.
    - The vendor/business' is doing something on behalf of the Agency;
    - That "something" involves the use and/or disclosure of PHI.
    - Note that there are certain disclosures to vendors/businesses that do not require establishment of a BAA. These disclosures include:
        - Disclosures to disclosures by a covered entity to a health care provider concerning the treatment of the individual;
        - Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or
        - Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.
- The Agency may determine the need for BAA's through:
    - Reviewing contract management documents/software and identifying where PHI is disclosed to external entities.
    - Assessing new vendor/business arrangements to determine if PHI will be used and/or disclosed.

- When it has been determined that a BA arrangement exits, a designee shall contact the responsible individual to initiate a BAA. The designee shall provide the following information to customize the BAA:
    - The name and contact information of the BA.
    - A general description of the type of service being provided by the BA.
    - The name of the Agency's department supervisor who established the BAA.
    - Date of establishment of the BA relationship and BAA.
- If a vendor/business relationship requiring a BA agreement/addendum is in the process of contract negotiation and development, the provisions of the BAA may be incorporated into the contract as an option (a separate BAA would not be required).
- Obligations and activities which must be addressed in the BAA document include:
    - **Privacy Rule Provisions:**
        - Stated Purposes for Which BA May Use or Disclose PHI: BA is permitted to use and disclose PHI it creates or receives for or from the Agency for the purposes as described in the addendum. BA may also use Protected Health Information it creates or receives for or from the Agency as minimally necessary for BA's proper management and administration or to carry out BA's legal responsibilities.

          Limitations on Use and Disclosure of PHI: BA agrees it shall not use or disclose, and shall ensure that its directors, officers, employees, contractors and agents do not use or disclose PHI for any purpose other than as expressly permitted by the BAA, or required by law, or in any manner that would constitute a violation of the Privacy Standards if used by the BA.
            - The BAA may permit the BA to use and disclose PHI for the proper management and administration of the BA; and
            - The BAA may permit the BA to provide data aggregation services relating to the health care operations of the covered entity.
        - Disclosure by Others: To the extent BA is authorized by the BAA to disclose PHI to a third party, BA must obtain, prior to making any such disclosure, reasonable assurances from the third party that the PHI will be held confidential as provided pursuant to the BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and an agreement from the third party to immediately notify BA of any breaches of

confidentiality of the PHI, to the extent it has obtained knowledge of such breach.

- Minimum Necessary: BA shall disclose to its subcontractors, agents or other third parties, and request from them, only the minimum PHI necessary to performing or fulfilling a specific required or permitted function.
- Safeguards Against Misuse of Information: BA will establish and maintain all appropriate safeguards to prevent any use or disclosure of PHI other than pursuant to the terms and conditions of the BAA.
- Reporting of Disclosures of PHI: BA shall, within 60 days of discovery of any use or disclosure of PHI in violation of the BBA, report any such use or disclosure to the Agency.
- Agreements by Third Parties: BA shall enter into an agreement with any agent or subcontractor that will have access to PHI that is received from, or created or received by BA on behalf of, the BA pursuant to which such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to BA pursuant to the BAA with respect to PHI.
- Access to Information: Within 7 days of a request by the Agency for access to PHI about an individual contained in a Designated Record Set, BA shall make available to the Agency the PHI it requests for so long as that information is maintained in the Designated Record Set. If any individual requests access to PHI about the individual directly from BA, BA shall make available and provide a right of access to the PHI to the individual, at the times and in the manner required by the Privacy Standards. After receiving the request, BA shall notify the Agency within 7 days of such request.
- Availability of PHI for Amendment: BA agrees to make PHI available for amendment and to incorporate any such amendments in the PHI, at the times and in the manner required by the Privacy Standards.
- Accounting of Disclosures: Within 7 days of notice by the Agency to BA that it has received a request for an accounting of disclosures of PHI regarding an individual during the six years prior to the date on which the accounting was requested, BA shall make available to the Agency such information as is in BA's possession and is required for the Agency to make the accounting required by the Privacy Standards. At a minimum, BA shall provide the Agency with the following information: the date of

the disclosure; the name of the entity or person who received the PHI, and, if known, the address of such entity or person; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure which includes an explanation of the basis for the disclosure. If the request for an accounting is delivered directly to BA, BA shall within 7 days forward the request to the Agency. The Agency is responsible for preparing and delivering the accounting requested. BA agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

- Availability of Books and Records: BA agrees to make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by BA on behalf of, the Agency available to the Secretary for purposes of determining the Agency's and BA's compliance with the Privacy Standards.

- **Security Rule Provisions:**
  - Implementation of Safeguards: BA agrees to implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, and transmits on behalf of the Agency.
  - Agents and Subcontractors: BA agrees that any agent, including a subcontractor, to which the BA provides ePHI, agrees to implement reasonable and appropriate safeguards to protect the ePHI.
  - Security Incidents: BA agrees to report to the Agency any security incident of which it becomes aware.
- **Other Provisions:**
  - The Agency may want to seek legal counsel guidance prior to entering into a BAA that includes language addressing:
    - Insurance responsibilities
    - Indemnification requirements
  - If the Agency chooses to terminate the arrangement with the BA or the BA chooses to terminate the arrangement with the Agency, the agreement must be terminated as outlined in the provisions of the BA agreement/addendum or contract.
  - Upon termination or expiration of the business arrangement between the BA and the Agency, the BA shall either return or destroy all PHI received from the Agency or created or received by BA on behalf of the Agency that the BA still maintains in any

form as outlined in the provisions of the BAA/addendum or contract.

c. The Agency does not have a statutory obligation to monitor the activities of its BAs. The Agency, however, must respond to reported privacy breaches and security incident events should they occur. The Agency realizes it will be found to be non-compliant unless the Agency took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- Terminated the contract or arrangement, if feasible; or
- If termination is not feasible, reported the problem to the Department of Human Services.

d. The Agency may serve as a BA to another covered entity and may be asked to review and sign that covered entity's external BA agreement/addendum or contract. As a BA, the Agency should:

- Forward the external information to the Privacy Officer to review the submitted BAA to ensure that the provisions outlined are consistent with those set forth in this policy.
- If the BAA is not consistent with this policy or contains additional provisions or provisions that are inconsistent with the privacy regulation, the Privacy Officer may recommend the following alternatives.
    - Agree to the additional provisions and sign the agreement.
    - Refer the agreement to legal counsel to determine appropriateness before signing.
    - Refuse to agree to the provisions and notify the covered entity to establish a resolution.

e. To meet the documentation requirements of the Security Rule, the responsible individual shall maintain a file of BAAs/addendums/contracts.

f. All BAA documentation shall be maintained for a period of six years beyond the date of when the BAA relationship is terminated.

g. The BAA shall be effective for the length of the relationship between the BA and the Agency, unless otherwise terminated under the provisions outlined in the BAA.

Section 12 - Sales and Marketing

a. SWHHS's current practices or procedures do not include any of the following: Fundraising and PHI, Sale of PHI, Marketing and PHI, Research and PHI, De-identification and Limited Data Sets.

Supporting Documents and Resources:

- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Omnibus Rule)
- ARRA Title XIII Section 13402 – Notification in the Case of Breach
- FTC Breach Notification Rules - 16 CFR Part 318
- 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
- 45 CFR 164.510 (b) - notification purposes
- 45 CFR 164.512 (k) (5) - individual in custody
- 45 CFR 164.528(a)(2) - accounting of disclosures
- 45 CFR § 164.308(a)(1)(ii)(D) – Information System Activity Review
- 45 CFR § 164.308(a)(5)(ii)(B) & (C) – Protection from Malicious Software & Log-in Monitoring
- 45 CFR § 164.308(a)(2) – HIPAA Security Rule Periodic Evaluation and Assigned Security Responsibility
- 45 CFR § 164.312(b) –Audit Controls
- 45 CFR § 164.312(c)(2) – Mechanism to Authenticate ePHI
- 45 CFR § 164.312(e)(2)(i) – Integrity Controls
- 45 CFR §164.308(a)(1)(ii)(c) HIPAA Security Rule Sanction Policy
- 45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
- 45 CFR §164.308(a)(5)(ii)(A) HIPAA Security Rule Security Reminders
- 45 CFR §164.316(a-b) HIPAA Security Rule Documentation
- 45 CFR 164.308(a)(1)(ii)(A) – HIPAA Security Rule Risk Analysis
- 45 CFR 164.308(a)(1)(ii)(B) – HIPAA Security Rule Risk Management
- 45 CFR 164.308(a)(8) – HIPAA Security Rule Evaluation
- 45 CFR § 164.504(e)(2) - Privacy Rule Provisions
- 45 CFR § 164.314 - Security Rule Provisions/ Organizational Requirements BAs Contracts or Other Arrangements
- 45 CFR 164.512 – social responsibility reporting/Uses and disclosures for Research purposes as contained in the final HIPAA Privacy Rules.
- 45 CFR § 164.308(b)(1) – HIPAA Security Rule Administrative Safeguards BAs Contracts and Other Arrangements
-

- 45 CFR § 164.502(e)(1) – HIPAA Privacy Rule Uses and Disclosures of PHI: General Rules – Disclosures to BAs
- 45 CFR §164.504 – HIPAA Privacy Rule Uses and Disclosures: Organizational Requirements

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 18

EFFECTIVE DATE: 12/19/12
REVISION DATE: 06/15/16
AUTHORITY: Southwest Health and Human Services Joint Governing Board

--- PASSWORDS ---

Section 1 - Overview

a. Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Southwest Health and Human Services resources. All users, including contractors and vendors with access to Southwest Health and Human Services systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Section 2 - Purpose

a. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Section 3 - Scope

a. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Southwest Health and Human Services facility, has access to the Southwest Health and Human Services network, or stores any non-public Southwest Health and Human Services information.

Section 4 - Policy

a. General

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a monthly basis and are a minimum of 15 characters. Passwords must be unique and cannot be reused for 6 months. Server passwords require alphabetic numeric and special characters. Only IT personnel have access to the server (administrator) passwords.
- ~~All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.~~

- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

- General Password Construction Guidelines All users at Southwest Health and Human Services should be aware of how to select strong passwords.

- Strong passwords have the following characteristics:
  - Contain at least three of the five following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuation
    - "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
  - Contain at least fifteen alphanumeric characters.

- Weak passwords have the following characteristics:
  - The password contains less than fifteen characters
  - The password is a word found in a dictionary (English or foreign)
  - The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Southwest Health and Human Services", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the

phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
(NOTE: Do not use either of these examples as passwords!)

b. Password Protection Standards

- Always use different passwords for Southwest Health and Human Services accounts from other non-Southwest Health and Human Services access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various Southwest Health and Human Services access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share Southwest Health and Human Services passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Southwest Health and Human Services information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora, OutLook, and Internet Explorer).

If an account or password compromise is suspected, report the incident to the IT Department.

c. Use of Passwords for Remote Access Users Access to the Southwest Health and Human Services Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

Section 5 – Enforcement

a. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the IT Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

SOUTHWEST HEALTH AND HUMAN SERVICES
ADMINISTRATIVE POLICY NUMBER 24

EFFECTIVE DATE: 02/17/16
REVISION DATE: 06/15/16
AUTHORITY: Southwest Health and Human Services Governing Board

--- EQUIPMENT DISPOSAL POLICY ---

Section 1 – Purpose

a. The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Southwest Health and Human Services.

Section 2 – Introduction

a. Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Southwest Health and Human Services data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Section 3 - Scope

a. This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Southwest Health and Human Services including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All Southwest Health and Human Services employees and affiliates must comply with this policy.

Section 4 – Policy Technology Equipment Disposal

a. When Technology assets have reached the end of their useful life they should be sent to the IT Department office for proper disposal.

b. The IT Department will securely erase all storage mediums in accordance with current industry best practices.

c. All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

d. No computer or technology equipment may be sold to any individual other than through the processes identified in this policy.

e. No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around Southwest Health and Human Services. These can be used to dispose of equipment. The IT Department will properly remove all data prior to final disposal.

f. All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

g. Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

h. The IT Department will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

i. Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

j. Prior to leaving Southwest Health and Human Services premises, all equipment must be removed from the Information Technology inventory system.

~~**Section 5 – Policy Compliance**~~

~~a. Compliance Measurement~~

- ~~The IT Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.~~

~~b. Exceptions~~

- ~~Any exception to the policy must be approved by the IT Manager in advance.~~

~~c. Non-Compliance~~

- ~~An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.~~

SOUTHWEST
HEALTH & HUMAN
SERVICES

Southwest Health and Human Services Comprehensive Civil Rights Plan (CCRP)

Southwest Health and Human Services
607 W. Main Suite 100
Marshall, MN 56258
507-637-6747
MN Relay Service: 711 or (800) 627-3529

Civil Rights Coordinator: Christopher Sorensen (507) 532- 1248 (voice)
ADA Coordinator: Dale Hiland (507) 532-1224 (voice)
Limited English Proficiency Coordinator: Kathy Herding (507) 836-6144 (voice)

This CCRP is posted in the lobby of each office

Americans with Disabilities Act Advisory

This information is available in accessible formats to individuals with disabilities and for information about equal access to services, call (507) 537-6747. TTY users place calls through MN Relay Service: 711 or (800) 627-3529

TABLE OF CONTENTS

1. **Purpose**
   As a recipient of federal financial assistance, Southwest Health and Human Services is responsible for providing core services to assist and support Minnesota's most vulnerable individuals and families so they can meet their basic needs and be treated with respect and dignity. Southwest Health and Human Services has a CCRP to ensure that all eligible individuals receive equal access to program services and information. Its programs are operated in a nondiscriminatory way, without regard to race, color, national origin, age, disability, sex, sexual orientation, religion, political beliefs, creed and public assistance status. In medical programs, *sex* includes sex stereotypes and gender identity under any health program or activity receiving federal funds. This CCRP also serves as a source of information for county agency staff and the general public. It sets out Southwest Health and Human Services' civil rights administrative policies and procedures, identifying key contacts within the agency and linking the reader to applicable state and federal civil rights laws and resources.

2. **Legal Authorities** (See full list in Appendix, Attachment A)
   - Title VI of the Civil Rights Act of 1964 (race, color, national origin)
   - Section 504 of the Rehabilitation Act of 1973 (disability)
   - Section 508 of the Rehabilitation Act of 1973 (disability)
   - Title II of the Americans with Disabilities Act of 1990; State and local government services (disability)
   - Age Discrimination Act of 1975 (age)
   - Section 1557 of the Patient Protection and Affordable Care Act (added sex discrimination in health care programs)
   - Title IX of the Education Amendments of 1972 (sex)
   - Bilingual Requirements in the Food Stamp Program, Food and Nutrition Service, U.S. Department of Agriculture
   - FNS Instruction 113-1, Civil Rights Compliance and Enforcement – Nutrition Programs and Activities, Food and Nutrition Service, U.S. Department of Agriculture (2005)
   - Minnesota Human Rights Act, Chapter 363A

3. **Civil Rights Contact**
   Southwest Health and Human Services designates Christopher Sorensen to serve as the agency's Civil Rights Contact, agency point person on civil rights matters.

   Christopher Sorensen
   (507) 532-1248
   MN Relay Service: 711 or (800) 627-3529
   chris.sorensen@swmhhs.com

4. **Equal Opportunity Policy and Procedure**
   Southwest Health and Human Services Equal Opportunity Policy and Procedure
   It is the policy of Southwest Health and Human Services to make sure that program benefits and services are available to everyone and provided to all eligible individuals without discrimination, in compliance with civil rights laws.

   Southwest Health and Human Services employees, services, programs, benefits and policies will not discriminate against applicants, clients or members of the public because of race, color, national origin, sex, sexual orientation, age, creed, religion, political beliefs, disability or public assistance status. "Sex" includes sex stereotypes and gender identity under any medical or health program receiving federal financial assistance, such as Medical Assistance, CHIP programs, health clinics, insurance companies and state health insurance exchanges.

   This policy covers Southwest Health and Human Services 's full range of services, programs and benefits, including, but not limited to, access to information about services, eligibility determinations and intake, admission procedures and treatment. The policy applies to the agencies and providers receiving federal and state funds under contracts, licenses and other arrangements with Southwest Health and Human Services. The Minnesota Human Rights Act also applies to the work of Southwest Health and Human Services and those agencies carrying out its programs.

Program Accessibility for People with Disabilities
Southwest Health and Human Services and all of its services, programs and benefits, are accessible to and usable by people with disabilities, including people with hearing loss, low vision and other sensory disabilities.

To avoid disability discrimination, Southwest Health and Human Services will:

- Notify the public about rights and protections for people with disabilities under the Americans with Disabilities Act
- Designate an ADA Contact and maintain a complaint procedure
- Make sure that its buildings are physically accessible for people with disabilities
- Assist individuals with disabilities to apply and qualify for benefits based on their eligibility
- Provide appropriate auxiliary aids and services, including accessible formats, to ensure effective communication with people with disabilities
- Provide services, programs and benefits that are accessible to and usable by qualified people with disabilities

Physical access includes:

- Convenient off-street parking designated specifically for people with disabilities
- Curb cuts and ramps between parking areas and the Southwest Health and Human Services building
- Level access into the first floor of the Southwest Health and Human Services building with elevator access to all other floors

Reasonable Modifications to Policies, Procedures or Practices
Southwest Health and Human Services will make reasonable modifications to its policies, procedures or practices when necessary to avoid discrimination on the basis of disability, unless Southwest Health and Human Services can demonstrate that making the modifications would fundamentally alter the nature of the services, programs or benefits.

Effective Communication and Auxiliary Aids and Services
Southwest Health and Human Services will take appropriate steps to ensure that communications with people with disabilities and companions with disabilities are as effective as communications with others. To ensure effective communications, Southwest Health and Human Services will provide appropriate auxiliary aids and services, including accessible formats, so that people with disabilities can receive services, programs and benefits and participate in them in the same way as people without disabilities. Auxiliary aids and services include qualified readers, writers and interpreters who convey information effectively, accurately and impartially using any necessary specialized vocabulary.

To determine what types of auxiliary aids or services are necessary, Southwest Health and Human Services will give primary consideration to the requests of people with disabilities. Southwest Health and Human Services will honor the choice of the person requesting the auxiliary aid or service unless it would fundamentally alter the nature of the service, program or benefit or cause an undue administrative or financial burden. If this happens, Southwest Health and Human Services will find another equally effective auxiliary aid or service.

5. Complaint Resolution Procedure

Southwest Health and Human Services Civil Rights Complaint Procedure
You have the right to equal access to services, if you are an applicant, client or member of the public trying to gain access to human services program information or benefits. Southwest Health and Human Services has a civil rights complaint procedure that provides prompt and thorough resolution of civil rights complaints.

Civil rights complaints allege discrimination. You have a right to file a civil rights complaint if you believe you have been discriminated against because of your race, color, national origin, sex, sexual orientation, age, creed, religion, political beliefs, disability or public assistance status. *Sex* includes sex stereotypes and gender identity discrimination that occurs in medical or health programs and clinics receiving federal financial assistance, such as Medical Assistance, MNCare, CHIP programs, insurance companies and state health insurance exchanges.

It is against the law for anyone who works for Southwest Health and Human Services to retaliate against a person who files a complaint or who cooperates in the investigation of a civil rights complaint.

To file a complaint, ask for Southwest Health and Human Services' equal opportunity policy, complaint procedure and complaint form. Use the contact information below to help you to file your complaint. You can also review the law and regulations that outlaw discrimination in the Civil Rights Contact's office at Southwest Health and Human Services:

Christopher Sorensen
Southwest Health and Human Services
607 W. Main Marshall, MN 56258
(507)537-6747(voice)
MN Relay Service: 711 or (800) 627-3529
(507)537-6088 (fax)
chris.sorensen@swmhhs.com

Procedure:

1. Civil rights complaints **must** be submitted to the Civil Rights Contact within 180 days of the date the alleged discrimination occurred.

2. A complaint **must** be in writing and contain the name and address of the person filing it. You should also give your telephone number or relay service number if you are deaf or hard of hearing. Give your email address if it helps get in touch with you. The complaint **must** state the problem or action alleged and the relief desired. If you need assistance with your complaint, the Civil Rights Contact will help you.

3. Southwest Health and Human Services **must** conduct an investigation of the complaint. The investigation may be informal, but it **must** be thorough and timely. People who have an interest in the complaint **must** have an opportunity to submit relevant evidence about the complaint. Southwest Health and Human Services will issue a written decision on the complaint within 90 days after its filing. Southwest Health and Human Services will maintain the complaint records and files for three years. Complaints about program rules are not civil rights complaints and will be resolved through a different complaint process.

4. The person filing the complaint may appeal the decision by writing to the agency's Civil Rights Contact within 15 days of receiving the written decision. The Civil Rights Contact **will** issue a written decision in response to the appeal, no later than 30 days after the filing. This decision is final. – This appeal process is not the same as filing a fair hearings appeal with the Department of Human Services' Appeals and Regulations Division.

5. The person filing the complaint must be informed that he/she can file a discrimination complaint **directly** with the U.S. Department of Health and Human Services' Office for Civil Rights or the U.S. Department of Agriculture (USDA) for the SNAP Program.

   (a) The **U.S. Department of Health and Human Services' Office for Civil Rights** prohibits discrimination in its programs because of race, color, national origin, age, disability, sex and religion. *Sex* includes sex stereotypes and gender identity discrimination that occurs in medical or health programs and clinics receiving federal financial assistance, such as Medicaid, CHIP programs and insurance companies and state health

insurance exchanges under Title I of the Affordable Care Act. Contact the federal agency directly:

U.S. Department of Health and Human Services
Office for Civil Rights
Region V
233 N. Michigan Avenue
Suite 240
Chicago, IL 60601
312-886-2359 (voice)
800-368-1019 (toll free)
800-537-7697 (TTY)

(b) USDA requires that the following nondiscrimination statement be provided **exactly** as it is shown below:

In accordance with Federal civil rights law and **U.S. Department of Agriculture** (USDA) civil rights regulations and policies, the USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, sex, religious creed, disability, age, political beliefs, or reprisal or retaliation for prior civil rights activity in any program or activity conducted or funded by USDA.

Persons with disabilities who required alternative means of communication for program information (e.g., Braille, large print, audiotape, American Sign Language, etc.), should contact the Agency (State or local) where they applied for benefits. Individuals who are deaf, hard of hearing or have speech disabilities may contact USDA through the Federal Relay Service at (800) 877-8339. Additionally, program information may be made available in languages other than English.

To file a program complaint of discrimination, complete the USDA Program Discrimination Complaint Form, (AD-3027) found online at: http://www.ascr.usda.gov/complaint_filing_cust.html, and at any USDS office, or write a letter addressed to USDA and provide

in the letter all of the information requested in the form. To request a copy of the complaint form, call (866) 632-9992. Submit your completed form or letter to USDA by:

(1)mail: U.S. Department of Agriculture
Office of the Assistant Secretary for Civil Rights
1400 Independence Avenue, SW
Washington, D.C. 20250-9410;

(2)fax: (202) 690-7442; or

(3)email: program.intake@usda.gov

This institution is an equal opportunity provider.

6. Filing Complaints with State Agencies:
The person filing the complaint **must** also be informed that he/she can file a discrimination complaint **directly** with the Minnesota Department of Human Rights and the Minnesota Department of Human Services.

(a)The Minnesota Department of Human Rights prohibits discrimination in public services programs because of race, color, creed, religion, national origin, disability, sex, sexual orientation, or public assistance status. Contact the Minnesota Department of Human Rights directly:

Minnesota Department of Human Rights
Freeman Building, 625 North Robert Street
St. Paul, MN 55155
651-539-1100 (voice)
800-657-3704 (toll free)
711 or 800-627-3529 (MN Relay)

(b)The **Minnesota Department of Human Services** prohibits discrimination in its programs because of race, color, national origin, creed, religion, sexual orientation, public assistance status, age, disability, or sex, including sex stereotypes and gender identity discrimination that occurs in health programs or

activities receiving federal financial assistance, such as Medical Assistance, MNCare, CHIP programs and insurance companies and state health insurance exchanges. Contact the Equal Opportunity and Access Division **directly** only if you have a discrimination complaint:

Minnesota Department of Human Services
Equal Opportunity and Access Division
P.O. Box 64997
St. Paul, MN 55164-0997
651-431-3040 (voice) or use your preferred relay service

(c) County agencies are not permitted to investigate civil rights complaints in the Supplemental Nutrition Assistance Program (SNAP) because counties directly administer SNAP benefits. County agencies **must** refer SNAP civil rights complaints to DHS or the USDA regional office in Chicago. The USDA regional address is:

Civil Rights Director
Midwest Regional Office
USDA/Food and Nutrition Service
77 W. Jackson Blvd., 20th Floor
Chicago, IL 60604-3591
(312) 353-6657 (voice) or use your preferred relay service
Tamara.earley@fns.usda.gov

7. Arrangements for People with Disabilities:
Southwest Health and Human Services **will** make appropriate arrangements to ensure that people with disabilities are provided accommodations to participate in the complaint process in an equal to manner to people without disabilities. Appropriate arrangements include, but are not limited to, providing interpreters for people who are deaf or hard-of-hearing; providing taped cassettes and accessible formats for people who are blind or have low vision; and assuring a physically accessible location for complaint proceedings. The Civil Rights Contact or designee is responsible for making these arrangements.

8. Southwest Health and Human Services will refer all SNAP civil rights complaints to DHS or the USDA regional office in Chicago as soon as possible after received.

6. Complaint Notification Form

Southwest Health and Human Services will use the *Complaint Notification Form* to notify DHS in writing of all service delivery discrimination complaints filed against Southwest Health and Human Services and resolved on the county agency level. Southwest Health and Human Services will make sure the complaint notification form is completed and sent to DHS within 90 days of the date the complaint was filed in the county, so DHS can report the complaint to the appropriate federal office. A copy of the *Complaint Notification Form* is located in the Appendix; Attachment B.

7. Disability Compliance

a. Disability Law and Standard of Access for State and Local Government Services

Section 504 of the Rehabilitation Act of 1973 protects qualified individuals with disabilities from discrimination based on their disability in federally funded programs and services.

Title II of the Americans with Disabilities Act of 1990 (Title II of the ADA) protects qualified individuals with disabilities from discrimination on the basis of their disability when the discrimination occurs in state or local government services. An agency does not have to receive federal financial assistance to be required to comply with Title II of the ADA. An agency just has to be a state or local government entity.

County human services agencies must ensure that people with disabilities are able to use their programs and services. Disability laws set out an equal access standard for providing services. This means that individuals with disabilities are entitled to equal access to human services programs; the same standard of access that applies to people without disabilities.

A public agency must reasonably modify its policies, procedures and practices to avoid discrimination. A public

agency must also take appropriate steps to ensure that its communications with individuals with disabilities are as effective as communications with others.

b. ADA Contact

Southwest Health and Human Services has designated an ADA Contact person to serve as its point person on disability matters raised by applicants, clients and members of the public. ADA Contact information is located on the cover page of this CCRP.

Dale Hiland
(507)532-1224
MN Relay Service: 711 or (800) 627-3529
dale.hiland@swmhhs.com

c. Disability Complaints

People filing disability complaints will use Southwest Health and Human Services' civil rights complaint procedure.

d. ADA Notice Document

Southwest Health and Human Services will use the DHS brochure: *Do you have a disability* (DHS-4133-ENG) as its ADA notice document. This notice document informs applicants, clients and members of the public that Southwest Health and Human Services does not discriminate on the basis of disability. The notice document also gives information to the public about the rights of people with disabilities under the Americans with Disabilities Act.

Southwest Health and Human Services has a copy of DHS brochure: *Do you have a disability* (DHS-4133-ENG) posted in the lobby next to the reception desk.

A copy of the DHS brochure: *Do you have a disability* (DHS-4133-ENG) is located in the Appendix; Attachment C.

e. Disability Policy Prohibiting Discrimination

The Southwest Health and Human Services Equal Opportunity Policy and Procedure includes provisions which prohibit disability discrimination in human services programs. This policy is located in the agency lobby.

8. Limited English Proficiency Plan

EFFECTIVE DATE: 04/01/11
REVISION DATE: 05/20/15
AUTHORITY: Southwest Health and Human Services Board – Human Services Board
Instructional Bulletin #00-89-04
Instructional Bulletin #04-89-01

--- LIMITED ENGLISH PROFICIENCY PLAN ---

Limited English Proficiency (LEP) Plan

Director:	Christopher Sorensen	507-532-1248
Deputy Director:	Nancy Walker	507-532-1256
Social Services Division Director:	Cindy Nelson	507-532-1260
LEP Coordinator:	Kathryn Herding, Supervisor	507- 836-6144
Financial Services:	Jennifer Beek, Supervisor	507- 532-1235
Social Services:		
Jenifer Klein, Supervisor		507-532-1228
Cindy Nelson, Supervisor		507-532-1260
Dale Hiland, Supervisor		507-532-1224
Child Support & Fraud:	Ann Schiller, Supervisor	507-637-1262

Section 1 - Purpose and Legal Basis

a. The following document serves as the Southwest Health and Human Services (SWHHS) plan to meet the legal obligation of language access requirements in compliance of Title VI of the Civil Rights Act of 1964; 7 CFR, 273 et seq; and 42 CFR 435 et seq. There are four components to this document.

- 200 - Assessment
- 300 - Policy
- 400 - Training

- 500 - Monitoring

Section 2 - 200 - Assessment

a. 201 - Needs Assessment - SWHHS will on at least an annual basis make a needs assessment of the unique language needs within Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties. Consultation will be done with the school districts in the six counties along with the Legal Aid offices located in Willmar and Worthington to determine the types of non-English languages that are most dominant to the populations of Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties. The common agency will also incorporate county specific data from the Department of Human Services to assist in this form of needs assessment. The following non-English languages have been identified as being the most likely to be encountered in Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties: Spanish, Somali, Hmong.

b. 202 - Case Finding - Specific language needs of each applicant with LEP will occur at the time of intake or application. This will primarily be done by reviewing the language preference questions on the Health Care Application (HCAPP) and the Combined Application Form (CAF). Language preferences will be entered into the applicant's primary language field in the MAXIS system. If an interpreter is needed, it will be recorded in MAXIS case notes. If the main receptionist or intake worker suspects that the applicant is a person with LEP, the worker will provide the LEP person with a list of possible languages to determine which language is spoken. The list includes; "I Speak" cards, "I Speak" posters, "Language Identification Card" from Language Line Services. It is expected that reasonable efforts will be made by SWHHS to provide same-day interpreter services.

c. 203 - Points of Contact - The greatest likelihood of need for interpreter services will be at the point of intake - at the time of an emergency or application for financial assistance. The principal point of contact will most likely be in the office setting in Ivanhoe, Marshall, Slayton, Pipestone, Luverne, and/or Redwood Falls. The most appropriate form of interpreter services will likely be language assistance in completion of an application for financial assistance or

health care. The other point of contact may involve field-based contact when conducting child protection assessments. These contacts will typically take place in the home of the child's caretaker or parent.

d. 204 - Resources Needed - SWHHS will utilize its contract with private interpreters and those interpreters employed by contracted agencies located in Marshall, Minnesota for Spanish, Somali, Hmong, and Laotian interpreter services. Additionally, SWHHS will contract with Language Line Services (1-800-367-9559) for the languages involved with Language Lines Services "tier" system. When feasible, on-site interpreter services will be made available and will be the first preference. (Note: The closest available Spanish interpreter for Lincoln, Murray, and Pipestone Counties is 30 miles from each office.) Use of reciprocal faxing processes will be used when necessary, this is to facilitate completion of applications and processing of interviews.

e. 205 - Timely Access - Interpretive services are available during customary business hours, Monday through Friday, 8:00 a.m. to 4:30 p.m. They also provide emergency service outside of regular business hours when needed. Language Line Services are available 24x7. Contact with any entity will be made by phone. When on-site interpreter services are to be used, it will be necessary to schedule appointments at mutually convenient times for the client and the interpreter.

Section 3 – 300 - Policies and Procedures

a. 301 - Agency Commitment - SWHHS is committed to the spirit of the Civil Rights Act of 1964. We recognize the importance of providing meaningful access to all persons, including persons with LEP, to the various programs provided by SWHHS. SWHHS has, by prior action, adopted a policy statement entitled Civil Rights Compliance Requirements effective 1-1-95 and affirmed again on 1-1-01, this in conformity with DHS Bulletin #94-84A dated 12-27-94.

b. 302 - Range of Oral Language Assistance - Due to the current absence of bi-lingual employees at SWHHS, use will be made of the formal linkage with our contracted agencies and other privately contracted interpreters. With Spanish, Somali, and Hmong seen as the primary non-English language in Lincoln, Lyon, Murray, Pipestone,

Redwood, and Rock Counties, use of our contracted agencies and privately contracted interpretive services are seen as encompassing close to 100% of the LEP needs of SWHHS. Use of Language Line Services for all other non-English language will take place as necessary. SWHHS will take advantage of the 10 brief "notice of rights to language services" documents for persons with LEP as they are made available by the Department of Human Services.

c. 303 - Uncommon Languages - There may be circumstances when customers come to the office for services that use a language other than those most commonly used in Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties. There may be languages such as Russian, Vietnamese, Chinese, Laotian, Oromo, Khymer/Cambodian, etc. After identifying the language need, the receptionist staff or intake worker will consult with their Supervisor or Director to determine the most appropriate and expedient interpreter service.

d. 304 - Affirmative Action - The SWHHS employee handling the case will inform either the customer or the interpreter once it has been determined that interpreter services are needed, that there is no charge or fee for the service. This will be communicated in verbal form. At no time in the service delivery process will the customer incur any costs associated with LEP-directed interpreter services.

e. 305 - Use of Family and Friends - Use of family or friends as interpreters is not the preferred method of providing interpreter services. But when the intake worker has determined that it is not feasible to use formalized interpreter services, a consultation will be made with that worker's immediate Supervisor or Director. Alternative methods of customer service will need to be discussed. If the worker has determined that a family member, friend or other responsible party can adequately perform the interpreter service, approval may be given. The worker needs to feel confident that the client's data privacy rights will be protected and that the quality of the interpreter services to be provided by the family member or friend will be acceptable. The worker will need to document in the case file the extenuating circumstances for use of family or friends, particularly that the family was offered other interpreter services and that the client insisted that a family member or

friend be used. Under no circumstances may minor children be used for interpreter services.

f. 306 - Competency Standards for Interpreters - Any interpreter used for LEP services must be bi-lingual: fluent in English and fluent in the language of the customer needing the service. When using interpreter services provided from a recognized agency, contracted interpreters and Language Line Services, competency is presumed. When using family, friends or significant others, the intake worker must make a judgment as to the competency of the proposed interpreter. "Certification" as an interpreter is not a pre-requisite.

g. 307 - Dissemination of LEP Plan - Copies of the LEP Plan will be provided to the following: all SWHHS employees who have direct customer contact, area Legal Aid offices, Private Industry Council, and Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Government Agencies. A copy of the main public announcement, "I Speak" poster, will be prominently displayed in the SWHHS central reception areas. LEP requirements will also be included in all contracts maintained by SWHHS.

h. 308 - Services to Illiterate - When confronted with a situation in which the customer is illiterate - cannot read or write in his or her native language - it is required that SWHHS find a suitable interpreter; one who can assist the person in completion of necessary forms, documents and the like. The SWHHS intake worker needs to make the determination, in conjunction with the interpreter, about the customers' literacy skills. The clear choice in dealing with cases of illiteracy will be to have an on-site interpreter. It may be necessary to schedule interviews when face-to-face interpreter services can be provided. Use of faxing of forms and over-the-phone services may be required on a case-by-case basis.

i. 309 - Emergency Situations - When programs require access to services within short time frames, SWHHS will take whatever steps necessary to ensure that all clients, including clients with LEP, have access to services within the appropriate time frames. For example, when a client needs an interpreter or other language assistance services to obtain expedited program services, SWHHS's goal is to

make the services accessible within the required time frame, whether that means using an interpreter or any other appropriate type of language assistance.

j. 310 - Access to and Costs of Interpreters - Under no circumstances will SWHHS indicate - either verbally or in writing - that any applicant or client in need of LEP services will be charged for an interpreter or translation service. All such services shall be at no expense to the applicant or client. Such services will be provided during all normal business hours and, when necessary, during non-business hours when an emergency has been determined to exist.

k. 311 - Notice of Service Availability - LEP clientele will be informed of the availability of free interpreter and translation services at the point when it appears that the customer is not able to communicate in English. Notice of service availability will come from the "I Speak" poster document in the central reception areas of the six county offices. Distribution of the LEP Plan to various parties cited above will help by putting those entities on notice that interpreter and translation services are available on a timely basis and free of charge. Material that has been translated into Spanish, Somali, and Hmong will be used immediately when it has been determined that the person presenting for service is not able to understand English. Insofar as the Department of Human Services has translated many forms into multiple languages, SWHHS will access these forms as necessary through the Department's website at http://edocs.dhs.state.mn.us/forms. Additionally, translated income maintenance forms located in TEMP Manual 12.01.13 will be accessed as needed.

l. 312 - County-Produced Materials - At this time it is not anticipated that SWHHS will develop any SWHHS produced material. Rather, SWHHS will rely on the state-produced documents as the primary source of translated materials. Downloading of documents from the DHS web-page will also be used as necessary. SWHHS will follow DHS' translation numerical guidelines as required.

m. 313 - Complaint Resolution Protocol - Any action taken by SWHHS with which an applicant or recipient disagrees is subject to

complaint. SWHHS has a formal complaint process that can be utilized to try to resolve any dispute. In the absence of local resolution, the person making the complaint will be informed in a language understandable to the grievant, of the process to follow in making a complaint to DHS or the Office of Civil Rights. The complaint process will follow SWHHS's procedures included in Civil Rights Compliance Requirements. Appropriate use of interpreter services with contracted agencies, contracted interpreters, or Language Line Services to facilitate the dispute resolution process will take place. All such complaints can be made to any of the parties listed at the top of this LEP Plan.

n. 314 - Posting - A copy of the SWHHS LEP Plan will be posted on the main bulletin board in the central lobby of each agency office.

Section 4 – 400 - Training

a. 401 - Distribution of LEP Plan - All SWHHS employees who have direct contact with customers will be provided a copy of the LEP Plan upon its adoption. If any changes are made in the document, a revised copy will also be provided to the same entities listed in #307. At this time, all employees of SWHHS will be recipients of the document.

b. 402 - Training of Staff - Initial - With approval of the LEP Plan, there will be initial training on the document. This training will take place for current staff in their individual unit meetings. For any new employee affected by the LEP Plan, this document will be incorporated into that person's "generic orientation" protocol at the time of hire.

c. 403 - Training of Staff - Ongoing - On an annual basis the LEP Plan will be reviewed and updates clarified.

Section 5 - 500 - Monitoring

a. 501 - Evaluation of the LEP - On at least an annual basis, the LEP Plan will be reviewed for effectiveness. This review will normally take place in December. It will be coordinated by the SWHHS LEP Coordinator. The evaluation will involve consultation with representatives of the Financial Services Unit and Social Services Unit

to determine compliance with the LEP Plan, identification of any problem areas and development of required corrective action strategies. Elements of the evaluation will include the following:

- Number of persons with LEP in Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties.
- Assessment of current language needs of SWHHS applicants and clients to determine if the client needs an interpreter and/or translated materials; updating case files which lack information about a client's language preference; determining if clients need to be asked their language preference at the time of certification.
- Determining whether existing assistance is meeting the needs of applicants and clients with LEP.
- Assessing whether staff members understand SWHHS LEP policies and procedures and how to carry them out, and whether language assistance resources and arrangements for those resources are still current and accessible.
- Seeking and obtaining feedback from non-English or limited-English speaking communities in Lincoln, Lyon, Murray, Pipestone, Redwood, and Rock Counties including applicants and clients as well as any known community organization or advocacy group working with non-English or limited-English speaking communities.

b. 502 - LEP Contact Person - For purposes of the LEP Plan, Southwest Health and Human Services designated contact person is the Financial Assistance Supervisor/LEP Coordinator with appropriate delegation made to the Agency Director, Deputy Director and the Social Services Supervisors of the agency.

Southwest Health and Human Services
607 West Main Street, Suite 100
Marshall, MN. 56258
Limited English Proficiency Plan Table of Contents

9. Annual Civil Rights Training for the Supplemental Nutrition Assistance Program (SNAP)

Southwest Health and Human Services will use DHS' PowerPoint presentation to train staff, document the date of the training each year and document who attends the training.

10. Civil Rights Assurance of Compliance

The Southwest Health and Human Services director and agency attorney representative have signed the *2016 Civil Rights Assurance of Compliance.* A copy is located in the Appendix; Attachment D.

11. CCRP Administration

Southwest Health and Human Services will:

- Post a copy of its CCRP in the agency lobby where members of the public can review it and in the employee break room where staff can review it
- Post the CCRP on the agency's public website
- Review the CCRP annually with ALL staff
- For the benefit of applicants, clients and members of the public, prominently post in the lobby a copy of the equal opportunity policy and procedure that includes provisions prohibiting disability discrimination and a copy of its civil rights complaint procedure
- Post a copy of the DHS brochure: *Do you have a disability* (DHS-4133-ENG) in the lobby next to the reception desk
- Conduct annual SNAP civil rights training for all staff who administer the SNAP program and all staff who have direct contact with the public, including support staff, supervisors and managers. Southwest Health and Human Services will document the date of the training each year and document who attends the training.

12. Appendix

a. Attachment A – Full List of Legal Authorities

Federal

1. Title VI of the Civil Rights Act of 1964 (race, color, national origin)
2. Section 504 of the Rehabilitation Act of 1973 (disability)
3. Section 508 of the Rehabilitation Act of 1973 (disability)
4. Title II of the Americans with Disabilities Act of 1990; State and local government services (disability)
5. Age Discrimination Act of 1975 (age)
6. Community Service Assurance Provisions of the Hill-Burton Act (health facilities receiving Hill-Burton Funds)

7. Section 1557 of the Patient Protection and Affordable Care Act (added sex discrimination in health care programs)
8. Nondiscrimination Provisions of the Omnibus Budget Reconciliation Act of 1981 (Federal Block Grants):
    - Community Services Block Grant (race, color, national origin, sex) **Remaining block grants** (race, color, national origin, age, disability, sex, religion)
    - Social Services Block Grant
    - Maternal and Child Health Services Block Grant
    - Projects for Assistance in Transition from Homelessness Block Grant
    - Preventive Health and Health Services Block Grant
    - Community Mental Health Services Block Grant
    - Substance Abuse Prevention and Treatment Block Grant
9. Title IX of the Education Amendments of 1972 (sex)
10. Family Violence Prevention and Services Act (race, color, national origin, age, disability, sex, religion)
11. Food Stamp Act of 1977
12. Nondiscrimination Compliance Requirements in the Food Stamp Program, Food and Nutrition Service, U.S. Department of Agriculture
13. Bilingual Requirements in the Food Stamp Program, Food and Nutrition Service, U.S. Department of Agriculture
14. FNS Instruction 113-1, Civil Rights Compliance and Enforcement – Nutrition Programs and Activities, Food and Nutrition Service, U.S. Department of Agriculture (2005)
15. Equal Opportunity for Religious Organizations Regulation

State

Minnesota Human Rights Act, Chapter 363A

Attachment B – Complaint Notification

COUNTY HUMAN SERVICE AGENCY COMPLAINT NOTIFICATION FORM COMPLAINTS ALLEGING DISCRIMINATION IN SERVICE DELIVERY

AUTHORITY: U.S. Department of Agriculture, Food and Nutrition Service Instruction 113-1.

REQUIREMENT: County human service agencies must notify the DHS Civil Rights Coordinator within 90 days of all service delivery discrimination complaints (i.e., civil rights complaints) filed against them (see bottom of Page 2 for contact information).

ACTION REQUIRED:

Complete this form and send it to the DHS Civil Rights Coordinator within 90 days of the date the complaint was filed.

1. Name, address, telephone number of complainant:

_____

_____

2. Name and address of county agency delivering the benefits, including names of any employees accused of wrongdoing:

_____

_____

3. Type of discrimination alleged.

_____

_____

_____

_____

4. Describe the alleged discrimination, including the dates it happened. Give names and contact information of any witnesses:

_____

_____

5. Give a summary of the investigation findings, including any corrective action ordered:

_____

_____

_____

_____

_____

_____

CONTACT INFORMATION: DHS Civil Rights Coordinator
Minnesota Department of Human Services
Equal Opportunity and Access Division
P.O. Box 64997
St. Paul, MN 55164-0997
651-431-3034 (voice) or use your preferred relay service
651-431-7444 (fax)
joann.daSilva@state.mn.us

Attachment C – DHS Brochure: *Do you have a disability*; DHS-4133-

Do you have a disability?

If you have a disability, you have the same rights as others. Please tell us if you have a disability so we can help you access human services programs and benefits.

What medical conditions may be disabilities?

A disability is a physical, sensory, or mental impairment that materially limits a major life activity.

Types of disabilities may include:

Diseases like diabetes, epilepsy or cancer
Learning disorders like dyslexia
Developmental delays
Clinical depression
Hearing loss or low vision
Movement restrictions like trouble with walking, reaching or grasping
History of alcohol or drug addiction, although current illegal drug use is not a disability.

If you are asking for or are getting benefits through either a county human services agency or the Minnesota Department of Human Services, that office will let you know if you have a disability using information from you and your doctor.

What help is available?

If you have a disability, your county or the state human services agency can help you by:

Calling you or meeting with you in another place if you are not able to come into the office

Using a sign language interpreter

Giving you letters and forms in other formats like computer files, audio recordings, large print or Braille

Telling you the meaning of the information we give you

Helping you fill out forms

Helping you make a plan so you can work even with your disability
Sending you to other services that may help you.

Helping you to appeal agency decisions about you if you disagree with them.

You will not have to pay extra for help. If you want help, ask your agency as soon as possible. An agency may not be able to accommodate requests made within 48 hours of need.

How does the law protect people with disabilities?

The Americans with Disabilities Act (ADA) and the ADA Amendments Act are federal laws, and the Minnesota Human Rights Act is a state law. Each gives individuals with disabilities the same legal rights and protections as people without disabilities, including access to public assistance benefits. You will not be denied benefits because you have a disability. Your benefits will not be stopped because of your disability.

If your disability makes getting benefits hard for you, your county human services agency will help you access all of the programs that are available to you.

Discrimination is against the law

You have the right to file a complaint if you believe you were treated in a discriminatory way by a human services agency. You can contact any of the following agencies directly to file a civil rights complaint.

The Minnesota Department of Human Services, Equal Opportunity and Access Division, prohibits discrimination in its programs because of race, color, national origin, creed, religion, sexual orientation, public assistance status, age, disability or sex (including sex stereotypes and gender identity under any health program or activity receiving federal financial assistance).

Contact the Equal Opportunity and Access Division directly:

Minnesota Department of Human Services
Equal Opportunity and Access Division
P.O. Box 64997
St. Paul, MN 55164-0997
651-431-3040 (voice) or use your preferred relay service

The Minnesota Department of Human Rights prohibits discrimination in public services programs because of race, color, creed, religion, national origin, disability, sex, sexual orientation, or public assistance status. Contact the Minnesota Department of Human Rights directly:
Minnesota Department of Human Rights
Freeman Building, 625 North Robert Street
St. Paul, MN 55155
651-539-1100 (voice)
800-657-3704 (toll free)
711 or 800-627-3529 (MN Relay)

The U.S. Department of Health and Human Services' Office for Civil Rights prohibits discrimination in its programs because of race, color, national origin, age and disability; in block grant complaints, religion and sex are included; and in medical program complaints, sex includes sex stereotypes and gender identity under any health program or activity receiving federal financial assistance, such as Medicaid and CHIP programs, hospitals, clinics, employers, insurance companies and state health insurance exchanges created under Title I of the Affordable Care Act. Contact the federal agency directly:
U.S. Department of Health and Human Services
Office for Civil Rights, Region V
233 North Michigan Avenue, Suite 240
Chicago, IL 60601
312-886-2359 (voice)
800-368-1019 (toll free)
800-537-7697 Y)

The U.S. Department of Agriculture prohibits discrimination against its customers, employees, and applicants for employment on the bases of race, color, national origin, age, disability, sex, gender identity, religion, reprisal, and where applicable, political beliefs, marital status,

familial or parental status, sexual orientation, or all or part of an individual's income is derived from any public assistance program, or protected genetic information in employment or in any program or activity conducted or funded by the Department.
(Not all prohibited bases will apply to all programs and/or employment activities.)

If you wish to file a Civil Rights program complaint of discrimination, complete the USDA Program Discrimination Complaint Form, found online at:
http://www.ascr.usda.gov/complaint_filing_cust.html,

or at any USDA office, or call (866) 632-9992 to request the form.

You may also write a letter containing all of the information requested in the form. Send your completed complaint form or letter to us by mail at:

U.S. Department of Agriculture, Director, Office of Adjudication, 1400 Independence Avenue, S.W., Washington, D.C. 20250-9410, by fax (202) 690-7442 or email at program.intake@usda.gov.

Individuals who are deaf, hard of hearing or have speech disabilities may contact USDA through the Federal Relay Service at (800) 877-8339; or (800) 845-6136 (Spanish).

For any other information dealing with Supplemental Nutrition Assistance Program (SNAP) issues, persons should either contact the USDA SNAP Hotline Number at 800-221-5689, which is also in Spanish or call the State Information/Hotline Numbers (click the link for a listing of hotline numbers by State); found online at http://www.fns.usda.gov/snap/contact_info/hotlines.htm.
USDA is an equal opportunity provider and employer.
CB 4 (1-15)
This information is available in accessible formats for individuals with disabilities by contacting your county worker. For other information on disability rights and protections to access human services programs, contact the agency's ADA coordinator.
ADA5 (12-12)

Attachment D – Signed Copy of the *2016 Civil Rights Assurance of Compliance*

MINNESOTA DEPARTMENT OF HUMAN SERVICES
CIVIL RIGHTS ASSURANCE OF COMPLIANCE
NONDISCRIMINATION IN STATE AND FEDERALLY FINANCED PROGRAMS

Southwest Health and Human Services

(HEREAFTER CALLED THE "AGENCY") THE AGENCY provides this civil rights Assurance of Compliance (hereafter called the "Assurance") in consideration of and for the purpose of obtaining any and all federal financial assistance from the United States Departments of Health and Human Services and Agriculture. The County Agency agrees that compliance with this Assurance is a condition of continued receipt of federal financial assistance and that it is binding upon the County Agency directly or through contract, license, or other provider of services, as long as it receives federal or state financial assistance; and shall be submitted with the required Comprehensive Civil Rights Plan update.

THE AGENCY ASSURES that it will comply with:
Title VI of the Civil Rights Act of 1964, as amended; Department of Health and Human Services, Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons; Age Discrimination Act of 1975, 42 U.S.C. 6101, as amended; Section 504 of the Rehabilitation Act of 1973, as amended; Section 508 of the Rehabilitation Act of 1973, as amended; Title II of the Americans with Disabilities Act of 1990; Section 1557 of the Patient Protection and Affordable Care Act of 2010; Federal Block Grant Programs of the Omnibus Budget Reconciliation Act of 1981; as amended; Title IX of the Education Amendments of 1972, as amended; Family Violence Prevention and Services Act; Food Stamp Act of 1977, as amended, including the Nondiscrimination Compliance Requirements in the Food Stamp Program and the Bilingual Requirements in the Food Stamp Program; FNS Instruction 113-1, Civil Rights Compliance and Enforcement – Nutrition Programs and

Activities, Food and Nutrition Service, U.S. Department of Agriculture (2005); and Interethnic Adoption Provisions of the Small Business Job Protection Act of 1996 (formerly Multiethnic Placement Act of 1994).

PURSUANT TO THE CIVIL RIGHTS PLAN for the Minnesota Department of Human Services, by accepting this Assurance, the County Agency agrees to allow access, by authorized personnel of the Minnesota Department of Human Services and the United States Departments of Health and Human Services and Agriculture, during normal working hours, to private and/or confidential data maintained by the County Agency (or other sub-recipient of federal financial assistance) to the extent necessary to conduct a full and complete investigation into any complaint of discrimination, including to compile data, maintain records and submit reports as required to determine compliance with the above mentioned laws, rules and regulations. The Minnesota Department of Human Services agrees to comply with all requirements of the Minnesota Government Data Practices Act (Minnesota Statutes, section 13.01 et seq.). No private and/or confidential data collected, maintained or used in the course of an investigation shall be disseminated except as authorized by statute, either during the period of the investigation or after it has been concluded. If there are any violations of this assurance, DHS shall have the right to invoke fiscal sanctions or other legal remedies in accordance with Minnesota Statutes, section 256.017.

THE PERSON WHOSE SIGNATURE APPEARS BELOW is authorized to sign this Assurance and commit the County Agency to its terms.

_____

Director's Signature

_____

Date

I CERTIFY that the signatory for the Agency has lawful authority to bind the Agency to the terms of this civil rights Assurance.

_____

Agency Attorney's Signature

_____

Date

JUNE 2016
BOARD APPROVAL ON THE FOLLOWING:

☐ **Lower Sioux Indian Community (Redwood County)** – 04/15/16 to 06/30/18; An agreement in cooperation with the Lower Sioux Tribe to provide child welfare services to at risk children of the Lower Sioux; DHS Child Welfare Disparities grant of $313,851 allocated as $34,432 SFY16, $137,728 SFY17, and $141,691 SFY18 (NEW).

☐ **Woodland Centers (Willmar, MN & various locations)** – 06/01/16 to 12/31/16; Addendum to current contract adding Detoxification services, per diem at $480/day (NEW).

☐ **Children's Home Society (Sioux Falls, SD) –** 07/01/16 to 06/30/17; provide client residential mental health treatment services in 3 facility types, Madsen House $239.38/day (no increase), Boys Unit $323.78/day (no increase), and VanDeMark House $239.38/day (no increase) (renewal).

☐ **DHS Planning & Implementation (P&I) Grant** – 07/01/16 to 06/30/21; new grant with the Alcohol and Drug Abuse Division to promote a collective impact model (multiple agencies and community sectors working towards a common goal) to implement Community-Level Interventions to reduce youth alcohol use; $945,245 over a 5 year period (NEW).

☐ **MDH Public Health Emergency Preparedness (PHEP) BP5** – 07/01/16 to 06/30/17; amendment for budget period #5 (July 2016 through June 2017); amended amount $109,089 for a new grant total over the five year period of $491,774 (renewal).

☐ **MDH CHB Master Grant** – 01/01/15 to 12/31/19; Amendment to contract language to assure compliance with federal requirements (Uniform Guidance or 2 CFR 200); this contract is designed to administratively simplify the review of grant project agreements for community health boards and applies to all grants MDH distributes (renewal).