Northern Inyo Healthcare District

Board Meetings

August 16, 2023 Regular Board of Directors Meeting

NORTHERN INYO HEALTHCARE DISTRICT
One Team. One Goal. Your Health.

AGENDA
NORTHERN INYO HEALTHCARE DISTRICT
BOARD OF DIRECTORS REGULAR MEETING

August 16, 2023 at 5:30 p.m.

Northern Inyo Healthcare District invites you to join this meeting:

TO CONNECT VIA **ZOOM**: (*A link is also available on the NIHD Website*)
https://zoom.us/j/213497015?pwd=TDlIWXRuWjE4T1Y2YVFWbnF2aGk5UT09
Meeting ID: 213 497 015
Password: 608092

PHONE CONNECTION:
888 475 4499 US Toll-free
877 853 5257 US Toll-free
Meeting ID: 213 497 015

The Board is again meeting in person at 2957 Birch Street Bishop, CA 93514. Members of the public will be allowed to attend in person or via zoom. Public comments can be made in person or via zoom.

---

1. Call to Order (at 5:30 pm).
2. ***Public Comment***: The purpose of public comment is to allow members of the public to address the Board of Directors. Public comments shall be received at the beginning of the meeting and are **limited to three (3) minutes per speaker**, with a total time limit of thirty (30) minutes for all public comment unless otherwise modified by the Chair. Speaking time may not be granted and/or loaned to another individual for purposes of extending available speaking time unless arrangements have been made in advance for a large group of speakers to have a spokesperson speak on their behalf. Comments must be kept brief and non-repetitive. The general Public Comment portion of the meeting allows the public to address any item within the jurisdiction of the Board of Directors on matters not appearing on the agenda. Public comments on agenda items should be made at the time each item is considered.

3. New Business:
   A. Ad Hoc Committee Reports (*Board will provide this information*)
      a. Governance (Jean Turner)
      b. HR (Mary Mae Kilpatrick)
      c. Finance (Melissa Best-Baker)
      d. Compliance (Jody Veenker)

B. Chief Executive Officer Report *(Board will receive this report)*
    a. Foundation Report
    b. New Chief Medical Officer – Dr. Adam Hawkins
C. Chief Financial Officer Report
    a. Financial & Statistical Reports (*Board will consider the approval of these reports*)
    b. TAG Update *(Board will receive this report)*
D. Revenue Cycle Report, Interim CEO Stephen DelRossi *(Board will receive this report)*
E. Security Report, Bryan Harper *(Board will receive this report)*
F. Disaster Plan Manual, Bryan Harper (*Board will consider the approval of this manual*)
G. BUSD and NIHD MOU for Bronco Clinic (*Board will consider the approval of this MOU*)

4. Chief of Staff Report, Sierra Bourne MD:
    A. Policies (*Board will consider the approval of these Policies and Procedures*)
        a. *Medical Ethics Referrals and Consultation*
        b. *Medical Records Delinquency Policy*
        c. *Medical Staff History & Physical (H&P) Policy*
    B. Medical Executive Committee Report *(Board will receive this report)*

Consent Agenda

All matters listed under the consent agenda are considered routine

and will be enacted by one motion unless any member of the

Board wishes to remove an item for discussion.

5. Approval of minutes of the July 17, 2023 Special Board Meeting *(Board will consider the approval of these minutes)*
6. Approval of Policies and Procedures – Biennial Review, no changes required (*Board will consider the approval of these Policies and Procedures)*
    a. *Attendance at Meetings*
    b. *NIHD Board Meeting Minutes*
    c. *NIHD Board Meeting / Brown Act Compliance*
    d. *Officers and Committees of the Board of Directors*
    e. *Requests for Public Funds, Community Grants, Sponsorships*
    f. *Use by NIHD Directors of District Email Accounts*

---

7. Reports from Board Members (*Board will provide this information*)

8. Adjournment

In compliance with the Americans with Disabilities Act, if you require special accommodations to participate in a District Board meeting, please contact administration at (760) 873-2838 at least 48 hours prior to the meeting.

NIH Foundation Budget - FY 2023

INCOME	$30,000.00
EXPENSE	$10,000.00
TOTAL FUNDRAISING	$20,000.00

Grateful Patient - 2023-09

Item	Income	Expense	Difference
Mailing	$3,000.00	$1,500.00	$1,500.00
Total	**$3,000.00**	**$1,500.00**	**$1,500.00**

Grateful Patient - 2024-03

Item	Income	Expense	Difference
Mailing	$3,000.00	$1,500.00	$1,500.00
Total	**$3,000.00**	**$1,500.00**	**$1,500.00**

Fall Fundraiser - 2023-10

Item	Income	Expense	Difference
Mixer Event	$8,000.00	$3,000.00	$5,000.00
Total	**$8,000.00**	**$3,000.00**	**$5,000.00**

Grateful Patient - 2024-06

Item	Income	Expense	Difference
Mailing	$3,000.00	$1,500.00	$1,500.00
Total	**$3,000.00**	**$1,500.00**	**$1,500.00**

Grateful Patient - 2023-12

Item	Income	Expense	Difference
Mailing	$3,000.00	$1,500.00	$1,500.00
Total	**$3,000.00**	**$1,500.00**	**$1,500.00**

Annual Donor Direct Mail - 2024

Item	Income	Expense	Difference
Annual Appeal	$10,000.00	$1,000.00	$9,000.00
Total	**$10,000.00**	**$1,000.00**	**$9,000.00**

Northern Inyo Healthcare District
Income Statement
Fiscal Year 2023

	7/31/2022	7/31/2021	8/31/2022	8/31/2021	9/30/2022	9/30/2021	10/31/2022	10/31/2021	11/30/2022	11/30/2021	12/31/2022	12/31/2021	1/31/2023	1/31/2022	2/28/2023
Gross Patient Service Revenue															
Inpatient Patient Revenue	3,986,305	2,774,294	3,395,933	2,563,061	1,938,350	3,193,923	2,813,064	3,361,605	3,474,955	3,958,181	3,417,547	2,404,683	3,898,882	3,708,290	2,545,535
Outpatient Revenue	11,474,649	11,563,898	12,619,549	10,530,380	11,643,340	10,677,079	12,337,627	10,581,296	12,582,796	10,120,970	11,309,707	11,882,529	11,943,811	8,803,380	11,030,636
Clinic Revenue	1,112,050	1,074,051	1,281,637	1,155,594	1,298,041	1,126,962	1,312,937	1,206,362	1,616,268	1,137,285	1,602,344	1,136,568	1,552,193	1,448,892	1,266,634
Gross Patient Service Revenue	16,573,004	15,412,242	17,297,119	14,249,034	14,879,730	14,997,964	16,463,628	15,149,263	17,674,019	15,216,437	16,329,598	15,423,780	17,394,886	13,960,561	14,842,805
Deductions from Revenue															
Contractual Adjustments	(6,172,708)	(4,886,114)	(7,321,120)	(6,636,885)	(6,082,559)	(6,880,919)	(9,137,803)	(7,559,945)	(8,553,896)	(7,207,126)	(8,204,159)	(7,224,448)	(7,536,311)	(6,081,113)	(6,829,397)
Bad Debt	(1,834,762)	(1,956,168)	(831,081)	(524,864)	(1,268,812)	(120,841)	589,809	115,976	(134,138)	(132,762)	(2,354,124)	(266,596)	(687,018)	(599,855)	(1,387,069)
A/R Writeoffs	(378,045)	(6,801)	(717,468)	(138,222)	(739,907)	(70,088)	(325,216)	(73,605)	(338,106)	(181,117)	(344,283)	(286,045)	(380,030)	(211,549)	(234,813)
Other Deductions from Revenue	497,912	67,000	(67,000)	67,000	-	67,000	950	67,000	17,166	67,000	410	91,038	-	91,039	-
Deductions from Revenue	(7,887,603)	(6,782,083)	(8,936,670)	(7,232,972)	(8,091,278)	(7,004,848)	(8,872,259)	(7,450,574)	(9,008,974)	(7,454,005)	(10,902,156)	(7,686,051)	(8,603,358)	(6,801,478)	(8,451,279)
Other Patient Revenue															
Incentive Income	-	34,766	-	(35,500)	-	665	-	24,456	-	1,619	-	10	-	(24,026)	-
Other Oper Rev - Rehab Thera Serv	5,303	17,014	4,367	18,560	4,346	13,352	10,361	15,820	7,875	15,908	3,545	2,625	566	8,388	1,660
Medical Office Net Revenue	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Other Patient Revenue	5,303	51,780	4,367	(16,940)	4,346	14,017	10,361	40,275	7,875	17,528	3,545	2,635	566	(15,638)	1,660
Net Patient Service Revenue	**8,690,703**	**8,681,939**	**8,364,816**	**6,999,123**	**6,792,798**	**8,007,133**	**7,601,730**	**7,738,965**	**8,672,921**	**7,779,959**	**5,430,987**	**7,740,364**	**8,792,094**	**7,143,445**	**6,393,187**
Cost of Services - Direct															
Salaries and Wages	2,175,027	2,138,510	2,269,022	2,212,918	2,195,439	2,099,073	2,179,142	2,131,194	2,262,511	2,303,918	2,158,750	2,726,796	2,338,917	2,346,958	1,959,005
Benefits	2,008,070	1,618,760	1,759,698	1,635,349	1,801,034	1,795,655	1,669,695	1,801,576	1,754,398	2,059,894	1,064,181	2,085,215	1,867,561	2,199,930	1,681,176
Professional Fees	1,381,538	1,415,923	1,438,889	1,354,663	1,650,775	1,487,469	1,797,498	1,766,505	1,963,643	1,340,719	1,652,265	1,388,736	1,652,745	1,452,179	1,942,950
Contract Labor	655,016	455,352	622,813	541,517	1,451,288	491,195	1,024,423	527,022	1,493,476	449,716	(20,338)	434,773	1,001,828	865,229	219,870
Pharmacy	211,326	274,517	671,932	354,714	54,166	344,942	136,557	405,802	596,330	392,006	268,920	380,870	360,384	286,978	327,171
Medical Supplies	315,752	277,812	290,221	255,157	578,033	358,049	366,356	369,855	474,848	451,788	448,838	497,972	476,757	184,989	203,442
Hospice Operations	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
EHR System Expense	107,979	112,267	230,353	114,869	220,408	132,491	183,047	112,342	146,908	108,392	54,304	115,958	126,194	119,346	138,908
Other Direct Expenses	546,374	589,703	667,228	544,051	808,934	585,893	572,765	689,732	793,341	618,316	471,021	679,861	598,990	643,886	531,119
Total Cost of Services - Direct	7,401,082	6,882,843	7,950,156	7,013,237	8,760,076	7,294,767	7,929,482	7,804,027	9,485,455	7,724,749	6,097,940	8,310,179	8,423,377	8,099,494	7,003,641
General and Administrative Overhead															
Salaries and Wages	360,265	319,290	365,276	323,708	370,478	319,740	381,872	305,823	373,439	355,039	373,193	412,400	401,590	361,734	368,344
Benefits	356,264	283,420	312,157	299,665	316,570	312,500	1,160,994	243,511	302,169	322,152	(788,291)	382,695	262,752	335,529	272,374
Professional Fees	535,217	342,533	190,076	351,845	318,029	177,703	265,196	194,953	274,630	188,260	191,161	360,435	291,948	225,696	278,757
Contract Labor	30,218	78,500	52,224	69,031	92,958	44,534	57,021	87,853	156,142	111,853	(102,132)	102,071	(25,859)	103,502	27,901
Depreciation and Amortization	318,087	370,335	332,153	358,995	334,828	347,178	362,317	358,655	346,018	347,192	340,523	369,148	342,452	334,665	344,315
Other Administative Expenses	79,314	234,811	164,310	117,308	199,538	140,164	119,767	134,758	314,165	154,566	152,489	190,884	191,302	158,172	172,710
Total General and Administrative Overhead	1,679,363	1,628,889	1,416,196	1,520,552	1,632,402	1,341,820	2,347,167	1,325,552	1,766,564	1,479,063	166,944	1,817,634	1,464,185	1,519,298	1,464,400
Total Expenses	**9,080,446**	**8,511,732**	**9,366,352**	**8,533,790**	**10,392,477**	**8,636,587**	**10,276,649**	**9,129,578**	**11,252,019**	**9,203,811**	**6,264,884**	**10,127,813**	**9,887,562**	**9,618,792**	**8,468,041**
Financing Expense	183,196	179,672	182,350	179,585	180,796	176,035	182,190	138,640	178,894	136,649	183,171	101,007	180,418	227,252	172,904
Financing Income	64,203	173,785	431,229	173,785	247,716	173,785	247,716	173,785	247,716	173,785	247,716	173,785	247,716	173,785	247,716
Investment Income	74,115	23,766	23,389	16,876	(18,154)	20,534	99,582	20,443	16,704	16,045	50,390	27,865	124,884	6,662	41,183
Miscellaneous Income	484,508	499,440	(364,949)	1,105,828	146,486	9,508,790	10,519	384,016	68,632	407,081	2,271,115	2,688,686	485,200	844,798	1,810,358
Net Income (Change is Financial Position)	**49,888**	**687,526**	**(1,094,218)**	**(417,762)**	**(3,404,427)**	**8,897,620**	**(2,499,292)**	**(951,010)**	**(2,424,941)**	**(963,590)**	**1,552,152**	**401,879**	**(418,086)**	**(1,677,354)**	**(148,502)**
Operating Income	(389,742)	170,207	(1,001,537)	(1,534,666)	(3,599,679)	(629,454)	(2,674,919)	(1,390,614)	(2,579,099)	(1,423,852)	(833,897)	(2,387,449)	(1,095,469)	(2,475,347)	(2,074,854)

Northern Inyo Healthcare District
Income Statement
Fiscal Year 2023

	2/28/2022	3/31/2023	3/31/2022	4/30/2023	4/30/2022	5/31/2023	5/31/2022	6/30/2023	6/30/2022	2023 YTD	2022 YTD	Comments
Gross Patient Service Revenue												
Inpatient Patient Revenue	2,908,927	3,633,689	3,231,022	2,295,049	2,950,716	3,261,629	4,083,934	2,123,257	2,987,037	36,784,193	38,125,673	
Outpatient Revenue	8,539,211	12,610,463	11,061,511	12,236,228	11,801,078	13,355,732	12,009,784	12,723,066	11,789,931	145,867,603	129,361,046	
Clinic Revenue	1,067,009	1,550,929	1,246,889	1,390,394	1,250,044	1,526,050	1,264,841	1,443,993	1,292,210	16,953,471	14,406,706	
Gross Patient Service Revenue	12,515,147	17,795,080	15,539,422	15,921,672	16,001,838	18,143,411	17,358,560	16,290,316	16,069,178	199,605,267	181,893,425	
Deductions from Revenue												
Contractual Adjustments	(5,364,554)	(9,900,790)	(6,807,575)	(8,452,990)	(7,317,362)	(8,271,575)	(8,244,588)	(7,565,721)	(11,035,027)	(94,029,030)	(85,245,656)	
Bad Debt	(1,071,017)	525,913	(1,307,312)	(240,320)	(1,288,758)	(1,264,180)	(717,209)	(2,498,013)	(1,712,866)	(11,383,795)	(9,582,273)	
A/R Writeoffs	(417,884)	(721,088)	(362,354)	(450,123)	(611,004)	(245,437)	(362,952)	(265,508)	(314,527)	(5,140,023)	(3,036,147)	
Other Deductions from Revenue	1,910,955	38	67,000	(637,163)	2,121,000	-	399,000	-	2,811,577	(187,687)	7,826,609	
Deductions from Revenue	(4,942,500)	(10,095,928)	(8,410,241)	(9,780,597)	(7,096,123)	(9,781,192)	(8,925,748)	(10,329,242)	(10,250,844)	(110,740,535)	(90,037,467)	
Other Patient Revenue												
Incentive Income	(16)	-	-	-	-	-	-	-	-	-	1,974	
Other Oper Rev - Rehab Thera Serv	11,929	5,396	(10,570)	1,029	(12,701)	696	57,940	-	10,364	45,144	148,629	
Medical Office Net Revenue	-	-	-	-	-	-	-	-	-	-	-	
Other Patient Revenue	11,913	5,396	(10,570)	1,029	(12,701)	696	57,940	-	10,364	45,144	150,603	
Net Patient Service Revenue	**7,584,561**	**7,704,549**	**7,118,611**	**6,142,104**	**8,893,013**	**8,362,915**	**8,490,752**	**5,961,074**	**5,828,698**	**88,909,877**	**92,006,561**	
Cost of Services - Direct												
Salaries and Wages	2,047,905	2,511,015	2,305,644	2,962,848	2,108,120	2,543,864	2,403,672	4,693,942	2,130,467	30,249,481	26,955,174	5,491,366
Benefits	1,799,225	1,831,123	1,750,987	1,865,932	1,630,456	1,780,302	1,813,625	1,776,252	(3,132,943)	20,859,423	17,057,727	2,073,621
Professional Fees	1,498,674	1,716,884	1,493,507	1,923,375	1,432,688	1,615,480	1,746,507	1,814,698	1,992,928	20,550,740	18,370,498	
Contract Labor	971,010	788,024	976,833	500,915	783,328	758,950	950,945	729,261	1,549,007	9,225,525	8,995,926	
Pharmacy	362,249	333,474	330,943	225,543	368,587	(96,169)	292,996	781,308	499,818	3,870,941	4,294,421	
Medical Supplies	159,263	485,465	244,786	466,422	370,285	323,953	343,886	(1,766,340)	866,075	2,663,747	4,379,917	
Hospice Operations	-	-	-	-	-	-	-	-	-	-	-	
EHR System Expense	112,757	160,195	148,178	147,652	126,124	330,555	122,781	435,979	411,023	2,282,482	1,736,527	190,207
Other Direct Expenses	646,224	651,545	655,135	530,520	368,774	495,063	650,384	520,929	1,167,346	7,187,830	7,839,306	
Total Cost of Services - Direct	7,597,308	8,477,724	7,906,014	8,623,208	7,188,362	7,751,998	8,324,795	8,986,029	5,483,720	96,890,168	89,629,495	
General and Administrative Overhead												
Salaries and Wages	334,886	458,763	363,951	520,721	344,920	426,210	355,219	797,424	300,827	5,197,574	4,097,538	
Benefits	310,036	2,870,040	310,978	367,789	366,397	223,735	343,418	297,368	3,983,905	5,953,921	7,494,207	
Professional Fees	198,574	260,367	159,404	403,951	443,120	525,104	124,351	634,797	184,735	4,169,234	2,951,610	
Contract Labor	95,420	27,375	116,407	21,225	68,926	62,613	83,737	74,020	124,669	473,705	1,086,503	
Depreciation and Amortization	298,932	341,803	331,373	340,467	329,978	344,450	341,988	339,325	346,201	4,086,740	4,134,640	
Other Administative Expenses	157,128	163,294	163,160	182,836	208,881	202,135	138,354	140,594	491,990	2,082,454	2,290,176	
Total General and Administrative Overhead	1,394,976	4,121,641	1,445,273	1,836,989	1,762,222	1,784,248	1,387,068	2,283,528	5,432,328	21,963,628	22,054,674	
Total Expenses	**8,992,284**	**12,599,365**	**9,351,287**	**10,460,197**	**8,950,584**	**9,536,246**	**9,711,863**	**11,269,558**	**10,916,047**	**118,853,796**	**111,684,169**	
Financing Expense	472,448	180,509	218,276	178,979	204,403	183,480	210,496	182,548	358,369	2,169,434	2,602,830	
Financing Income	148,687	247,716	173,785	247,716	173,785	247,716	173,785	247,716	1,313,294	2,972,589	3,199,828	
Investment Income	4,964	40,992	(1,624)	158,772	39,227	56,107	2,912	58,185	8,101	726,149	185,770	
Miscellaneous Income	856,972	5,590,718	1,871,757	236,130	823,579	137,633	931,497	153,540	(2,030,176)	11,029,889	17,892,269	
Net Income (Change is Financial Position)	**(869,548)**	**804,101**	**(407,035)**	**(3,854,455)**	**774,617**	**(915,356)**	**(323,414)**	**(5,031,592)**	**(6,154,500)**	**(17,384,726)**	**(1,002,571)**	
Operating Income	(1,407,724)	(4,894,817)	(2,232,677)	(4,318,093)	(57,571)	(1,173,331)	(1,221,111)	(5,308,483)	(5,087,350)	(29,943,919)	(19,677,607)	

Northern Inyo Healthcare District
Balance Sheet
Fiscal Year 2023

	Prior Year Balances	June 2023	June 2022	Comments
Assets				
Current Assets				
Cash and Liquid Capital	9,223,997	19,390,555	9,223,997	(6,144,786)
Short Term Investments	26,808,421	10,497,077	26,808,421	(4.86)
PMA Partnership	-	-	-	
Accounts Receivable, Net of Allowance	21,729,704	9,351,360	21,729,704	
Other Receivables	3,102,882	5,711,717	3,102,882	
Inventory	3,145,539	5,159,474	3,145,539	
Prepaid Expenses	942,007	1,694,180	942,007	
Total Current Assets	**64,952,549**	**51,804,362**	**64,952,549**	
Assets Limited as to Use				
Internally Designated for Capital Acquisitions	-	-	-	
Short Term - Restricted	1,953,496	1,466,355	1,953,496	
Limited Use Assets				
LAIF - DC Pension Board Restricted	639,041	798,218	639,041	
Other Patient Revenue	19,296,858	19,296,858	19,296,858	
PEPRA - Deferred Outflows	-	-	-	
PEPRA Pension	-	-	-	
Total Limited Use Assets	19,935,899	20,095,076	19,935,899	
Revenue Bonds Held by a Trustee	1,111,723	1,078,189	1,111,723	
Total Assets Limited as to Use	**23,001,118**	**22,639,619**	**23,001,118**	
Long Term Assets				
Long Term Investment	2,274,315	2,767,655	2,274,315	
Fixed Assets, Net of Depreciation	77,085,263	77,430,543	77,085,263	
Total Long Term Assets	**79,359,579**	**80,198,197**	**79,359,579**	
Total Assets	**167,313,246**	**154,642,179**	**167,313,246**	
Liabilities				
Current Liabilities				
Current Maturities of Long-Term Debt	2,606,169	822,049	2,606,169	
Accounts Payable	6,250,898	7,768,116	6,250,898	
Accrued Payroll and Related	5,337,975	10,634,804	5,337,975	
Accrued Interest and Sales Tax	99,832	93,155	99,832	
Notes Payable	2,133,708	1,633,671	2,133,708	
Unearned Revenue	2,394,847	(4,542)	2,394,847	
Due to 3rd Party Payors	1,124,159	693,247	1,124,159	
Due to Specific Purpose Funds	-	-	-	
Other Deferred Credits - Pension	2,146,080	2,146,080	2,146,080	
Total Current Liabilities	**22,093,667**	**23,786,581**	**22,093,667**	
Long Term Liabilities				
Long Term Debt	33,455,947	33,455,530	33,455,947	
Bond Premium	240,908	203,263	240,908	
Accreted Interest	16,725,130	17,123,745	16,725,130	
Other Non-Current Liability - Pension	47,950,740	50,366,473	47,950,740	
Total Long Term Liabilities	**98,372,724**	**101,149,011**	**98,372,724**	
Suspense Liabilities	-	-	-	
Uncategorized Liabilities	425,933	649,721	425,933	
Total Liabilities	**120,892,324**	**125,585,313**	**120,892,324**	
Fund Balance				
Fund Balance	44,833,877	43,831,306	44,833,877	
Temporarily Restricted	2,589,615	2,610,286	2,589,615	
Net Income	(1,002,571)	(17,384,726)	(1,002,571)	
Total Fund Balance	**46,420,922**	**29,056,866**	**46,420,922**	
Liabilities + Fund Balance	**167,313,246**	**154,642,179**	**167,313,246**	
(Decline)/Gain		633,135	(8,236,504)	
	-	-	-	

NORTHERN INYO HEALTHCARE DISTRICT

One Team. One Goal. Your Health.

2023 PENETRATION TEST

CYBERSECURITY
EXECUTIVE PRESENTATION

Stern Security™

TABLE OF CONTENTS

Stern Security™

BACKGROUND

2023 Penetration Test

EXTERNAL PENETRATION TEST

1 Attacks are launched from the internet. Simulates an external attacker.

INTERNAL PENETRATION TEST

2 Attacks are launched from inside the network via an on-site laptop. Simulate a compromise on the internal network (ex. successful phishing or malware)

REPORT

3 Results are compiled into a comprehensive report

REMEDIATION

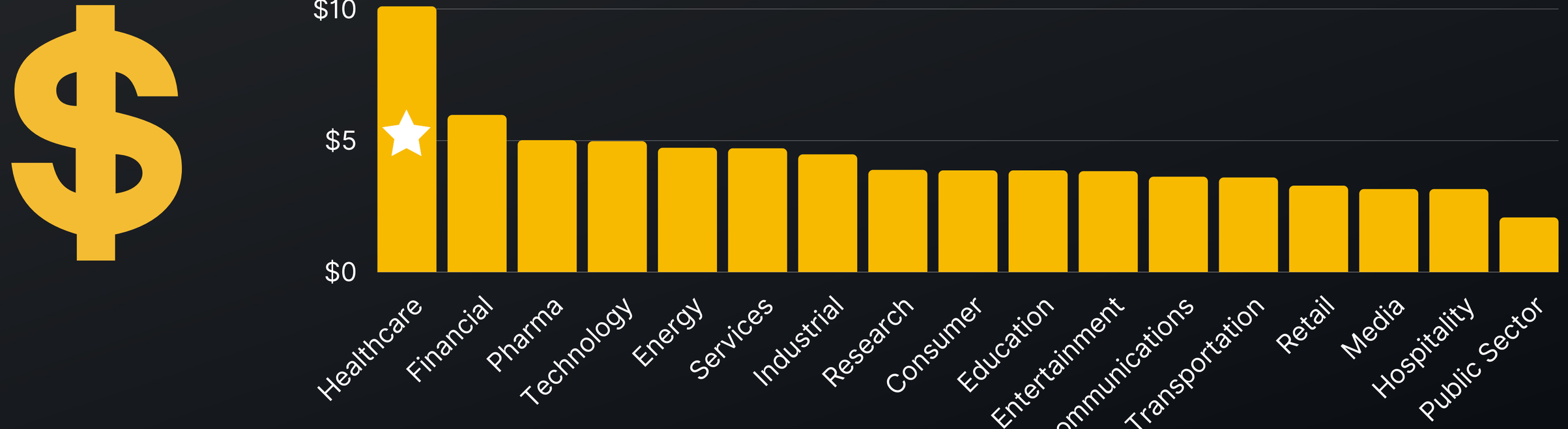
4 Vulnerabilities are resolved. This often occurs during the testing if major issues are discovered.

Stern Security

RISK

2023

Average Cost of a Breach
Measured in US$ millions



Source: Ponemon Institute, 2022

EXTERNAL FINDINGS

No major external findings in 2023

Primary External Findings Include:

Finding	Risk Rating
Outdated Encryption Protocols in Use	LOW
HTTP Header Discloses Internal IP Address	VERY LOW

Stern Security

INTERNAL FINDINGS

Major internal findings in 2023

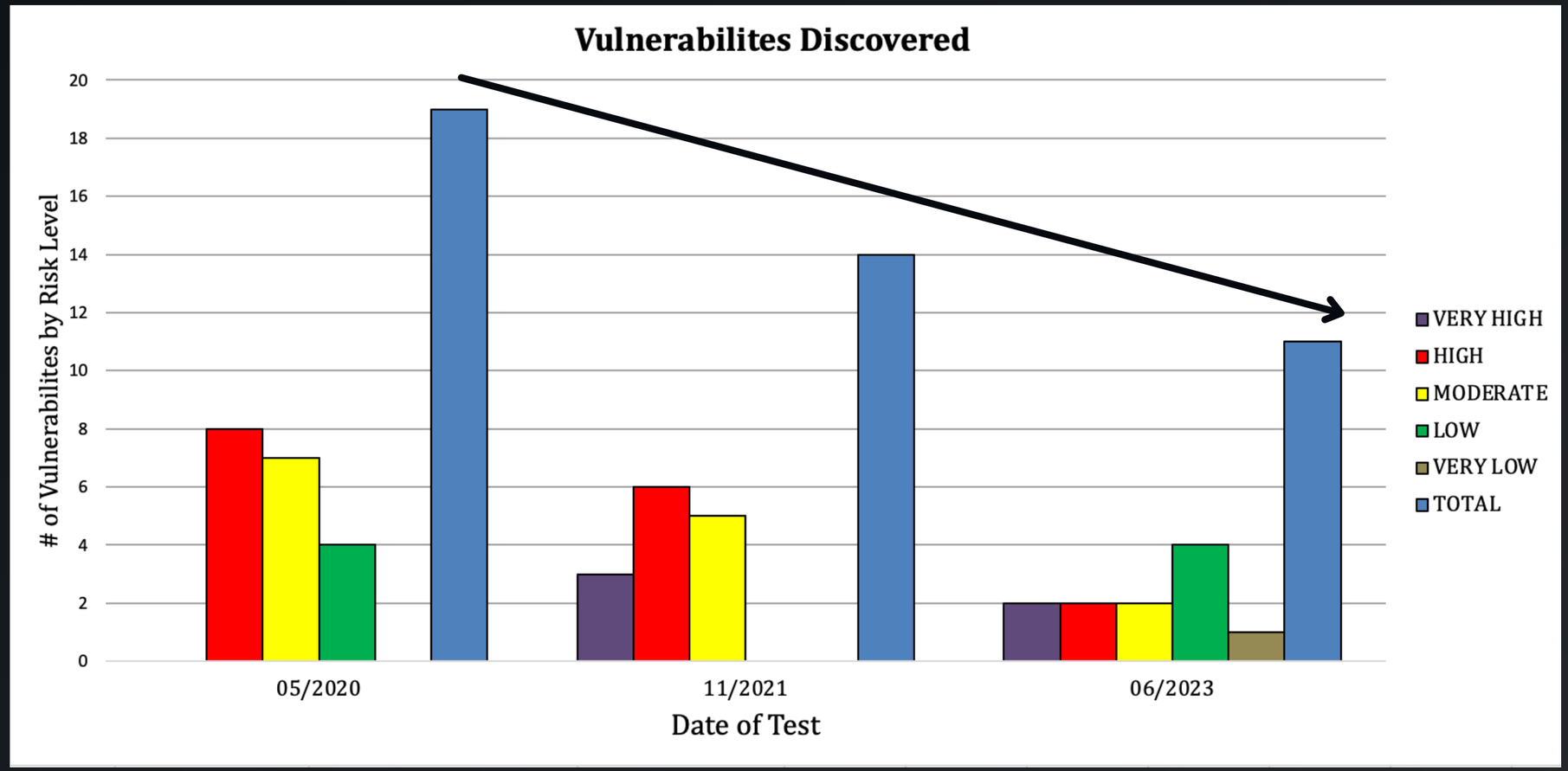
Primary Internal Findings Include:

Finding	Risk Rating
Share Files Contain Sensitive Information	VERY HIGH
Unencrypted PHI/PII in SQL Databases	VERY HIGH
Unsupported Software / Missing Patches	HIGH

Stern Security

DISCOVERED FINDINGS

By Risk Level and Date of Test



Stern Security

SUMMARY

Strong External Security

The security posture continues to improve

Solid Internal Security Improvement

Despite having only one dedicated security employee, year after year, NIHD continues to improve its internal security posture.

THANK YOU

Stern Security

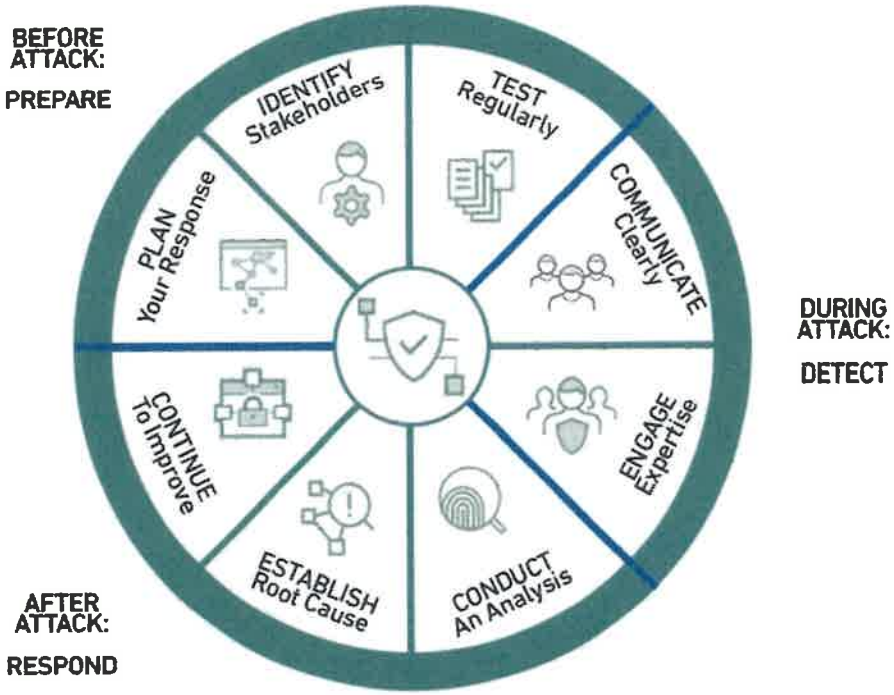
NIHD

Northern Inyo Healthcare District

Cyber Security Incident Response Manual (CSIRM)

&

Disaster Recovery & Planning (DRP)



REV 1.0

Last Update: 04/2023

Hospital Cyber Security Incident Plan

Introduction:
The purpose of this plan is to establish the procedures for managing cyber security incidents that may affect the hospital's information technology systems, staff, patients, and visitors. The plan outlines the roles and responsibilities of hospital staff, communication protocols, and incident response procedures.

Identification of potential cyber security incidents:
The following cyber security incidents are considered most likely to occur in our hospital's environment:

- Unauthorized access to patient records or other confidential information
- Ransomware attacks or other malware infections
- Denial of service attacks on hospital systems or networks
- Social engineering attacks, such as phishing scams

Roles and Responsibilities:
The hospital incident response team (IRT) will be activated in the event of a cyber security incident. The following roles and responsibilities will be assigned:

- Incident commander: Responsible for overall management of the incident response team.
- Cyber security officer: Responsible for identifying and mitigating the cyber security incident.
- Communications coordinator: Responsible for communicating with internal and external stakeholders, including staff, patients, families, media, and law enforcement.
- Technical support: Responsible for providing technical support and expertise to the incident response team.
- Legal and compliance representative: Responsible for ensuring compliance with legal and regulatory requirements.

Communication protocols:
Communication protocols will be established to ensure timely and accurate information is shared with internal and external stakeholders. The following communication protocols will be used:

- All staff must report suspected or actual cyber security incidents to the hospital's incident response team.
- Incident response team members will communicate via secure channels, such as encrypted email or secure messaging platforms.
- Communications with external stakeholders will be coordinated by the communications coordinator.

Incident response procedures:
The following incident response procedures will be followed in the event of a cyber security incident:

- Initial assessment: The incident response team will assess the scope and severity of the cyber security incident.
- Containment: The incident response team will take immediate action to contain the incident and prevent further damage.
- Investigation: The incident response team will conduct a thorough investigation of the cyber security incident to determine the cause and extent of the breach.
- Mitigation: The incident response team will take appropriate steps to mitigate the cyber security incident, such as removing malware, restoring backups, or implementing additional security measures.
- Recovery: The incident response team will work to restore normal operations as quickly as possible.
- Post-incident analysis: The incident response team will conduct a post-incident analysis to identify areas for improvement and update the hospital's cyber security incident plan accordingly.

Conclusion:
This hospital cyber security incident plan is intended to guide the hospital's response to cyber security incidents and ensure the safety of our patients, staff, and visitors. It will be regularly reviewed and updated to ensure its effectiveness in addressing evolving cyber threats.

Important steps to take in cyber attack

- Activate the Incident Response Team (IRT): This involves quickly assembling a team of experts who will lead the response efforts, coordinate communication, and ensure that the incident is contained and resolved as quickly as possible.
- Identify and contain the incident: This involves identifying the scope and severity of the incident and taking steps to contain it, such as disconnecting affected systems or disabling user accounts to prevent further damage.
- Preserve evidence: It's important to preserve evidence of the incident, such as system logs, network traffic data, and user activity, to help identify the source and nature of the incident.
- Investigate the incident: The IRT should conduct a thorough investigation of the incident to determine how it happened, what systems or data were affected, and what actions were taken by the attackers.
- Communicate with stakeholders: Communication is critical during a cyber incident. The IRT should communicate with stakeholders, such as management, employees, customers, vendors, and regulatory bodies, to provide updates on the incident and how it is being addressed.
- Remediate the incident: The IRT should take steps to remediate the incident, such as restoring affected systems or data, applying patches or upgrades to address vulnerabilities, and implementing new security controls to prevent similar incidents from occurring in the future.
- Review and improve incident response procedures: After the incident is resolved, it's important to review the incident response procedures to identify any gaps or areas for improvement and update the procedures accordingly to be better prepared for future incidents.

Who to Contact during an Incident

In the case of a cyber attack in California, there are several entities that may need to be notified, depending on the severity and scope of the attack. The following are some of the key entities that may need to be notified:

- Law enforcement: If the cyber attack involves criminal activity, such as hacking, theft of sensitive information, or cyberstalking, it should be reported to local or state law enforcement. The California Department of Justice also has a Cyber Crime Unit that can assist with cyber crime investigations.

- California Office of Emergency Services (OES): If the cyber attack has the potential to impact critical infrastructure or cause significant harm to public health or safety, it should be reported to the OES. The OES is responsible for coordinating the state's response to emergencies and disasters.

- California Information Security Office (CISO): If the cyber attack involves a state agency or government system, it should be reported to the CISO. The CISO is responsible for overseeing the state's information security program and can assist with incident response and recovery.

- Customers and stakeholders: If the cyber attack involves sensitive or personally identifiable information, customers and stakeholders should be notified as soon as possible. The California Consumer Privacy Act (CCPA) requires businesses to notify consumers in the event of a data breach that exposes their personal information.

- Cybersecurity and Infrastructure Security Agency (CISA): If the cyber attack involves a critical infrastructure sector or has national security implications, it should be reported to the CISA. The CISA is a federal agency that is responsible for protecting the nation's critical infrastructure from cyber threats.

Contact Information

1. Bishop Police Address: 207 W Line St, Bishop, CA 93514 Phone: (760) 873-5866

2. California Office of Emergency Services (OES): You can contact the OES Duty Officer at (916) 845-8911 or email oesnews@caloes.ca.gov.

3. California Information Security Office (CISO): You can contact the CISO at (916) 445-5239 or email ciso@state.ca.gov.

4. Customers and stakeholders: The notification process for customers and stakeholders will vary depending on the type of business or organization involved. However, the California Attorney General's Office has a Data Breach Report Form that can be used to report data breaches and to notify affected customers.

5. Cybersecurity and Infrastructure Security Agency (CISA): You can report cyber incidents to CISA by calling their 24/7 Cyber Incident Hotline at 1-866-615-6464 or by submitting an incident report through their website at https://us-cert.cisa.gov/report.

Items needed for incident command

- Incident Response Plan (IRP): An IRP outlines the steps to be taken in the event of a cyber attack, and it is essential to have it on hand during an incident command. It provides guidance on what actions to take, who is responsible for what, and when to escalate the incident.
- Contact List: A list of key contacts should be available, including IT staff, incident response team members, vendors, legal, and public relations. The contact list should have names, email addresses, phone numbers, and other relevant information to contact the necessary parties quickly.
- Communication Tools: Communication is crucial during an incident, and it is essential to have communication tools available such as walkie-talkies, phones, radios, and instant messaging applications.
- Incident Response Team (IRT): An IRT is a team of experts responsible for managing and resolving cyber attacks. The team should have clear roles and responsibilities, and members should be available to respond quickly to an incident.
- Technical Tools: Technical tools such as firewalls, intrusion detection systems, and anti-virus software should be available to detect and contain the attack.
- Forensic Tools: Forensic tools such as disk imaging software, packet analyzers, and memory analysis tools should be available to help in the investigation and analysis of the attack.
- Backup and Recovery Plan: A backup and recovery plan should be available to restore systems and data in the event of an attack.
- Command Center: A command center should be established where incident response team members can gather to coordinate their efforts, communicate with each other, and manage the incident.
- Incident Log: An incident log should be maintained to document the incident, including details such as the time of the attack, the systems affected, the actions taken, and the outcome.
- Legal and Public Relations Support: Legal and public relations support should be available to manage the legal and reputational aspects of the incident, including media communication and regulatory compliance.

Incident Response Team Responsibility

- Preparation: The IRT should be prepared by having the necessary tools and processes in place to handle incidents. This includes defining roles and responsibilities, establishing communication channels, and creating incident response plans.
- Identification: The IRT should quickly identify potential security incidents through various means such as network monitoring, security event logs, and user reports.
- Containment: The IRT should contain the incident by isolating the affected systems or network segments to prevent further damage or data loss.
- Analysis: The IRT should analyze the incident to determine the cause and scope of the attack or breach. This involves collecting and analyzing data from various sources, such as network traffic, system logs, and memory dumps.
- Remediation: The IRT should remediate the incident by removing the attacker's access, fixing any vulnerabilities or misconfigurations, and restoring systems or data as needed.
- Recovery: The IRT should work with other teams, such as IT and business continuity, to ensure that systems and services are fully restored and that operations can resume as quickly as possible.
- Lessons learned: The IRT should conduct a post-incident review to identify what worked well and what could be improved for future incidents. This includes updating incident response plans and procedures, as well as providing training to staff as needed.

Risk Assessment Steps

- Identify the assets: Identify the information assets that need protection, including hardware, software, data, and people.
- Identify the threats: Identify the potential sources of harm, including natural disasters, human error, and malicious attacks.
- Assess the likelihood: Assess the likelihood of each threat occurring and the impact it could have on the asset if it did occur.
- Assess the impact: Assess the potential impact of each threat, including financial loss, reputation damage, and legal penalties.
- Identify vulnerabilities: Identify vulnerabilities that could be exploited by the identified threats.
- Analyze the risk: Analyze the likelihood and impact of each threat, taking into account the identified vulnerabilities.
- Prioritize risks: Prioritize the identified risks based on their likelihood and potential impact.
- Develop a risk management plan: Develop a plan to manage the identified risks, which may include implementing controls to reduce the likelihood or impact of a threat, transferring risk to a third party, or accepting the risk.
- Implement the plan: Implement the risk management plan, including any controls or procedures necessary to mitigate identified risks.
- Review and update: Regularly review and update the risk assessment and risk management plan to ensure they remain relevant and effective.

Cyber Security Incident Roles

Incident commander:

Activate the hospital incident response team (IRT)
Ensure that all roles are assigned and that the incident response plan is being followed
Facilitate communication between incident response team members and external stakeholders, as needed
Make decisions about resource allocation and other issues that may arise during the incident response process

Cyber security officer:

Investigate the cyber security incident to determine the scope and nature of the attack
Identify the root cause of the incident and take steps to contain the attack
Assess the impact of the attack on hospital systems, data, and infrastructure
Implement mitigation measures, such as removing malware, patching vulnerabilities, or isolating affected systems
Coordinate with technical support to ensure that appropriate measures are taken to restore normal operations as quickly as possible

Communications coordinator:

Develop and execute a communication plan that includes internal and external stakeholders, such as staff, patients, families, media, and law enforcement
Provide regular updates to stakeholders on the status of the incident, including any measures being taken to address the incident and any potential impact on hospital operations
Manage any public relations issues that may arise as a result of the incident
Coordinate with legal and compliance representatives to ensure that any legal and regulatory requirements related to the incident are met

Technical support:

Provide technical expertise to the incident response team on cyber security issues, including malware removal, system restoration, and network isolation
Work with the cyber security officer to identify vulnerabilities and implement appropriate security measures
Ensure that backups are available and can be restored in the event of data loss
Implement additional security measures, such as firewalls, intrusion detection systems, or multi-factor authentication, as needed

Legal and compliance representative:

Ensure that the hospital is in compliance with all legal and regulatory requirements related to the cyber security incident, such as HIPAA, GDPR, or other data protection laws
Provide legal guidance to the incident response team, including advice on reporting requirements, data breach notifications, and liability issues
Work with the communications coordinator to develop messaging that is consistent with legal and regulatory requirements
Coordinate with external legal counsel, as needed, to ensure that the hospital's interests are protected

Incident commander role

- Activate the incident response plan: The incident commander should be the first person to activate the incident response plan and should communicate this to the relevant stakeholders.
- Assemble the incident response team: The incident commander should assemble the incident response team and designate roles and responsibilities. They should also ensure that all team members are informed of the current status of the incident and any relevant information.
- Assess the situation: The incident commander should assess the situation to determine the scope and severity of the incident. This may involve analyzing system logs, interviewing witnesses, and working with other members of the incident response team.
- Establish communication protocols: The incident commander should establish communication protocols for the incident response team and other stakeholders, including senior management, legal counsel, and external parties such as law enforcement or regulators.
- Develop and implement an action plan: The incident commander should develop and implement an action plan for responding to the incident. This may involve isolating affected systems, restoring backups, and implementing security controls to prevent further damage.
- Monitor progress and adjust the response: The incident commander should monitor the progress of the incident response and adjust the response plan as necessary. This may involve making changes to the action plan, communicating with stakeholders, or bringing in additional resources.
- Provide updates to stakeholders: The incident commander should provide regular updates to stakeholders, including senior management and legal counsel, on the status of the incident and the progress of the incident response.
- Document the response: The incident commander should ensure that all aspects of the incident response are properly documented, including actions taken, decisions made, and communication with stakeholders.
- Overall, the incident commander plays a critical role in managing the response to a cyber incident. Their leadership and decision-making skills are essential in ensuring that the incident is handled in an effective and efficient manner.

CISO Role

- Activate the incident response plan: The CISO should be one of the first people to activate the incident response plan and should communicate this to the incident response team.
- Provide technical expertise: The CISO should provide technical expertise to the incident response team and assist with the analysis of system logs, network traffic, and other data sources. They should also assist with identifying the root cause of the incident and determining the scope of the compromise.
- Coordinate with other teams: The CISO should coordinate with other teams, such as network operations, to ensure that the incident response is effective and efficient. They should also work with legal and compliance teams to ensure that the response is in compliance with applicable laws and regulations.
- Implement security controls: The CISO should implement security controls to prevent further damage and protect against future attacks. This may involve implementing firewalls, intrusion detection and prevention systems, and other security measures.
- Communicate with stakeholders: The CISO should communicate with stakeholders, including senior management and legal counsel, to keep them informed of the status of the incident and the progress of the incident response.
- Document the response: The CISO should ensure that all aspects of the incident response are properly documented, including actions taken, decisions made, and communication with stakeholders.
- Overall, the CISO plays a critical role in ensuring that the incident response is effective and efficient. Their technical expertise and knowledge of security controls are essential in identifying and mitigating the impact of a cyber incident.

Communication Plan

Internal communications:

- Send an initial notification to hospital staff, including managers, to inform them of the incident and the actions being taken to address it
- Provide regular updates to staff via email or other internal communication channels, including updates on the status of the incident and any measures being taken to address it
- Conduct staff training sessions to provide guidance on how to respond to the incident and how to prevent similar incidents in the future
- Provide guidance to staff on how to report any suspicious activity or incidents

External communications:

- Notify patients and their families about the incident, including any potential impact on their personal information or health data
- Provide updates to patients and their families on the status of the incident and any measures being taken to address it
- Notify regulatory agencies, such as the Office for Civil Rights (OCR) or other data protection authorities, as required by law
- Notify other stakeholders, such as vendors or contractors, who may be affected by the incident

Media communications:

- Develop a media statement that outlines the incident and the actions being taken to address it
- Designate a media spokesperson who is authorized to speak to the media about the incident
- Provide regular updates to the media on the status of the incident and any measures being taken to address it
- Coordinate with legal and compliance representatives to ensure that any public statements are consistent with legal and regulatory requirements

Legal Role during Incident

- Providing legal advice: The legal team should provide legal guidance and advice to the incident response team on how to handle the incident in compliance with relevant laws and regulations. They should also advise on the legal risks and consequences associated with different courses of action.

- Conducting legal analysis: The legal team should analyze the legal implications of the incident, including potential liability and regulatory obligations. They should also assess any contractual obligations that may be relevant to the incident.

- Managing regulatory and legal obligations: The legal team should ensure that the organization is meeting its legal and regulatory obligations in response to the incident. This may include reporting the incident to regulators or law enforcement, or complying with breach notification laws.

- Managing legal disputes: The legal team should manage any legal disputes that arise from the incident, including coordinating with external counsel, preparing documents and evidence, and representing the organization in court or arbitration proceedings.

- Ensuring compliance with privacy laws: The legal team should ensure that the organization is complying with all relevant privacy laws, including those related to the handling of personal information.

- Providing legal training and guidance: The legal team should provide training to employees on legal issues related to cyber incidents, including how to report incidents and how to handle sensitive information.

- Overall, the legal team plays a critical role in managing legal and regulatory risks associated with cyber incidents. Their input and guidance are essential in ensuring that the organization responds to the incident in a manner that is legally compliant and protects the organization's interests.

Incident Response Plan

- Activation: In the event of a cyber security incident, the incident response team will be activated by the Cyber Security Officer. The incident response team will consist of the Cyber Security Officer, IT Operations Manager, Legal Counsel, and other relevant personnel.
- Assessment: The incident response team will assess the scope and nature of the incident. This will involve reviewing system logs, network traffic, and other data sources to determine the root cause of the incident and the extent of the compromise.
- Containment: The incident response team will take immediate action to contain the incident and prevent further damage. This may involve isolating affected systems, disabling accounts, or blocking access to network resources.
- Analysis: The incident response team will conduct a detailed analysis of the incident to identify the root cause and determine the impact on systems and data. This will involve reviewing logs and other data sources, as well as conducting forensic analysis if necessary.
- Mitigation: The incident response team will develop and implement a plan to mitigate the impact of the incident. This may involve restoring data from backups, patching systems, or implementing new security controls.
- Communication: The incident response team will communicate with relevant stakeholders, including senior management, legal counsel, and other relevant parties. Communication will be ongoing throughout the incident response process to keep stakeholders informed of progress and actions taken.
- Documentation: The incident response team will document all aspects of the incident response process, including actions taken, decisions made, and communication with stakeholders. Documentation will be used to inform future incident response planning and training.
- Recovery: Once the incident has been contained and mitigated, the incident response team will work to restore systems and data to their previous state. This will involve testing systems and data to ensure that they are functioning properly and that no further compromise has occurred.
- Lessons learned: After the incident has been resolved, the incident response team will conduct a review to identify areas for improvement in the incident response plan and process. This review will be used to inform future incident response planning and training.

Incident Response Team Responsibility

- Preparation: The IRT should be prepared by having the necessary tools and processes in place to handle incidents. This includes defining roles and responsibilities, establishing communication channels, and creating incident response plans.
- Identification: The IRT should quickly identify potential security incidents through various means such as network monitoring, security event logs, and user reports.
- Containment: The IRT should contain the incident by isolating the affected systems or network segments to prevent further damage or data loss.
- Analysis: The IRT should analyze the incident to determine the cause and scope of the attack or breach. This involves collecting and analyzing data from various sources, such as network traffic, system logs, and memory dumps.
- Remediation: The IRT should remediate the incident by removing the attacker's access, fixing any vulnerabilities or misconfigurations, and restoring systems or data as needed.
- Recovery: The IRT should work with other teams, such as IT and business continuity, to ensure that systems and services are fully restored and that operations can resume as quickly as possible.
- Lessons learned: The IRT should conduct a post-incident review to identify what worked well and what could be improved for future incidents. This includes updating incident response plans and procedures, as well as providing training to staff as needed.

Technical Plan for Incident

Receive and triage support requests

- Ensure that all support requests are logged and assigned to the appropriate support agent
- Prioritize support requests based on urgency and impact to the business
- Communicate the status of the support request to the customer or user

Diagnose and troubleshoot the issue

- Gather information from the user or customer about the issue and any error messages they may have received
- Use appropriate diagnostic tools to identify the root cause of the issue
- Develop and implement a solution to address the issue

Escalate complex issues

- Identify issues that require escalation to a higher level of support, such as a senior support agent or a specialist team
- Provide all necessary information to the higher level of support to enable them to resolve the issue

Document and track support requests

- Record all details of the support request, including the issue, the solution implemented, and any follow-up actions required
- Use a tracking system to ensure that all support requests are addressed and resolved within a specified timeframe
- Analyze support request data to identify trends and areas for improvement in the support process

Provide ongoing support

- Follow up with users or customers to ensure that the issue has been resolved to their satisfaction
- Provide ongoing support to prevent similar issues from occurring in the future, such as providing guidance on how to avoid common issues or offering training on new systems or applications
- Overall, a tech support plan of action should be designed to provide timely and effective support to users and customers, while also ensuring that all support requests are documented and tracked to enable continuous improvement of the support process.

IRT Tools and Third Party Partners

- OSSEC: An open-source host-based intrusion detection system that can monitor system logs and detect suspicious activity.
- Suricata: An open-source network intrusion detection and prevention system that can monitor network traffic and detect threats.
- The Sleuth Kit: An open-source digital forensics toolkit that can help with file system analysis, data recovery, and forensic analysis.
- Security Onion: An open-source Linux distribution that includes several network security monitoring tools, including Snort, Suricata, Zeek, and OSSEC.
- MISP: An open-source threat intelligence platform that can help gather and share threat intelligence information.
- Elastic Stack: An open-source log management and analysis platform that can help with incident investigation and analysis.
- Wireshark: An open-source network protocol analyzer that can capture and analyze network traffic.

Third Party IRT(s)

1. Mandiant/FireEye
2. Kroll
3. CrowdStrike
4. SecureWorks
5. Trustwave
6. Symantec
7. IBM X-Force Incident Response and Intelligence Services
8. Deloitte

Forms to use during Incident

1. Incident Report Form: This form is used to document details of the incident, including date and time, type of attack, the affected systems, and the actions taken to respond. It helps to capture all relevant information about the incident in one place.

2. Evidence Collection Form: This form is used to document evidence collected during an investigation. It should include details such as the date and time of collection, the type of evidence, and the location of the evidence. It can help to ensure that all relevant evidence is collected and properly documented.

3. Communication Log: This form is used to document all communication related to the incident, including phone calls, emails, and other forms of communication. It should include the date and time of the communication, the name and contact information of the person or organization contacted, and a brief summary of the conversation.

4. Chain of Custody Form: This form is used to document the movement of evidence from the time it is collected until the time it is presented in court. It should include details such as the date and time the evidence was collected, the name of the person who collected it, and the name of the person who received it.

5. Post-Incident Review Form: This form is used to evaluate the incident response process and identify areas for improvement. It should include questions about what worked well, what didn't work well, and what changes could be made to improve the response process for future incidents.

Incident Report Form

- Date of Incident:
- Time of Incident:
- Location of Incident:
- Description of Incident:
- Impact of Incident:

Contact Information for Those Affected:

Name:
Phone Number:
Email Address:
Mailing Address:

Contact Information for Point of Contact:

Name:
Phone Number:
Email Address:
Mailing Address:

Description of Response:

Actions taken during the incident:
Additional information about the incident:
Recommendations for future prevention:

Attachments:

Any additional information or documents related to the incident.

Completed by:

Name:
Title:
Date:

Evidence Collection Form

Date and Time of Collection:

Location of Collection:

Item Description:

Type of item:
Manufacturer:
Model:
Serial Number:
Description of item:

Chain of Custody:

Date and time collected:
Name of person collecting evidence:
Signature of person collecting evidence:
Date and time transferred:
Name of person receiving evidence:
Signature of person receiving evidence:

Description of Evidence Collection:

Detailed description of how the evidence was collected:
Any relevant observations made during the collection process:

Attachments:

Any additional information or documents related to the evidence collection.

Completed by:

Name:
Title:
Date:

Communication Log Examples:

Date/Time: 2023-03-29, 10:00 AM Incident Type: Phishing Attack Affected System: Email System Impact: Several users received phishing emails and clicked on the links Actions Taken:

- Isolated the affected systems from the network to prevent further damage
- Notified the IT team and security personnel
- Conducted a preliminary investigation to determine the scope of the attack
- Identified the source of the attack and blocked the IP address
- Conducted a scan on all affected systems to ensure no malware was installed
- Notified affected users and provided them with instructions on what to do next
- Updated the security policies and procedures to prevent similar attacks from occurring in the future

Date/Time: 2023-03-29, 11:00 AM Incident Type: Denial of Service (DoS) Attack Affected System: Web Server Impact: Website was unavailable for 30 minutes Actions Taken:

- Isolated the affected systems from the network to prevent further damage
- Notified the IT team and security personnel
- Conducted a preliminary investigation to determine the scope of the attack
- Identified the source of the attack and blocked the IP address
- Configured the firewall to block similar attacks in the future
- Updated the security policies and procedures to prevent similar attacks from occurring in the future

Date/Time: 2023-03-29, 2:00 PM Incident Type: Malware Infection Affected System: Finance Department Server Impact: Data on the server was encrypted and unavailable Actions Taken:

- Isolated the affected systems from the network to prevent further damage
- Notified the IT team and security personnel
- Conducted a preliminary investigation to determine the scope of the attack
- Identified the type of malware and its origin
- Restored the data from the backup system
- Updated the security policies and procedures to prevent similar attacks from occurring in the future

Chain of Custody Form

Case Number: _____
Date Collected _____
Time Collected _____
Evidence Number: _____
Collected By: _____
Collected From: _____
Location: _____
Description of Evidence: _____

Chain of Custody:

Date	Time	Collected By	Collected From	Location Description

Comments:

Post-Incident Review Form

Date of review: _____

Incident details:

Date of incident: _____
Time of incident: _____
Type of incident: _____

Description of incident:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Disaster Recovery Plan

Introduction
The disaster recovery plan outlines the procedures to be followed in the event of a disaster that impacts the company's IT systems. The plan is designed to ensure that the company's critical systems are restored as quickly as possible to minimize the impact on operations.

Disaster Recovery Team
The disaster recovery team is responsible for managing the recovery effort. The team should include representatives from IT, operations, security, and other relevant departments.

Backup and Recovery
All critical data and systems should be backed up regularly to ensure that they can be restored in the event of a disaster. The backup data should be stored off-site in a secure location.

Disaster Recovery Procedures
The following procedures should be followed in the event of a disaster:

a. Alert the Disaster Recovery Team: The disaster recovery team should be notified as soon as possible after the disaster is detected.

b. Assess the Damage: The extent of the damage should be assessed, and the priority systems that need to be restored should be identified.

c. Activate the Disaster Recovery Plan: The disaster recovery plan should be activated, and the recovery team should begin restoring the critical systems.

d. Restore Data and Systems: The backed-up data and systems should be restored to the appropriate locations.

e. Test the Restored Systems: The restored systems should be tested to ensure that they are functioning correctly.

f. Resume Operations: Once the restored systems have been tested and verified, operations can be resumed.

Communication Plan
A communication plan should be established to ensure that all stakeholders are informed of the recovery efforts. This plan should include contact information for key stakeholders, such as employees, customers, vendors, and regulatory agencies.

Training and Testing
The disaster recovery plan should be tested regularly to ensure that it is effective. The recovery team should also receive regular training to ensure that they are prepared to respond to a disaster.

Revision and Maintenance
The disaster recovery plan should be revised and updated regularly to ensure that it remains effective. This should include updates to the backup and recovery procedures, as well as any changes to the IT systems or business operations.

Conclusion
A well-designed disaster recovery plan can help minimize the impact of a disaster on a company's operations. By following the procedures outlined in this plan, the company can restore its critical systems as quickly as possible and resume normal operation

Disaster Recovery Planning Form

Name: Northen Inyo Healthcare District

Date: _____

Prepared By: _____

Critical Systems and Data

- Identify the critical systems and data that need to be backed up and restored in the event of a disaster.

System/Data Location Backup Frequency Backup Location

- Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Define the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical system and data.

System/Data RTO RPO

- Disaster Recovery Team
- Identify the members of the disaster recovery team and their roles and responsibilities.

Name Role Contact Information

- Communication Plan
- Define the communication plan to be followed in the event of a disaster.

Communication Method Recipient Contact Information

- Backup and Recovery Procedures
- Define the backup and recovery procedures for each critical system and data.

System/Data Backup Procedure Recovery Procedure

- Training and Testing
- Define the training and testing requirements for the disaster recovery team.

Training Requirement Testing Requirement

- Revision and Maintenance
- Define the revision and maintenance requirements for the disaster recovery plan.

Revision Frequency Maintenance Requirement

By signing below, I acknowledge that I have reviewed and approved this disaster recovery planning form.

Signature: _____

Date: _____

Disaster Recovery Plan - Steps

Purpose
The purpose of this disaster recovery plan (DRP) is to ensure the continuity of critical business functions in the event of a disaster or disruptive incident. This DRP provides a framework for the organization to respond to, and recover from, any unplanned event that impacts the availability of critical systems, processes or facilities.

Scope
This DRP applies to all critical business functions, systems and processes of the organization, and all employees and third-party service providers who have a role in the recovery of these critical business functions.

Risk Assessment
The organization will perform a risk assessment to identify potential threats and risks to the critical business functions and develop appropriate mitigation and contingency plans.

Disaster Response
The following steps will be taken in the event of a disaster or disruptive incident:

- The incident will be immediately reported to the Incident Response Team (IRT) by any employee who discovers it.
- The IRT will assess the situation and determine the severity and scope of the incident.
- The IRT will activate the DRP and initiate the recovery process.
- The IRT will communicate with all relevant stakeholders including employees, third-party service providers, customers, and vendors.

Recovery Procedures
The following procedures will be followed during the recovery process:

- The IRT will determine the recovery strategy and plan, which includes restoring critical systems, data, and facilities.
- The IRT will prioritize recovery efforts based on the criticality of the business function.
- The IRT will monitor progress and update stakeholders on the recovery process.
- The IRT will test the recovery plan to ensure that it is effective and efficient.

Plan Maintenance
The DRP will be reviewed and updated at least annually, or more frequently if changes in the business, systems, or processes occur. The review will include testing and validating the DRP.

Conclusion
This DRP outlines the procedures to be followed in the event of a disaster or disruptive incident. It provides a framework to ensure the continuity of critical business functions and minimize the impact of a disaster on the organization.

Services to Restore Action Planning

NIHD restore order of most critical to least (Services and Servers):

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____
20. _____
21. _____

22. _____

23. _____

24. _____

25. _____

26. _____

27. _____

28. _____

29. _____

30. _____

31. _____

32. _____

33. _____

34. _____

35. _____

36. _____

37. _____

38. _____

39. _____

40. _____

41. _____

42. _____

43. _____

44. _____

45. _____

46. _____

47. _____

48. _____

49. _____

50. _____

51. _____

52. _____

53. _____

54. _____

55. _____

56. _____

57. _____

58. _____

59. _____

60. _____

61. _____

62. _____

63. _____

64. _____

65. _____

66. _____

67. _____

68. _____

69. _____

70. _____

71. _____

72. _____

73. _____

74. _____

75. _____

76. _____

77. _____

78. _____

79. _____

80. _____

81. _____

82. _____

83. _____

84. _____

85. _____

86. _____

87. _____

88. _____

89. _____

90. _____

91. _____

92. _____

93. _____

94. _____

95. _____

96. _____

97. _____

98. _____

99. _____

MEMORANDUM OF UNDERSTANDING

BETWEEN BISHOP UNIFIED SCHOOL DISTRICT AND NORTHERN INYO HEALTHCARE DISTRICT

This Memorandum of Understanding ("**MOU**") is entered into this ____ day of June, 2023 ("**Effective Date**"), by and between Bishop Unified School District (the "**District**") and Northern Inyo Healthcare District, a political subdivision of the State of California, doing business as Northern Inyo Hospital ("**NIH**"). District and NIH are collectively referred to as the "**Parties**."

RECITALS

A. WHEREAS, pursuant to Education Code sections 38130 et seq. (the "**Civic Center Act**"), the management, direction, and control of school facilities are vested in the District's Board of Trustees ("**Board**"), and the Board may provide for the use of school facilities as a civic center where such use is consistent with school purposes and does not interfere with the regular conduct of schoolwork; and

B. WHEREAS, the District owns and operates certain real property known as Bishop Union High School, located at 301 N. Fowler Street, Bishop, California, 93514 (the "**School Site**"), which includes certain facilities the District is willing to make available to NIH to operate a school-based health center when such facilities are not being used for District purposes; and

C. WHEREAS, NIH is federally qualified to provide health care services through a hospital based rural health clinic and a school-based health center program ("**Health Center Program**") to be located at the School Site (the "**Health Center**"); and

D. WHEREAS, NIH is willing to operate and manage the Health Center, and to provide those medical, mental health, health education, and other services as set forth in **Exhibit A,** attached hereto and incorporated herein ("**Services**") to District students attending Bishop Union High School and Palisade Glacier High School; and

E. WHEREAS, the District has determined that such Services to be provided by NIH are beneficial for eligible District students and that enhancing the health of students through such Services thereby supports their academic growth and achievement; and

F. WHEREAS, the District is willing to contract with NIH for the provision of the Health Center Program, and is further willing to permit NIH to use and occupy certain District facilities located at the School Site, more particularly identified and described hereunder and in the Site Plan attached as **Exhibit B,** under the terms and conditions set forth in this MOU, and in accordance with law, for the purpose of operating the Health Center.

NOW, THEREFORE, in consideration of the covenants and conditions of this MOU, including the Recitals hereof, which herein incorporated by reference, the Parties hereby agree as follows:

MEMORANDUM OF UNDERSTANDING

1. Purpose of MOU. The Parties agree that the purpose of this MOU is to set out the terms and conditions whereby NIH will be permitted to use and occupy the Health Center for the purpose of providing eligible District students with those Services as described in **Exhibit A** at no- or low-cost to eligible District students.

2. Eligibility for Services. All District students attending Bishop Union High School ("**BUHS**") and Palisade Glacier High School ("**PGHS**") are eligible for Services under this MOU ("**Eligible Students**"). Eligible Students also include those students attending BUHS or PGHS who are deemed to have complied with the residency requirements for school attendance in the District as set out in Education Section 48204, including students placed in group homes, Licensed Children's Institutions, and foster homes within the District. Students who have been suspended or expelled from BUHS or PGHS but who continue to reside within the District's boundaries, remain eligible for Services during the pendency of the students' suspension or expulsion.

3. Term. The term of this MOU shall be from the Effective Date, through June 30, 2025 ("**Term**"), unless earlier terminated as provided herein or extended by written agreement signed by the Parties.

4. Waiver of Fees. In acknowledging the importance of the Services that will be made available to eligible District students through the operation of the Health Center, the District hereby agrees to waive all facilities use fees for NIH's use of the Health Center for the Term of this MOU.

5. Operation and Management of Health Center. NIH will be responsible for supervising, managing and directing all Health Center operations, including the hiring and supervision of all employees of the Health Center, who will at all times be employees or independent contractors of NIH. NIH will be responsible for obtaining all required permits, and for complying with all laws and regulations pertaining to the operation of the Health Center and the provision of the Services, in addition to compliance with any applicable granting terms and requirements regarding the operation of the Health Center and the use of grant funds, whether such terms and requirements are now in force or hereinafter enacted (the "**Grant Terms**"). NIH will provide all budgeting and development services for the operation of the Health Center including, without limitation, grant writing and solicitation of individual giving. The District will be entitled, but not required, to reasonably monitor and inspect the operation of the Health Center for conformity with the terms of this MOU and any applicable Grant Terms.

6. Financial Responsibility for Operations. NIH will pay costs associated with Health Center operations including, without limitation, the hiring and employment of the Health Center employees and independent contractors, the processing of payroll, tax payments, workers' compensation insurance or self-insurance, group health insurance benefits, accounting and wage reporting services for Health Center employees, annual independent audits of the Health Center as part of NIH's overall audit process, the preparation of legally required reports to funding sources, and the like. NIH's responsibility for operations of the Health Center shall also include the collection, maintenance, and provision of all statistical information, demographics, and information required to be gathered, maintained, or submitted regarding the operations of the Health Center pursuant to law, regulation or any applicable Grant Terms.

7. Provision of Services.

a. NIH shall provide only those Services as described in **Exhibit A** to Eligible Students, on those terms and conditions described herein.

b. Urgent or emergency care or services beyond the scope of those Services set out in **Exhibit A** shall not be provided at the Health Center. Eligible Students requiring urgent or emergency services or services other than those Services listed in **Exhibit A,** shall be referred, as appropriate, to NIH clinics, other specialty health care providers, or to the nearest hospital emergency room.

c. Eligible Students who become ill or are injured during school hours may first be seen by a District School Nurse or Health Aide in accordance with District policy. However, NIH staff may provide emergency first aid or treatment for a student or stabilization of a student who is seriously injured during school hours before that student is transported to an emergency room or other health care provider.

d. Except where applicable law authorizes confidential medical services, parents or legal guardians must provide written authorization for the provision of all Services to minor children.

e. District schools will maintain and provide Health Center parent consent forms with new student registration mailing and other mailings as appropriate.

8. Qualifications of Health Center Personnel. Services shall be made available and provided to Eligible Students by trained and qualified NIH physicians, physician's assistants, nurse practitioners, registered nurses, and qualified support staff ("**NIH Staff**") at the Health Center on following schedule: a maximum of 2 half days per week (4 hours per day). NIH shall adhere to all applicable state licensing requirements and applicable credentialing and privileging standards when hiring health care providers to provide Services to Eligible Students at the Health Center.

9. Billing and Collection Activities by NIH; Enrollment in Public Benefit Programs. NIH may bill and collect payment for all services provided to its patients, including Eligible Students, through appropriate third party payors such as Medi-Cal, CHDP, and insurance. All revenues generated by the Health Center are understood and agreed to be the property of NIH and retained by NIH. NIH staff may assist parents or legal guardians of Eligible Students without private or public health insurance in applying for and completing applications for qualification in any available public health benefit program. The District will have no responsibility for Eligible Student patients' unpaid bills.

10. Equipment. Except as otherwise provided herein, NIH shall provide, at its sole cost, all necessary furnishings, durable and disposable medical equipment, supplies, materials and other items necessary to properly provide the Services under this MOU and to maintain and operate the Health Center.

11. Utilities. With the exception of any specialized services required for the disposal of medical waste, the District will pay all utilities necessary for the operation of the Health Center including, without limitation, water, gas, electricity and trash disposal.

12. Telephones & Computer Equipment. NIH will provide its own telephones, computer hardware and software, and related equipment for use at the Health Center, and shall pay for all of its telephone and internet services therein.

13. Custodial Services. The District shall provide all routine custodial services for the Heath Center; however, NIH shall be responsible for any medical waste requiring specialized disposal. NIH will maintain the cleanliness of the Health Center in accordance with federal and state regulations, including all OSHA regulations, for the cleanliness of health centers.

14. Communication. In the interest of promoting and maintaining a strong and positive collaboration, The District and NIH shall each identify one employee to serve as a "Health Center Liaison" to be responsible for regular communication and coordination with each other regarding issues concerning the Health Center. District personnel will respond to requests from Health Center personnel in a reasonable time period in order to ensure continuity and quality of health care to Eligible Students.

15. Fingerprinting Requirements. Pursuant to California Education Code section 45125.1, before any agents or employees of NIH may enter school grounds where they may have any contact with pupils, NIH shall submit fingerprints of its employees and agents or independent contractors in a manner authorized by the California Department of Justice, together with applicable fees. NIH shall not permit any employee or agent or independent contractor to come in contact with pupils of the District until the Department of Justice has ascertained that such NIH employee has not been convicted of a felony as defined in Education Code section 45122.1.

16. Access to Information. Subject to compliance with federal and state law concerning pupil record information, Health Center personnel will be given access to student information, such as class schedules, so that the Health Center can more easily provide the Services set forth in this MOU. For example, Health Center personnel may access student emergency and contact information maintained by the District through emergency cards and/or the school's online student information system. Such access to information shall be coordinated through the District's Health Center Liaison.

17. Confidentiality.

a. HIPAA. The Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") governs the privacy and security of patients' protected health care information. NIH shall comply with all aspects of HIPAA as well as other state and federal privacy laws in providing Services to Eligible Students by, among other things: (i) properly using or disclosing health care information that comes into NIH's possession in the operation of the Health Center and only using such information for the purposes for which it was intended; and (ii) safeguarding all District students' health care information from misuse. The District agrees to assist NIH in complying with its duties under HIPAA to the extent any District student's protected health care information comes into the District's possession in the performance of any of its duties under this MOU and to otherwise respect student's right to privacy and confidentiality of their protected health care information, including mental health care records, and information in accordance with applicable regulations, rules and guidelines. The District agrees to execute a standard business associate agreement committing the District to comply with HIPAA guidelines in the use and disclosure of any District student's protected health care information.

b. FERPA & California Education Code. The Family Educational Rights and Privacy Act of 1974, 20 USC § 1232g, and Chapter 6.5 (commencing with section 49060) of Part 27 of Division 4 of Title 2 of the California Education Code govern the privacy of the District's pupil records. The District shall comply with all aspects of said laws as well as other state and federal privacy laws in providing pupil record information to NIH by, among other things: (i) properly using or disclosing pupil record information that comes into the District's possession in connection with the operation of the Health Center and only using such information for the purposes for which it was intended; and (ii) safeguarding District pupil record information from misuse. NIH agrees to assist the District in complying with its duties under said laws to the extent any District protected pupil record information comes into NIH's possession in the performance of any of its duties under this MOU and to otherwise respect student's right to privacy and confidentiality of their protected pupil information. If so requested, NIH agrees to execute a standard agreement committing it to comply with said laws in the use and disclosure of any District protected pupil record information.

18. No Referrals.

a. Nothing in this MOU requires, is intended to require, or provides payment or benefit of any kind (directly or indirectly) for the referral of individuals or business to either Party. Neither Party shall track such referrals for purposes relating to setting the compensations of their professionals or influencing their choice.

b. The Parties agree and understand that neither Party is offering or soliciting remuneration to/from the other Party for patient referrals. Nothing in this MOU restricts the ability of patients to choose their own provider and each provider shall inform its patients of their freedom to choose any willing provider.

c. Each Party agrees that it will at all times operate in compliance with all federal, state, and local laws, rules, and regulations relating to its activities hereunder, including but not limited to instructions issued by the Centers for Medicare and Medicaid Services, the False Claims Act, the Anti-Kickback Statute, the Physician Self-Referral Law (Stark law), the Office of Inspector General's Exclusion Authorities, and the Civil Monetary Penalties Law.

19. Assurances of Non-Discrimination. NIH shall not unlawfully discriminate in employment or in the provision of Services on the basis of any characteristic or condition upon which discrimination is prohibited by state or federal law or regulation applicable to NIH.

20. Policies and Procedures. The District will inform Health Center personnel in writing of the District procedures on how to handle the following:

a. Protocols when a student is sick or injured, no District Nurse or Health Center Nurse is onsite, and/or a parent/guardian is not reachable; and

b. Emergency procedures for events including fire, earthquake, violence or threat of violence on campus.

21. Student Access. In accordance with District policy and practice, the District will ensure that students who have been given an approved pass are allowed to leave class or other school activities to use the Health Center.

22. Indemnification.

a. NIH shall hold harmless, defend and indemnify District, its agents, officers and employees from and against any liability, claims, actions, costs, damages or losses of any kind, including death or injury to any person and/or damage to property, including District property, arising from, or in connection with: (i) the operation of the Health Center; or (ii) any negligent acts or omissions, or any intentional misconduct of NIH or its agents, officers employees, and/or subcontractors in performance of services rendered pursuant to this MOU. This indemnification specifically includes any claims that may be made against District by any taxing authority asserting that an employer-employee relationship exists by reason of this MOU, and any claims made against District alleging civil rights violations by NIH under Government Code section 12920 et seq., California Fair Employment and Housing Act or Title VII of the federal Civil Rights Act. This indemnification obligation shall continue beyond the term of this MOU as to any acts or omissions occurring under this MOU or any extension of this MOU.

b. The District shall hold harmless, defend and indemnify NIH, its agents, officers, and employees from and against any liability, claims, actions, costs, damages, or losses of any kind, including death or injury to any person and/or damage to property, including NIH property, arising from, or in connection with, any negligent acts or omissions, or any intentional misconduct of the District or its officers, employees, agents, and/or subcontractors, other than NIH, in performance of services rendered pursuant to this MOU. This indemnification obligation shall continue beyond the term of this MOU as to any acts or omissions occurring under this MOU or any extension of this MOU.

23. Independent Contractor. In the performance of the Parties' duties and obligations under this MOU, it is mutually understood and agreed that each Party is at all times acting and performing as an independent contractor. Neither Party shall exercise or have control or direction over the methods by which other Party shall perform its duties and obligations under this MOU. This MOU is not intended to create a partnership, joint venture, or other relationship between NIH and District other than an independent contractor relationship.

24. Insurance. NIH shall maintain in force, at all times during the term of this MOU, commercial, automobile, Workers' Compensation and Employee's Liability, and medical malpractice liability insurance, or programs of self-insurance, in the amount, manner and form set forth in the attached **Exhibit C.** NIH shall, to the extent required by law, provide Workers' Compensation and Employee's Liability insurance at NIH's own cost and expense, and neither NIH, nor its carrier, shall be entitled to recover from the District any costs, settlements, or expenses of Workers' Compensation or Employer's Liability claims arising out of this MOU, except when such claims are the sole result of District negligence.

25. Termination. Either party hereto may terminate this MOU at any time without cause on 120 days' written notice. In addition, this MOU may also be terminated by either party for "cause" on 30 days' notice to the other, after written notice and opportunity is given to the breaching party to "cure" the breach and the breach has not been cured. For purposes of this MOU "cause" shall include a determination by either Party that any of the following events has occurred: (a) that the other Party is in breach of any material term or condition of this MOU; or (b) in the event of the inability of the other Party to perform the duties described in this MOU.

26. Entire Understanding. This MOU constitutes the entire understanding with respect to the subject matter hereof and supersedes all prior or contemporaneous oral or written agreements or understandings as to this particular subject matter. This MOU may not be amended except by the written agreement signed by authorized representatives of both Parties.

27. Governing Law. This MOU shall be governed by and interpreted under the laws of the State of California applicable to instruments, persons, transactions, and subject matter which have legal contacts and relationships exclusively within the State of California. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the Superior Court of the State of California for Inyo County, subject to any motion for transfer of venue.

28. Binding upon Successors and Assigns. All covenants, terms, provisions, and agreements contained herein shall be binding upon and inure to the benefit of the permitted successors, executors, heirs, representatives, administrators, and assigns of the Parties hereto.

29. Assignment/Subcontracting. Unless otherwise provided in this MOU, the District is relying on the personal skill, expertise, training, and experience of NIH and NIH's employees in providing Services under this MOU, and no part of this MOU may be assigned or subcontracted by NIH without prior written consent of District; provided, however, NIH shall have the right, without obtaining District's prior consent, to assign or subcontract all or any portion of its obligations under this MOU to any affiliate of NIH. As used in this paragraph "affiliate of NIH" means an entity that controls, is controlled by, or is under common control with NIH.

30. Severability. If any provision of this MOU shall for any reason and to any extent be deemed invalid or unenforceable, the remainder of this MOU and application of such provisions to other persons or circumstances shall remain valid and enforceable to the fullest extent of the law.

31. No Waiver. The failure of any party to enforce any provision of this MOU shall not be construed to be a waiver of the right of such a party thereafter to enforce such provisions.

32. Headings. Section headings are provided for organizational purposes only and do not in any manner affect the scope, meaning or intent of the provisions under the headings.

33. Notices. Except as may be otherwise required by law, any notice to be given shall be written and shall be either personally delivered, sent by facsimile transmission, or sent by first class mail, postage prepaid and addressed as follows:

DISTRICT:

Bishop Unified School District
Attn: Superintendent
301 N. Fowler Street,
Bishop, CA 93514
Telephone No.: (760) 872-3680
Fax No.: (760) 872-6016

NIH:

Northern Inyo Healthcare District
150 Pioneer Lane

Bishop, CA 93514
Telephone No. : (760) 873-5811
Fax No.: (760) 872-5800

Except as otherwise provided by law, any and all notices or other communications required or permitted by this MOU or by law to be served on or given to either Party by the other shall be in writing and shall be deemed duly served and given when personally delivered to any representative of the Party to whom they are directed, or in lieu of such personal service when deposited in the United States mail, first-class postage prepaid, addressed to the Party at the address set forth above. Either Party may change its address for purposes of this paragraph by giving written notice of such change to the other Party in the manner provided by this paragraph.

IN WITNESS WHEREOF, the Parties hereto have executed this MOU on the date last set forth below.

Executed: _____, 2023

BISHOP UNIFIED SCHOOL DISTRICT

By _____
Katherine Kolker
Superintendent

Executed: _____, 2023

NORTHERN INYO HEALTHCARE DISTRICT
dba Northern Inyo Hospital

By _____
Stephen DelRossi
CFO and Interim Chief Executive Officer

EXHIBIT A

Services to be provided by NIH to Eligible Students

The School-based health center will provide the following services:

1. Diagnosis and treatment of minor illness, injury and medical conditions

2. STD screening and treatment

3. Reproductive health related services

4. Health education for students and families

5. Coordinate care, including appropriate follow-up and referrals to health and social service providers on and off site

EXHIBIT B

Site Map

(to be attached)

EXHIBIT C

INSURANCE REQUIREMENTS

1. NIH Coverage. NIH shall, at its own cost and expense, secure promptly after the effective date of this MOU and the commencement of the MOU term, and maintain during the entire term of this MOU, the following insurance coverage from a California licensed, authorized and/or admitted insurer with an A minus (A-), VII, or better rating from A.M. Best acceptable to District, or a program of self-insurance acceptable to District, sufficient to cover any claims, damages, liabilities, costs, losses, liabilities and expenses (including counsel fees) arising out of or in connection with NIH's fulfillment of any of its obligations under this Agreement and/or use and occupation of the Health Center:

A. Broad Form Comprehensive General Liability and Hospital Professional Liability (medical malpractice) (GL/HPL) occurrence based coverage including both bodily injury and property damage caused by its acts, errors or omissions, with limits as follows: $5,000,000 per occurrence, $15,000,000 aggregate.

The general liability insurance policy shall include coverage for liabilities arising out of premises, operations, personal & advertising injury, and liability assumed under an insured contract.

B. Business Auto Liability insurance to cover bodily, injury, personal injury, and property damage for all owned, non-owned or hired automobiles with a $1,000,000 combined single limit. NIH's automobile liability policy shall include as an insured, anyone held liable for NIH's conduct to the extent of that liability.

C. Workers' Compensation and Employer's Liability insurance or a program of self-insurance covering NIH's full liability in accordance with California and federal laws, with statutory limits.

2. **NIH Endorsements.** Each comprehensive general liability, insurance policy required hereunder will be endorsed with wording to secure the following effects:

(a) The District, its officers, agents and employees, are named as additional insureds/coverage participants for all liability arising out of the operations by or on behalf of NIH in the performance of this MOU.

(b) The inclusion of more than one insured will not operate to impair the rights of one insured against another insured, and the coverage afforded will apply separately to each additional coverage participant; but the inclusion of more than one coverage participant will not operate to increase the limits of NIH's coverage.

(c) NIH coverage shall be primary to and not contributing with any other insurance maintained by the District but with respect to the acts, errors and omissions of NIH.

(d) NIH's insurance policy will not be canceled or materially changed without first giving 30 calendar days' prior written notice to the District.

3. NIH's Documentation. NIH will provide the District with the following documentation after the signing of this MOU:

(a) Properly executed certificates of coverage evidencing all coverages, limits, and endorsements required above in this MOU. This documentation will be submitted within 10 days after the effective date of this MOU and the commencement of its term.

4. NIH's Policy Obligations. NIH's indemnity and other obligations will not be limited by the foregoing insurance requirements.

5. NIH's Material Breach. If NIH, for any reason, fails to maintain insurance coverage which is required pursuant to this MOU, this failure is deemed to be a material breach of the MOU. In that event, the District at its sole option may immediately terminate this MOU.

6. District's Coverage. During the entire term of this MOU and any extension or modification thereof, District shall keep in effect a policy or policies of general liability and general automobile liability insurance, or a program of self-insurance, including coverage of owned and non-owned vehicles used to provide any service in connection with this MOU, of at least $1,000,000 combined single limit for all damages arising from each accident or occurrence and $3,000,000 excess umbrella liability coverage for all damages arising out of injury to or destruction of property for each accident or occurrence.

7. **District's Endorsements.** Each comprehensive general liability policy, or a program of self-insurance, required hereunder will be endorsed with language to secure the following effects:

(a) NIH, its officers, agents and employees, are named as additional insureds/coverage participants for all liability arising out of the operations by or on behalf of District in the performance of this MOU.

(b) The inclusion of more than one insured will not operate to impair the rights of one insured against another insured, and the coverage afforded will apply as though separate policies had been issued to each insured; but the inclusion of more than one insured will not operate to increase the limits of District's insurance company's liability.

(c) District's insurance policy will not be canceled or materially changed without first giving 30 calendar days' prior written notice to NIH.

8. **District's Documentation.** District will provide NIH with the following documentation after the signing of this Agreement:

(a) Properly executed certificates of coverage evidencing all coverages, limits, and endorsements required above in this MOU. This documentation will be submitted

within 10 days after the effective date of this MOU and the commencement of its term.

9. **District's Policy Obligations.**

(a) District's indemnity and other obligations will not be limited by the foregoing insurance requirements.

(b) The District can fulfill these insurance requirements through its customary insurance policies and programs, and need not purchase separate policies, as long as its customary insurance policies and programs provide coverage equivalent to the coverage required hereunder.

10. **District's Material Breach.** If District, for any reason, fails to maintain insurance coverage which is required pursuant to this MOU, this failure is deemed to be a material breach of the MOU. In that event, NIH at its sole option may immediately terminate this MOU.

NORTHERN INYO HOSPITAL
Northern Inyo Healthcare District
150 Pioneer Lane, Bishop, California 93514

Medical Staff Office
(760) 873-2174 voice
(760) 873-2130 fax

TO: NIHD Board of Directors
FROM: Sierra Bourne, MD, Chief of Medical Staff
DATE: August 8, 2023
RE: Medical Executive Committee Report

The Medical Executive Committee met on this date. Following careful review and consideration, the Committee agreed to recommend the following to the NIHD Board of Directors:

A. Policies (*action item*)
    1. *Medical Ethics Referrals and Consultation*
    2. *Medical Records Delinquency Policy*
    3. *Medical Staff History & Physical (H&P) Policy*

B. Medical Executive Committee Meeting Report (*information item*)

NORTHERN INYO HEALTHCARE DISTRICT
CLINICAL POLICY AND PROCEDURE

Title: Medical Ethics Referrals and Consultations		
Owner: MEDICAL STAFF DIRECTOR	Department: Medical Staff	
Scope: District Clinical Departments		
Date Last Modified: 06/14/2023	Last Review Date: No Review Date	Version: 3
Final Approval by: NIHD Board of Directors	Original Approval Date: 06/21/2018	

PURPOSE:
The purpose of this document is to outline the procedure for medical ethics referrals to the Northern Inyo Healthcare District (NIHD) Medical Executive Committee. The Medical Executive Committee will serve as a forum to promote and clarify medical ethics practices throughout NIHD in order to enhance the quality of patient care.

POLICY:
1. The Medical Executive Committee shall serve as the Medical Staff Ethics Committee.
2. The activities of the Medical Executive Committee in relation to ethics include:
    a. Consultation – Consult with hospital staff regarding difficult clinical ethics cases, making recommendations when appropriate.
    b. Education – Identify educational opportunities to educate committee members, the hospital, and the community on medical ethics issues.
    c. Policy work – Review and create hospital policies and procedures to promote medical ethics practice guidelines and decrease future ethics conflicts.
3. Other healthcare professionals or members of the community may be asked to participate in the committee's activities when appropriate, including, but not limited to:
    a. Social workers
    b. Clergy
    c. Legal counsel

PROCEDURE:
1. Consultation Procedure (Referrals) – Inpatient or Outpatient
    a. Requests for consultation may be initiated by the patient, family, attending physician, other health care providers, or any person having a significant relationship with the patient.
    b. Requests for consultation are directed to the Medical Staff Office, the Chief of Staff, Vice Chief of Staff, or designee to initiate the referral.
    c. The Chief of Staff, Vice Chief of Staff, or designee reviews the request for appropriateness and urgency. If the request is appropriate, the Medical Staff Office will either:
        i. Add the referral to the next regularly scheduled Medical Executive Committee agenda for discussion in closed session, or
        ii. Convene a special meeting of the Medical Executive Committee if urgent.
    d. The committee reviews the case and proceeds as follows:
        i. Discusses issues that initiated the consultation including medical, family, psychosocial, spiritual, legal and ethical dilemmas.
        ii. Clarifies options, including the ethical justification or rationale for each option.

iii. Selects appropriate options to recommend. In this step, any providers that are directly responsible for the care of the patient will recuse themselves from voting on the committee's recommendations.

e. The Medical Executive Committee communicates its recommendation to the appropriate involved parties, either verbally or in writing.
f. A summary statement is placed in the patient's medical record by the Chief of Staff, Vice Chief of Staff, appropriate Chief or designee.

REFERENCES:

1. Nelson, William A. and Elliot, Barbara A. (2012) *Critical Access Hospital Ethics Committee Resource Guide*. Trustees of Dartmouth College, Hanover, New Hampshire.

RECORD RETENTION AND DESTRUCTION:

1. Minutes of the Medical Ethics Committee are confidential and are to be kept by the Medical Staff Office as official Medical Staff records. Retention will follow the same guidelines as other Medical Staff Committees.

CROSS REFERENCED POLICIES AND PROCEDURES:

1. None

Supersedes: v.2 Medical Ethics Referrals and Consultations

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Medical Records Delinquency Policy		
Owner: MEDICAL STAFF DIRECTOR	Department: Medical Staff	
Scope: Medical Staff and Advanced Practice Providers (APPs)		
Date Last Modified: 07/20/2023	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 08/19/2021	

PURPOSE:
To ensure compliant documentation and signatures on clinical documents and orders for patient's medical records.

POLICY:
1. For hospital-based medical records:
    a. History and Physical (H&P) shall be completed within 24 hours after admission.
    b. Discharge summary shall be completed within 7 days after discharge.
    c. The patient's complete medical records including H&P, progress notes, discharge summary shall be completed within 14 days following discharge.
    d. Verbal or telephone orders need to be cosigned within 48 hours of order placement.
2. For clinic-based medical records:
    a. The patient's office visit note should be completed and signed at the time the office visit, or no later than 3 days following the visit.
    b. Verbal or telephone orders need to be cosigned within 48 hours of order placement.
3. For surgery-based medical records:
    a. For H&P requirements, refer to H&P Policy.
    b. An immediate postoperative note is required on all surgical patients.
    c. Complete operative reports shall be completed immediately after surgery or within 24 hours of surgery/operation.

PROCEDURE:
1. If documentation and/or signatures are delinquent, the Health Information Management (HIM) manager shall notify the Medical Staff member or Advanced Practice Provider (APP) by NIHD email and/or certified mail that his/her privileges to admit or attend to patients shall be suspended 7 days from the date of notice and that the Medical Staff member or APP shall remain suspended until records have been completed.
2. Ongoing care of patients already in the hospital may be continued. The suspended member shall not care for any patients other than those currently admitted under his/her own name and may not provide consults on Hospital or emergency room patients.
3. If the suspended member is on call, he/she is responsible for finding another physician to see any patients requiring care while he/she is on call.
4. Suspension of admitting privileges does not affect the Medical Staff or APP's privilege to provide patient care in emergency circumstances when the member is the only provider available to provide that necessary care.

5. Any member whose privileges have been suspended for failure to complete medical records in a timely fashion for a total of 30 (thirty) days or longer in a 12 (twelve) month period may be reported to the Medical Board of California by the Chief Executive Officer, pursuant to California Business and Professions Code section 805 and the National Practitioner Data Bank.
6. If the Medical Staff member or APP is unavailable for a prolonged period of time, that Medical Staff member or APP is able to designate a proxy of the same specialty to sign orders on their behalf.

REFERENCES:

1. California Code, Business and Professions Code – BPC 805
2. Title 22, California Code of Regulations, Section 70751
3. Title 22, California Code of Regulations, Section 74731
4. Title 22, California Code of Regulations, Section 70263

RECORD RETENTION AND DESTRUCTION:

1. As per the District's medical record retention and destruction policies.

CROSS REFERENCE POLICIES AND PROCEDURES:

1. Verbal and/or Phone Medical Staff Practitioner Orders
2. Medical Staff History and Physical (H&P) Policy
3. Northern Inyo Healthcare District Medical Staff Bylaws

Supersedes: v.1 Medical Records Delinquency Policy

NORTHERN INYO HEALTHCARE DISTRICT

CLINICAL POLICY

Title: Medical Staff History and Physical (H&P) Policy		
Owner: MEDICAL STAFF DIRECTOR	Department: Medical Staff	
Scope: Medical Staff and Advanced Practice Providers (APPs)		
Date Last Modified: 07/11/2023	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 08/19/2021	

PURPOSE:

To define the elements of a patient's history and physical (H&P) examination and medical history on admission or before any operative or interventional procedure.

POLICY:

1. An H&P examination must be performed by a qualified licensed practitioner who is credentialed and privileged by the medical staff to perform an H&P.
2. An H&P must consist of chief complaint, history of present illness, allergies and medications, relevant social and family history, past medical history, review of systems as needed and physical examination, and assessment and plan appropriate to the patient's age.
    a. For surgical procedures, the surgeon's documentation (H&P or consult note) should also include risks, benefits, and alternatives.
3. An H&P examination must be performed within twenty-four (24) hours after admission and prior to surgery or procedure requiring anesthesia services.
4. If a complete H&P examination was performed within thirty (30) calendar days before admission, an updated medical record entry must be completed and documented in the patient's medical record within twenty-four (24) hours after admission and prior to surgery or procedure requiring anesthesia services.
    a. The update note must document an examination for any changes in the patient's condition since the patient's H&P was performed that might be significant for the planned course of treatment. The physician or qualified licensed individual uses his/her clinical judgment, based upon his/her assessment of the patient's condition and comorbidities, if any, in relation to the patient's planned course of treatment to decide the extent of the update assessment needed as well as the information to be included in the update note in the patient's medical record.
    b. If, upon examination, the licensed practitioner finds no change in the patient's condition since the H&P was completed, he/she may indicate in the patient's medical record that the H&P was reviewed, the patient was examined, and that "no change" has occurred in the patient's condition since the H&P was completed (71 FR 68676).
5. If the practitioner finds that the H&P done before admission is older than thirty (30) days, incomplete, inaccurate, or otherwise unacceptable, the practitioner reviewing the H&P, examining the patient, and completing the update must document in the medical record a new or corrected H&P within twenty-four (24) hours after admission, but prior to surgery or a procedure requiring anesthesia.
6. If the H&P and the informed consent for the surgery or procedure are not recorded in the patient's medical record prior to surgery, the procedure shall not be performed unless the attending physician states in writing that such delay could lead to an adverse event or irreversible damage to the patient.

REFERENCES:

1. Centers for Medicare and Medicaid Condition of Participation: Medical Staff 482.22(c)(5)
2. "History and Physical." UCLA Health Medical Staff Policy. Effective Date 04/03/2017. Retrieved 01/25/2021. https://www.uclahealth.org/medical-staff/workfiles/policies-rrucla/MS%20200%20History%20and%20Physical%2004302017%20GH.pdf

RECORD RETENTION AND DESTRUCTION:

1. H&Ps are part of the patient's medical records and shall follow the District's record retention and destruction policies.

CROSS REFERENCE POLICIES AND PROCEDURES:

1. Informed Consent Policy - Practitioner's Responsibility

Supersedes: v.1 Medical Staff History and Physical (H&P) Policy

CALL TO ORDER	The meeting was called to order at 5:30 p.m. by Mary Mae Kilpatrick, Northern Inyo Healthcare District (NIHD) Board Chair.
PRESENT	Mary Mae Kilpatrick, Chair Melissa Best-Baker, Vice Chair Jean Turner, Secretary Ted Gardner, Treasurer Jody Veenker, Member-at-Large Stephen DelRossi, MSA, Interim Chief Executive Officer / Chief Financial Officer
PUBLIC COMMENTS ON CLOSED SESSION ITEMS	Chair Kilpatrick announced at this time, persons in the audience may speak only on items listed on the Closed Session portion of this meeting. She announced there is one case on item b. There were no public comments.
ADJOURNMENT TO CLOSED SESSION	At 5:30, Chair Kilpatrick announced the meeting would adjourn to Closed Session to allow the District Board of Directors to: a. Conference with Legal Counsel – Existing Litigation. Government Code 54956.9(d)(1). Name of case: Tillemans v. NIHD Chair Kilpatrick announced there would be no reportable action.
ADJOURNMENT	Adjournment at 6:14 p.m.

_____
Mary Mae Kilpatrick, Northern Inyo Healthcare District, Chair

Attest: _____
Jean Turner, Northern Inyo Healthcare District, Secretary

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Attendance At Meetings		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope: Board of Directors		
Date Last Modified: 08/08/2023	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 04/18/2018	

PURPOSE: Establish policy for Board of Directors (BOD) meeting attendance.

POLICY:

1. Directors are expected to the extent reasonable, to make good faith efforts to schedule vacation, business and personal commitments at time that with not conflict with the schedule of regular Board meetings.
2. It is recognized the timing of business and family commitments, since they involve addition people and outside factors, cannot always be controlled.

PROCEDURE:

1. Notwithstanding any other provision of law the term of any member of the BOD shall expire if they are absent from three consecutive regular Board meetings, or from three of any five consecutive meetings of the Board and the Board by resolution declares a vacancy exists.
2. As set forth in the Ralph M. Brown Act in CA Government Code Section 54953, a Director may attend a meeting by teleconference.

REFERENCES:

1. CA Health and Safety Code Section 32100.2
2. Ralph M. Brown Act in CA Government Code Section 54953

RECORD RETENTION AND DESTRUCTION:
Minutes from the Board of Director's meeting must be retained for six (6) years.

CROSS REFERENCED POLICIES AND PROCEDURES:
1. Attendance At Meetings
2. Attendance At Meetings
3. Attendance At Meetings

Supersedes: v.1 Attendance At Meetings

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: NIHD Board Meeting Minutes		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope: Board of Directors		
Date Last Modified: 12/01/2022	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 06/20/2018	

PURPOSE: Establish documentation policy for Northern Inyo Healthcare District (NIHD) Board of Directors (BOD) meeting minutes.

POLICY: Northern Inyo Healthcare District Board of Directors meeting minutes shall be kept in action format. The following information shall be included in each meeting's minutes:

- Date, place and type (regular or special) of meeting
- Directors and Chief Executive team members present and absent by name.
- Call to Order (including time)
- Names (if given) of public commentators, and topic commented on.
- If a Director arrives late or leaves early, the time and name shall be recorded.
- Names of Directors absent during any agenda item on which action was taken.
- BOD directives to staff.
- Motions or resolutions on which action was taken.
- Names of Directors making and seconding motions.
- Public comments made by BOD members.
- Topics included in closed session.
- Announcement by BOD President stating what action, if any, was taken during closed session.
- Time of adjournment.

PROCEDURE:

1. The clerk of the BOD shall prepare and keep minutes of all regular and special BOD meetings.
2. The draft minutes of the previous regular BOD meeting and any special meeting(s) of the BOD held since the previous regular meeting shall be distributed to Directors as part of the information packet for the next regular BOD meeting at which time the BOD shall consider approving the minutes as presented or with corrections.
3. Unapproved minutes are "preliminary drafts that are not retained by the public agency in the ordinary course of business." (CA Government Code Section 6254). Therefore, draft minutes shall not be released until the BOD has approved them.
4. Once approved by the BOD the minutes shall be posted on the District website and maintained in the District's official files.
5. After approval, the Secretary of the BOD shall sign the minutes.
6. Motions and resolutions of regular and special BOD meetings shall be recorded as having passed or failed. Individual votes for and against and abstentions shall be recorded unless the action was unanimous.

7. All resolutions adopted by the BOD shall be numbered consecutively, starting new numbering at the beginning of each calendar year.

REFERENCES:

1. (CA Government Code Section 6254) Public Records Act

RECORD RETENTION AND DESTRUCTION:

CROSS REFERENCED POLICIES AND PROCEDURES:

Supersedes: v.1 NIHD Board Meeting Minutes

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Northern Inyo Healthcare District Board of Directors Meetings		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope:		
Date Last Modified: 12/01/2022	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 06/20/2018	

PURPOSE: Establish procedures for Northern Inyo Healthcare District (NIHD) Board of Directors' (BOD) meetings.

POLICY:

1. All meetings of the NIHD BOD shall be conducted in accordance with the Ralph Brown Act, Government Code 54950 et seq. and such additional requirements as set forth in any other BOD Policy and Procedures.

PROCEDURE:

1. Meetings of the BOD shall be held at the NIHD Board Room located at 2957 Birch St. Bishop CA 93514 except as otherwise set forth in agenda notices.
2. Regular meetings shall be held the third Wednesday of each calendar month unless it is deemed necessary to cancel or hold the regular monthly meeting on a different date.
3. As the BOD encourages public participation at its meetings (whether regular, special, study sessions, or emergency) and to facilitate communications, the BOD will ensure agendas are posted in the required timeframe on the NIHD website in addition to other legal requirements. The place, date and time of the meeting shall be indicated on the agenda.
4. Each agenda shall include a time for public comment on non-agenda items as well as comment opportunity on each action agenda item when called.
5. If any Director is attending the meeting by teleconference, the location shall be posted and accessible to the public.
6. The President of the NIHD BOD shall preside at all board meetings at which they are present. In absence of the President, the Vice President shall perform the President's duties and have the President's rights. If both the President and Vice President are absent then the Secretary shall perform the President's duties and have the President's rights.
7. The President shall call the meeting to order at the time set on the agenda or as soon as a quorum is present.
8. A majority (3 of 5 members) shall constitute a quorum for transaction of business. An abstention does not count as a vote for or against.
9. If no directors are present the clerk of the board shall adjourn the meeting to a future date and time. A notice of the adjournment including the future date and time of the adjourned meeting shall be conspicuously posted on or near the door of the place where the meeting was held.
10. If the date of the adjourned meeting is within five (5) days of the original meeting, no new agenda need be posted if no additional agenda items are added. If the date of the adjourned meeting is more than five (5) days a new agenda must be posted.

11. The President of the BOD, as necessary to conduct business of the District, can call special meetings or study sessions.
12. Ordinarily, items on the agenda will be considered in the order set forth in the agenda. However, the President may alter the order of items on the agenda, as the President deems necessary for the good of the meeting.
13. The President may declare a short recess during any meeting.
14. The President shall have the same rights as the other Board members in voting, introducing or seconding motions and resolutions as well as participating in discussions.
15. No action may be taken by secret ballot. (Government Code Section 54953(c).)
16. All votes taken during a teleconferenced meeting shall be by roll call. (Government Code Section 54953(b)(2).)
17. Directors shall observe all applicable conflict of interest rules. If a financial interest is determined by any board member they must abstain from any vote that may be in violation of Government Code 1090. The director shall leave the meeting room during any discussion and the vote and shall state the reason for abstention.
18. The annual organizational meeting shall be the regular BOD meeting held in December or at an earlier meeting if called. At that meeting officers shall be elected.5

REFERENCES:

1. Ralph Brown Act, Government Code 54950 et seq.
2. Government Code Section 54953(c)
3. Government Code Section 54953(b)(2)
4. Government Code 1090

RECORD RETENTION AND DESTRUCTION:

CROSS REFERENCED POLICIES AND PROCEDURES:

Supersedes: v.1 Northern Inyo Healthcare District Board of Directors Meetings

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Officers and Committees of the Board of Directors		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope: Board of Directors		
Date Last Modified: 12/01/2022	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 05/16/2018	

PURPOSE: Describe the District officers and Board Committees and their duties.

POLICY:

1. The officers of the Northern Inyo Healthcare District (NIHD) Board of Directors (BOD shall be a President, Vice President, Secretary, Treasurer, and Member at Large.
2. The Board of Directors may sit as a Committee of the Whole or as Task Force Committees as deemed appropriate.
3. The President of the Board shall appoint such Ad Hoc committees as may be deemed necessary or advisable by the President or by the BOD. The duties of an Ad Hoc committee shall be outlined at the time of appointment, and the committee shall be deemed dissolved when its final report has been made.
4. As provided in the BOD By-Laws, no committee so appointed shall have any power or authority to commit the BOD or the District in any manner unless the BOD directs the committee to act for and on its behalf by special vote.

PROCEDURE:

1. The Board of Directors at the December meeting of every calendar year shall choose the officers of the Board every year. Each officer shall hold office for one year or until a successor shall be elected and qualified or until the officer is otherwise disqualified to serve.
2. Any officer of the BOD may resign or be removed as a Board officer by the majority vote of the other Directors then in office at any regular or special meeting of the BOD. In the event of resignation or removal of an officer the BOD shall elect a successor to serve for the balance of that officer's unexpired term.
3. The **President** shall conduct the meetings of the BOD and shall act as the lead liaison between the BOD and District Management for communications and oversight in fulfilling the District's Mission, Vision and Values. The President shall have, subject to the advice and control of the BOD, general responsibility of the affairs of the District and shall discharge all other duties that shall be required of the President by the By-Laws of the BOD.
4. The **Vice President** shall in the event of absence or inability of the President, exercise all the powers and perform all the duties given to the President by the By-Laws of the District.
5. The **Secretary** shall act in this capacity for both the District and the BOD. In the absence or inability of the President and Vice President shall exercise all powers and perform all duties given to the President. Shall be responsible for seeing that all actions, proceedings and minutes of the meetings of the BOD are properly kept and are maintained at District Administrative offices. Shall perform such other duties as pertains to the office and as prescribed by the BOD and By-Laws of the BOD. The Secretary may delegate his/her duties to appropriate management personnel.

6. The **Treasurer** shall be responsible for the safekeeping and disbursal of the funds of the District in accordance with the provisions of the "Local Healthcare District Law: and in accordance with resolutions, procedures and directions as the BOD may adopt. Shall perform such other duties as pertains to the office and as prescribed by the BOD and By-Laws of the BOD. The Treasurer may delegate his/her duties to appropriate management personnel.
7. The **Member at Large** shall have all the powers and duties of the Secretary in the absence of the Secretary, and shall perform such other duties as may from time to time be prescribed by the BOD and By-Laws of the BOD.
8. The duties of the **committees** shall be to develop and make policy recommendations to the BOD and to perform such other functions as shall be stated in the BOD By-Laws or in the resolution or motion creating the committee. The President with the approval of the BOD may appoint special or Ad Hoc committees as special circumstances warrant. Composition of the committee may consist of only Board members or they may include individuals not on the Board.

REFERENCES:

1. Northern Inyo Healthcare District Board of Directors By-Laws

RECORD RETENTION AND DESTRUCTION:

CROSS REFERENCED POLICIES AND PROCEDURES:

Supersedes: v.1 Officers and Committees of the Board of Directors

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Requests for Public Funds, Community Grants, Sponsorships		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope: Board of Directors		
Date Last Modified: 01/18/2023	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 05/16/2018	

PURPOSE: Establish criteria for granting requests for Public Funds, Community Grants, and Sponsorships. A community's health needs are served not only by traditional acute care hospitals, but also by a broad array of other health-related programs and initiatives. These include local health and wellness programs, community based clinics, health provider educational programs, and other programs and organizations that promote physical health, emotional health, and behavioral health well-being.

POLICY:

As allowed by Northern Inyo Health Care District's (NIHD) financial condition and the law, the District may provide assistance to Healthcare programs, services, facilities and activities at any location within or without the NIHD for benefit of the District and the people served by the District.

PROCEDURE:

1. When considering funding a request, NIHD shall address identified community healthcare needs as envisioned by the Mission and Vision Statements and the strategic plan.
2. Within the limits of the budget and the law, sponsorship of events of qualified programs is allowed. NIHD staff will administer sponsorship requests.
3. In conjunction with setting the annual budget each year, the District shall determine whether to fund any requests for Community Grants and if so, what amount. NIHD staff shall administer the Community Grants program with the Directors making the final decision regarding grant recipients.
4. Information regarding the availability of the Community Grants and the application process shall be posted on the NIHD website and publicized appropriately so eligible programs may make timely applications.

REFERENCES:

1. California Health and Safety Code Sections 32121(j) and 32126.5.

RECORD RETENTION AND DESTRUCTION:

CROSS-REFERENCE POLICIES AND PROCEDURES:

Supersedes: v.1 Requests for Public Funds, Community Grants, Sponsorships

NORTHERN INYO HEALTHCARE DISTRICT
NON-CLINICAL POLICY AND PROCEDURE

Title: Use by NIHD Directors of District Email Accounts		
Owner: Board Clerk and CFO Assistant	Department: Board of Directors	
Scope: Board of Directors		
Date Last Modified: 08/08/2023	Last Review Date: No Review Date	Version: 2
Final Approval by: NIHD Board of Directors	Original Approval Date: 05/16/2018	

PURPOSE: Establish policy and procedure for appropriate use of the District's official email accounts by Northern Inyo Healthcare District (NIHD) Board of Directors (BOD)

POLICY:

1. The District shall issue an official email address, using the District's domain name for all Directors.
2. The District shall provide technical support to enable Directors to access their official email accounts from mobile devices and home computers.
3. No Director shall conduct District business on any email account other than the official District email account.
4. Director's emails pertaining to District business shall not be deleted during the Director's term of office.
5. Non-District related emails may be deleted at the Directors discretion.
6. All emails related to District business are understood to be a part of the public record.

PROCEDURE:

1. Communications from District staff to Directors regarding District business shall utilize the Directors official email accounts. A Director may not request, such communications be sent to a different email account.
2. Directors are required to use their official email for District-related communications. Email communications on a Director's personal or business account that relate to District business are subject to disclosure under the Public Records Act. Directors who knowingly or inadvertently use a personal or other business account shall make their personal and/or business email account available for review by the District's legal counsel when necessary to comply with a request under the Public Records Act.
3. The Director shall not delete any District Board related emails until such time as approved copies have been saved and stored in the District IT system.
4. In order to avoid inadvertent violations of the Brown Act, Directors and staff shall exercise caution when using the "reply all" email function. Directors may not communicate with more than one other Director including via email, except for trivial or scheduling matters. It is to be understood that comments or questions in a "reply all" response may constitute a serial meeting under the Brown Act.

REFERENCES:

1. Public Records Act
2. Ralph M. Brown Act

RECORD RETENTION AND DESTRUCTION:

CROSS-REFERENCE POLICIES AND PROCEDURES:

Supersedes: v.1 Use by NIHD Directors of District Email Accounts