HEALTHWEST

PROGRAM/PERSONNEL MEETING MINUTES

October 13, 2023
8:00 a.m.

376 E. Apple Ave.
Muskegon, MI 49442

CALL TO ORDER

The regular meeting of the Program/Personnel Committee was called to order by Chair Natte at 8:03 a.m.

ROLL CALL

Members Present:	Cheryl Natte, Janet Thomas, Tamara Madison, Thomas Hardy
Members Absent:	Janice Hilleary
Staff Present:	Gina Post, Shannon Morgan, Cyndi Blair, Amber Berndt, Rich Francisco, Linda Wagner, Christy LaDronka, Heather Wiegand, Brian Speer, Gary Ridley, Randi Bennett, Mike Kimble, Chelsea Kirksey, Pam Kimble, Melina Barrett
Guests Present:	Kristen Wade, John Weerstra

MINUTES

It was moved by Mr. Hardy, seconded by Ms. Madison, to approve the minutes of the August 11, 2023 meeting as written.

MOTION CARRIED.

PUBLIC COMMENT (ON AN AGENDA ITEM)

There was no public comment.

ITEMS FOR CONSIDERATION

It was moved by Ms. Thomas, seconded by Mr. Hardy, to authorize the policy and procedural changes as described above and attached, effective October 27, 2023.

MOTION CARRIED.

It was moved by Mr. Hardy, seconded by Ms. Thomas, to authorize the policy and procedural changes as described above and attached, effective October 27, 2023.

MOTION CARRIED.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATION

Heather Wiegand, Clinical Service Manager of Correctional Services, provided her Crisis Intervention Training presentation. Christy LaDronka, Access Service Manager, provided her Behavioral Health Alternative Response presentation.

DIRECTOR'S COMMENTS

Executive Director, Rich Francisco, provided an update. HealthWest is participating in the soft launch of MichiCANS, MDHHS has determined that they will be replacing the CAFAS and PECFAS, two assessments previously selected for our child population. HW agreed to do the soft launch, but the scope of testing MichiCANS has changed. MDHHS released a memo that they now want the soft launch sites to conduct the MichiCANS on the foster kid population as well. At the Director's forum about 2 weeks ago on the 29th, the CEOs and directors first learned of this, and there were many pushing back because of the additional scope that was added. MDHHS has since relaxed their stance and is offering more opportunities to work this out. We have now had several meetings with CMHA and developing a stance that if the soft launch sites will continue to do this, that it would have to have certain conditions. We were told during a meeting with MDHHS, Phil Kurdowicz that his instructions came from high above. Some of the concerns brought by CMHSPs are financing, administrative burden, staffing issues, coordination details. KATA and quality improvement, HW has completed another training for KATA, and trained more managers and supervisors this past Monday. Again today, there will be another training with about 17 more staff added to the list. Our QI director, Pam Kimble has taken on doing the training now and has received more requests to do these kata project initiatives.

AUDIENCE PARTICIPATION

There was no audience participation.

ADJOURNMENT

There being no further business to come before the board, the meeting adjourned at 8:48 a.m.

Respectfully,

Cheryl Natte
Program/Personnel Committee Chair

CN/hb

PRELIMINARY MINUTES
To be approved at the Program/Personnel Committee Meeting on December 1, 2023

HealthWest
Muskegon's Behavioral Wellness Connection

PROGRAM AND PERSONNEL COMMITTEE

Friday, October 13, 2023
8:00 a.m.

376 E. Apple Ave., Muskegon, MI 49442

Program and Personnel Committee Chair: Cheryl Natte
Program and Personnel Committee Vice-Chair: Janice Hilleary

AGENDA

1)	Call to Order	Action
2)	Approval of Agenda	Action
3)	Approval of the Minutes of August 11, 2023 (Attachment #1 – pg. 1-2)	Action
4)	Public Comment (on an agenda item)	
5)	Items for Consideration	
	A) Authorization to approve the HealthWest Policy and Procedural Changes to Policy 10-003 Contracting with New Service Providers, Compliance and Site Reviews (Attachment #2 – pg. 3-24)	Action
	B) Authorization to approve the HealthWest Policy and Procedural Changes to Policy 05-026 Information System Use (Attachment #3 – pg.25-66)	Action
6)	Old Business	
7)	New Business	
8)	Communication / Director's Report	
	A) Crisis intervention Training Overview – Heather Wiegand	Information
	B) Behavioral Health Alternative Response – Christy LaDronka	Information
	C) Director's Update – Rich Francisco	Information
9)	Audience Participation / Public Comment	
10)	Adjournment	Action

/hb

HEALTHWEST

PROGRAM/PERSONNEL MEETING MINUTES

August 11, 2023
8:00 a.m.

376 E. Apple Ave.
Muskegon, MI 49442

CALL TO ORDER

The regular meeting of the Program/Personnel Committee was called to order by Chair Natte at 8:00 a.m.

ROLL CALL

Members Present:	Cheryl Natte, Janet Thomas, Janice Hilleary, Tamara Madison, Thomas Hardy
Members Absent:	Stephanie Umlor, Kassandra Kitchen
Staff Present:	Holly Brink, Tasha Percy, Shannon Morgan, Cyndi Blair, Amber Berndt, Melina Barrett, Rich Francisco, Linda Wagner, Suzanne Beckeman, Gordon Peterman, Justine Belvitch, Justine Tufts, Urbain Ndoye, Kristina Baas
Guests Present:	Kristen Wade, John Weerstra

MINUTES

It was moved by Ms. Thomas, seconded by Mr. Hardy, to approve the minutes of the June 9, 2023 meeting as written.

MOTION CARRIED.

PUBLIC COMMENT (ON AN AGENDA ITEM)

There was no public comment.

ITEMS FOR CONSIDERATION

There was no items for consideration.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATION

Kristina Baas, Quality Improvement Project Manager, provided the Staff Satisfaction Survey Results.

DIRECTOR'S COMMENTS

Executive Director, Rich Francisco, gave an update. He is working on program updates and putting a structure to the Quality Improvement team. Mr. Francisco completed a KATA training session recently. This was essentially a "Train the Trainers" session, to continue training within the agency and working towards improvement. We have a few projects ahead of us already and beginning planning sessions for those. Mr. Francisco shared that the LRE site review is scheduled for September 12th – 14th. Mr. Francisco did share that he would like to bring a group of Directors to Full Board to present their programs and where they are at with them. At this time there are no significant changes planned for the organizational structure of HealthWest.

AUDIENCE PARTICIPATION

Mr. John Weerstra from the community introduced himself and provided his background and knowledge of community mental health. Mr. Weerstra also said that we can expect to see him in attendance regularly.

ADJOURNMENT

There being no further business to come before the board, the meeting adjourned at 8:25 a.m.

Respectfully,

Cheryl Natte
Program/Personnel Committee Chair

CN/hb

PRELIMINARY MINUTES
To be approved at the Program/Personnel Committee Meeting on October 13, 2023

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE	BUDGETED	NON-BUDGETED	PARTIALLY BUDGETED
Program/Personnel Committee	X		

REQUESTING DIVISION	REQUEST DATE	REQUESTOR SIGNATURE
Administration	October 13, 2023	Brandy Carlson, Chief Financial Officer

SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)

HealthWest Board authorization is requested to make the below and attached policy and procedural changes to the agency's Contracting with New Service Providers, Compliance, and Site Reviews as redlined in the attached document.

Changes Include:

1. Subject Line: Revised to "Contracting with New Service Providers, Compliance, and Site Reviews".
2. Section I Policy: Added Policy section.
3. Section II Purpose: Expanded on the purpose of the policy.
4. Section III Application: Added language to reflect current process.
5. Section IV Definitions: Updated language regarding application process, monitoring, and added open panel definition.
6. Section V Procedures: Defining and updating the process as a new provider is identified, updated Flow chart, and added Request for New Provider Services form (both included).
7. Section VI Review Process: Updated language to reflect current process.
8. Section VII Attachments: Updated the attachment list.
9. Section VIII References: Updated the reference list.

SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)

I move the HealthWest Board of Directors to authorize the policy and procedural changes as described above and attached, effective October 1, 2023.

COMMITTEE DATE	COMMITTEE APPROVAL
10/13/2023	_____ Yes _____ No _____ Other
BOARD DATE	**BOARD APPROVAL**
10/27/2023	_____ Yes _____ No _____ Other

DRAFT

HEALTHWEST

Policy and Procedure

No. 10-003

Prepared by:

Effective Date: October 1, 2005
Revised Date: August 17, 2023 ~~March 14, 2018~~

Jackie Farrar~~, Judith E. Cohen, Network Manager~~
Manager of Procurement and Provider Network

Commented [J1]: Should my name be here?

Commented [JC2R1]: Yes

Approved by:

Subject: Contracting with New Service Providers, Compliance, and Site Reviews ~~Contracted Provider Application and Compliance Review~~

Rich Franci~~e~~sco~~Julia B. Rupp~~, Executive Director

I. POLICY~~URPOSE~~

HealthWest will ensure there is a process in place for contracting with new providers of necessary/required services. These service providers may be in-network or out-of-network as necessary to meet the required provision of services for HealthWest consumers. HealthWest staff will also ~~To~~ en~~as~~sure initial and ongoing compliance with standards of care.

II. PURPOSE

This policy will describe the process for contracting with new service providers for both in-network and out-of-network, as HealthWest maintains an open panel for contracting agencies. HealthWest prefers to contract with accredited agencies. Contracts for services with non-accredited or single entities will be considered only if they are able to meet established eligibility criteria, or if services are of a highly specialized nature for which there is a limited provider pool listed in the application.

II. APPLICATION

Applies to Contracted Vendors/Providers of mental health services and substance abuse services for adults or children with mental illness, developmental disabilities and/or substance abuse.

Also applies to all HealthWest staff and services for its consumers.

~~Network Management Staff, other Designated Reviewer(s), Quality Improvement, Environment of Care Committee, and other Quality Improvement Committees.~~

III. DEFINITIONS

Completed Network Application: Documents sent out and collected by the Lakeshore Regional Entity (LRE) and/or HealthWest Contract Staff comprise the **Provider Application** ~~**Pack**~~**Packet**. It~~et~~ is reviewed by the LRE and HealthWest Contract Staff ~~Specialist~~ to~~and determined~~ ensure it ~~to~~ contains all required and completed documents.

Designated Reviewer: The HealthWest Contract ~~Specialist~~ Staff and/or the LRE Credentialing Staff assigned to the Provider or their designee.
Open Panel: Accepting new contract providers as needed/requested by HealthWest consumers and/or internal HealthWest staff as an agency of choice. Providers may contract with HealthWest at any time if they meet the requirements of the Standard Common Contract for the Lakeshore Regional Entity (LRE) of Region 3 in the State of Michigan.

A panel may be closed to new providers if accessibility to the requested service(s) is less than eighty-five percent (85%) capacity. When capacity for a service has been reached, a Request For Proposal (RFP) or a Request For Information (RFI) for any qualified new providers may be posted through the County of Muskegon Procurement Department to expand the capacity of the specific service(s) needed.

Commented [J3]: Brandy might be changing titles? What is your thought on Contract Department?

Commented [B4R3]: Still not sure on this name. We will work through this prior to approving the policy.

Commented [JC5R3]: Okay

IV. PROCEDURES

A. New Provider is identified.

1. Agency contacts HealthWest to request a contract be initiated, or a HealthWest staff person identifies the need for a new Provider of Service(s). The Requestor of the new or expanded requested service(s) will complete a HealthWest Request for New Service Provider Form (#A259—) and have it signed by their Program Supervisor.~~Provider Network~~~~Special~~

2. The Program Supervisor will forward this Request Form to the Manager of Procurement and Provider Network who will schedule a meeting of appropriate leadership team members to review the request. Following their discussion and group approval to move forward with procurement, the request must be approved via signatures by the Manager of Procurement and Provider Network, the Chief Financial Officer, and the Executive Director. A Board Motion is submitted to the HealthWest Board of Directors for approval to go forward with the procurement process. A HealthWest Contract Staff will be assigned to execute a contract following the procedures outlined in this Policy/Procedure.

3. There will be times when an urgent/emergent placement of a consumer is required either same day or within a few days. For those occasions, there may not be time to complete the paperwork necessary to present a motion to the Board of Directors and complete the credentialing processes within the short time frame. Staff will contact all known providers to see if any provider is willing and appropriately trained to take our consumer immediately; this would be considered a sole source procured provider. HealthWest Staff will review documentation that the Provider's staff is trained to manage the special needs of the specific consumer and a site review visit must occur prior to the placement.

Commented [J6]: I can't wait to see this form

Commented [B7R6]: When will we have this? Who is working on it?

Commented [JC8R6]: Beats me!

For those emergent/urgent placement situations, it will be necessary to have the Provider sign a Single Case Agreement for up to forty-five (45) days at which time the HW Contract Staff will have presented a board motion, have the LRE credential the Provider (if not already in our system), and have a signed contract with the provider completed. If there are extenuating circumstances, a continuation Single Case Agreement may be necessary.

Should this Provider not be willing to continue the placement beyond the forty-five (45- days, a thirty (30)-day notice is required from the Provider to HealthWest Staff. HealthWest Staff will need to seek another appropriate placement right away.

B. Following the procurement process for new Provider(s) selection, ~~ist~~the assigned HealthWest Contract ~~Manager~~Staff~~Specialist~~ will check within the LRE Credentialing SharePoint system for information on the selected Provider(s) already received by another CMHSP in the region. If present in the LRE SharePoint system, the documentation will be downloaded into the Provider file in the Current Contracts section of the Contracts Department. Any other additional information from the Provider as applicable shall be requested, including HealthWest specific forms. If the Provider is not located in the LRE SharePoint, the HealthWest Contract ~~Manager~~~~Specialist~~Staff verifies the Provider is not pending with the LRE Credentialing Committee by contacting the LRE Credentialing Staff.

C~~A~~. Application

1. ~~1.~~ All New Providers are ~~will be~~ required to complete a LRE Provider Application Packet ~~each year~~ prior to the issuing of a contract unless there is a current one already on file with the LRE.~~.~~

2. LRE Credentialing will send out the Application Packet for all agency providers and complete their credentialing process. For Licensed Independent Practitioners (LIP), the HealthWest Contract Staff will send out the Provider Application Packet with instructions to return to HealthWest. LRE Credentialing Staff will be sent a copy of the LIP's credentialing packet for their records in case another Region 3 CMHSP is interested in the same provider service(s).

~~2~~3. All Provider Applications for contracted services will be surveyed for compliance through a site review completed by the Lakeshore Regional Entity if within Region 3 or~~or~~ by a HealthWest Contract ~~Specialist~~Staff if out of Region 3. Another alternative is to contact the Provider's "home" CMHSP for a copy of their Provider site review and any other information they may wish to share regarding the Provider.

D~~B~~. Preparation for Monitoring Process

Commented [J9]: Add information from attachment D

1. ~~The~~ Contract ~~Specialist~~Staff will forward the Application Packet to the LRE Credentialing Staff and will complete a review of the ~~Provider Application~~ Packet

submitted by the Provider.

2. Upon receipt of the Provider Application Packet, the Contract ~~Specialist~~Staff will verify the packet is complete, and follow-up with the Provider to acquire missing content and proof documents.

3. ~~The~~ Contract ~~Specialist~~Staff will correct or add to the Application Packet any information sent or otherwise verified by the Provider~~.~~. Information acquired by telephone will not be acceptable verification for license, insurance, accreditation, financial solvency, conflict of interest, and/or rate for service.

4. When the Provider Application Packet is complete, ~~the Contract Specialist will inform the~~ the LRE will~~to~~ initiate a site review or obtain a review from another CMHSP who is already contracting with the ~~p~~Provider. ~~Should HealthWest intend to contract with the provider to perform administrative functions, the Contract Specialist will assess the provider's capacity to perform those functions prior to contracting with the provider.~~

5. ~~The~~ Designated Credentialing Reviewer (LRE Staff or HW Staff) will document all full compliance categories. All non-compliance or partial compliance must be documented on the Site Review Forms with sufficient information to permit follow-up. Only when the Provider is in full compliance with HealthWest and LRE standards will a contract be issued to the Provider.

6. Once the Provider is in full compliance, the Site Review Forms will be filed in the Compliance Review section of the Provider's HealthWest contract ~~in LaserFiche~~ file and/or stored on SharePoint.~~.~~

7. Requests for Plans of Correction must be written by the Designated Reviewer, and copies sent to the LRE/Contract ~~Specialist~~Staff to be filed in SharePoint/~~the~~ contract file. The Provider responses must also be filed in SharePoint/~~the~~ contract file.

Commented [J10]: We are not currently notified when a CAP has happened - we need to look in share point

8. ~~The~~ LRE Designated Reviewer~~r~~ and/or HealthWest Contract Staff will monitor all corrective action plans and conduct follow-up site reviews as necessary to assure full compliance; copies of all reports will be forwarded to the LRE/HealthWest Contract ~~Specialist~~Staff upon completion.

9. ~~The~~ LRE Designated Reviewer ~~the~~ and/or HealthWest Contract Staff must verify and document all corrective actions.

V. REVIEW PROCESS

~~A.~~ Accreditation (Copy of Accreditation Letter/Certificate Must be Included in Returned Packet)

1. ~~The~~ HealthWest Contract Staff~~LRE Designated Reviewer~~ must review all

accreditation documents. If accredited without a plan of correction, ~~the Designated Reviewer~~ Contract Staff will document the date he/she has verified full compliance on the Provider Application Review Form~~Site Review Form~~.

2. If the Provider is non-accredited, ~~the~~ Contract Staff~~Designated Reviewer~~ will document N/A on the Provider ~~Sit~~Application~~e~~ Review Form.

3. If the Provider is required to complete corrective actions by the accrediting body, ~~the~~ Contract Staff~~Designated Reviewer~~ will document such and the need for follow-up on the Provider ~~Site~~Application Review Form.

B. Conflict of Interest (Conflict of Interest Compliance Certificate Form completed and signed)

1. Upon review, if a conflict of interest is not identified or is identified but corrective actions are sufficient to remediate the conflict, ~~the~~ HealthWest Contract ~~Specialist~~Staff will document full compliance (Provider Application Review Form). ~~The~~ Contract ~~Specialist~~Staff may seek Corporate Counsel opinion.

2. ~~2.~~ If a conflict of interest is identified, ~~the~~ Contract ~~Specialist~~Staff must submit a copy of the forms to the Executive Director. ~~The~~ Executive Director/designee will schedule Corporate Counsel review and assure Corporate Counsel recommendations are ~~completed~~ implemented and documented. ~~and documented. The~~ Executive Director will notify the Contract ~~Specialist~~Staff when full compliance can be documented.

C. Insurance (Insurance Requirement Form)

1. If ~~type~~the type, amount, and coverage dates of insurance meet Agency requirements, ~~the~~ HealthWest Contract ~~Specialist~~Staff will contact the Provider for the appropriate Insurance certificate. Coverage dates meet~~is in~~ compliance if they~~it~~ cover~~s~~ the first day of the contract. A separate monitoring process is in place to identify coverage which expires during the contract year.

2. If type, amount, or coverage date(s) do not comply with Agency requirements, ~~the~~ Contract ~~Specialist~~Staff must initiate and document immediate follow-up with the Provider until full compliance can be documented and the contract initiated.~~.~~

D. Financial Solvency (Contractor Fiscal Certification Form, W-9 Form, and Audits completed and signed)

1. The most current ~~F~~financial forms/audit reports will be forwarded to the HealthWest Chief Financial Officer for review and approval once received by the Contract Staff.~~.~~

2. ~~2.~~ Financial forms/audit reports approved by the HealthWest Chief Financial Officer will be noted and documented as "in compliance". Formal audits returned by the ~~HealthWest~~ Chief Financial Officer with questions or recommendations will be considered non-compliant and will be followed-up by the HealthWest Contract ~~Specialist~~Staff until full compliance in this area can be verified and the

Commented [J11]: Should verbiage be added that HealthWest needs to be added to the policy?

Commented [B12]: When do we determine to put "HealthWest" before a job title or not. I am thinking just the first time in a section but could be wrong.

Commented [JC13R12]: Okay with me.

contract initiated.~~-~~

E. Disclosure of Ownership and Controlling Interest Statement (Completed and signed)
This form must be completed in its entirety for any individual in the Provider's organization with an ownership or controlling interest, including anyone with direct or indirect ownership of 5% or more, board members, or any managing employee such as general managers, business managers, administrators, and directors. This form is requested for new contracts, renewals, and when a provider has changes. LRE is the holder of this completed form.

~~E~~F. Provider Facility or Other License (Copies of all Licenses, Registrations, etc., included.)

~~The~~ HealthWest Contract ~~Specialist~~Staff will source-verify that the date of the license(s) cover(s) from the beginning contract date and will verify absence of sanctions or corrective action requirements.~~-~~ Licenses which expire during the contract year will be monitored by a separate monitoring process.

~~F~~G. Policies and Procedures and Guidelines

Each policy must be separately monitored, including each ~~e~~Environment of C~~c~~are policy.

1. ~~1.~~ All required HealthWest policies formally adopted by the Provider will be reported as in full compliance only when the ~~Designated Reviewer~~ Contract Staff and/or LRE staff has verified through~~at~~ the site review process that the Provider has evidence of procedures or processes in place for the policies.

2. ~~The~~ HealthWest Contract ~~Specialist~~Staff will request or review on-site the non-HealthWest policies which are included in the Provider Application Packet. The policies will be forwarded to the appropriate HealthWest staff member for formal approval or recommendations (e.g., Quality Improvement policy will be sent to HealthWest Quality Improvement Supervisor/Manager for review.)~~.~~ ~~The~~ Contract ~~Specialist~~Staff is responsible for tracking the flow of each document, follow-up, and documentation of any recommended changes, and final documentation of full compliance.~~-~~ (Attachment~~t A~~: Contract Provider Policy/Procedure Review and Approval Form) ~~-~~ ~~The~~ LRE Designated Reviewer will also review all required policies at their on-site review.

Commented [J14]: Provider Packet?

~~G~~H. Delegation of Administrative Functions (See Form in Contract Packet

~~The p~~Provisions of the Balanced Budget Act (BBA) of 1997 allow for delegation of administrative functions through contracts between the PIHP and HealthWest, and ~~the~~ HealthWest and Providers.~~-~~ ~~Administrative functions delegated to the Provider will be specified in the HealthWest/Provider contract. Providers will be assessed for capacity to perform delegated functions prior to contracting with the Provider. HealthWest will monitor the Provider for the performance of delegated functions as part of the contract monitoring process. HealthWest may revoke delegated functions in the event of non-compliance in the performance of those functions.~~For the purpose of HealthWest Provider contracts, HealthWest will not delegate Administrative Functions.

I. New Hire Employee Verification Form (For Substance Use Disorder (SUD) Treatment Staff Only)

Every SUD treatment staff member of the New Contracted Provider providing direct service must complete this form and ensure the staff's Supervisor and Program Director sign at the bottom of the last page. All forms must be returned with the LRE Application packet.

~~H~~J. Staff Credentialing, Competency and Training (See Form)

1. ~~The~~ Designated Reviewer (LRE Staff and/or HealthWest Contract Staff) will review the Provider's Credentialing and Re-credentialing policies and procedures to assure compliance with HealthWest Policy No. 10-004 and MDHHS Credentialing and Re-credentialing Processes.~~—~~ Accredited Providers are responsible for credentialing and re-credentialing their employees and subcontractors as part of the requirements for being accredited. ~~-~~HealthWest will credential and re-credential its contracted ~~l~~Licensed Independent ~~p~~Practitioners practicing independently or employed by a non-accredited agency. ~~—The~~ Designated Reviewer must verify each item in the Credentialing, Competency, and Training Section of the Site Review Form for all Providers.

2. For specialized residential services, ~~the~~ Designated Reviewer must verify staff training ~~of~~in the Group Home Core Curriculum.

3. For any provider of clinical services to children and adolescents, ~~the~~ Designated Reviewer must verify the annual documentation of twenty-four (24)-hours professional development training specific to children's issues.~~-~~

~~4~~4. For any site reported as having specialty medical equipment, ~~the~~ Designated Reviewer must verify evidence of equipment-specific training by a qualified trainer and maintenance of that equipment by the manufacturer or other qualified maintenance provider.

5

~~5~~. ~~The~~ Designated Reviewer must document any deficits on the Site Review Form.

6~~6~~. ~~The~~ Designated Reviewer will monitor until full compliance is achieved.

K. Background Check Authorization (Complete and sign form)

LRE staff or HealthWest Contract Staff will review the form for completion and have the background check completed by the HealthWest Human Resources Department or the LRE. These checks must be completed prior to Contract Providers working individually with HealthWest consumers.

L. Attestation Questions (Must be completed as part of the LRE Credentialing Packet)

This form is included in the LRE Credentialing packet and must be completed prior to a contract being issued to the Provider.

M. HCBS New Residential or Non-Residential Provider Survey (Must be completed and returned with the LRE Credentialing Packet)

The purpose of the provisional approval survey is to ensure that the settings in which new providers wish to provide Home and Community Based Services are not institutional or isolated in nature. LRE Staff must ensure all new providers complete this initial survey, and the LRE Staff will review and determine provisional approval.

N. Training Requirements for New and Ongoing Service Providers (See Attachment I list)

The training requirements are set up by services to be provided. Based upon the New Provider's services, there is a list for each service on the Training Requirements Form, Attachment I.

~~I~~O. Compliance Tracking

1. ~~The~~ Designated Reviewer will notify the Provider in writing of the results of the site review, noting that the Provider was found either in full compliance or out of compliance, and copy the report to the LRE and HealthWest Contract ~~Specialist~~Staff.

2. If the ~~-~~Provider is found to be out of compliance, a~~the~~ letter of notification will require them to submit a Plan of Correction for approval within thirty days (30) of receipt of the letter identifying how the deficit(s) will be brought into compliance along with a target date ~~of~~ when compliance will be achieved.

~~HealthWest~~
3. ~~The~~ Contract ~~Specialist~~Staff will review the Plan of Correction once it is received from the LRE Designated Reviewer and assist the Provider with any corrections which fall under the CMHSP category for correction.

Commented [J15]: LRE does not send these - we have to look for them on share point

P. Latitude 43 (PCE) Account Access (Forms to be completed at Orientation of New Provider)

New Providers must choose the appropriate link below for their organization to request access to HealthWest's Electronic Health Record (EHR) system. Access will allow the

New Provider to view their consumers' clinical documentation, enter claims, and bill for rendering providers.

1. Behavioral Health Contracts-Provider Access Form

BH Provider EHR User Account Form (#A261)

2. Substance Use Disorder Contracts-Provider Access and Credentialing Forms

SUD New Hire Employee Verification Form
SUD Provider EHR User Account Form
SUD Providers Requiring ASAM Continuum Training- Online Course Required

for SUD Clinical Staff that will be completing assessments.

VI. ATTACHMENTS

Policy Flow Chart
Provider Application Review Form (Q071~~#__~~)
Action Transmittal Form (A098)
HealthWest Request for New Service Provider Form (#A259~~___~~)
~~Attachment A:~~ Contract Provider Policy/Procedure Review and Approval Form (Q071)~~Form~~

LRE/HealthWest Site Review Form (Need this form)
Background Check Authorization Form
HCBS New Residential Provider Survey
HCBS Non-Residential Provider Survey
Training Requirements for Providers: Attachment I
Conflict of Interest Form
Insurance Requirements Form
Contractor Fiscal Certification Form
W-9--Request for Taxpayer Identification Number and Certification Form
Disclosure of Ownership and Controlling Interest Statement Form
New Hire Employee Verification Form (For Substance Use Disorder (SUD) Treatment Staff Only)

VII. REFERENCES

~~Attachment A: Contract Provider Policy/Procedure Review and Approval Form~~
MDHHS/HealthWest Contract (Current)
Lakeshore Regional Entity/HealthWest Contract (Current)
Medicaid Provider Manual: Mental Health/Substance Abuse Section (Current Revision)
CARF Behavioral Health Standards Manual (Current)
ASAM Continuum User Manual For Michigan Providers

/jec (Revised 8/17/23)

DRAFT

HEALTHWEST

Policy and Procedure

No. 10-003

Prepared by:

Jackie Farrar,
Manager of Procurement and Provider Network

Effective Date: October 1, 2005
Revised Date: August 17, 2023

Approved by:

Subject: Contracting with New Service Providers, Compliance, and Site Reviews

Rich Francisco, Executive Director

I. POLICY

HealthWest will ensure there is a process in place for contracting with new providers of necessary/required services. These service providers may be in-network or out-of-network as necessary to meet the required provision of services for HealthWest consumers. HealthWest staff will also ensure initial and ongoing compliance with standards of care.

II. PURPOSE

This policy will describe the process for contracting with new service providers for both in-network and out-of-network, as HealthWest maintains an open panel for contracting agencies. HealthWest prefers to contract with accredited agencies. Contracts for services with non-accredited or single entities will be considered only if they are able to meet established eligibility criteria, or if services are of a highly specialized nature for which there is a limited provider pool listed in the application.

II. APPLICATION

Applies to Contracted Vendors/Providers of mental health services and substance abuse services for adults or children with mental illness, developmental disabilities and/or substance abuse. Also applies to all HealthWest staff and services for its consumers.

III. DEFINITIONS

Completed Network Application: Documents sent out and collected by the Lakeshore Regional Entity (LRE) and/or HealthWest Contract Staff comprise the **Provider Application Packet**. It is reviewed by the LRE and HealthWest Contract Staff to ensure it contains all required and completed documents.

Designated Reviewer: The HealthWest Contract Staff and/or the LRE Credentialing Staff assigned to the Provider or their designee.

Open Panel: Accepting new contract providers as needed/requested by HealthWest consumers and/or internal HealthWest staff as an agency of choice. Providers may contract with HealthWest at any time if they meet the requirements of the Standard Common Contract for the Lakeshore Regional Entity (LRE) of Region 3 in the State of Michigan.

A panel may be closed to new providers if accessibility to the requested service(s) is less than eighty-five percent (85%) capacity. When capacity for a service has been reached, a Request For Proposal (RFP) or a Request For Information (RFI) for any qualified new providers may be posted through the County of Muskegon Procurement Department to expand the capacity of the specific service(s) needed.

IV. PROCEDURES

A. New Provider is identified.

1. Agency contacts HealthWest to request a contract be initiated, or a HealthWest staff person identifies the need for a new Provider of Service(s). The Requestor of the new or expanded requested service(s) will complete a HealthWest Request for New Service Provider Form (#A259) and have it signed by their Program Supervisor.

2. The Program Supervisor will forward this Request Form to the Manager of Procurement and Provider Network who will schedule a meeting of appropriate leadership team members to review the request. Following their discussion and group approval to move forward with procurement, the request must be approved via signatures by the Manager of Procurement and Provider Network, the Chief Financial Officer, and the Executive Director. A Board Motion is submitted to the HealthWest Board of Directors for approval to go forward with the procurement process. A HealthWest Contract Staff will be assigned to execute a contract following the procedures outlined in this Policy/Procedure.

3. There will be times when an urgent/emergent placement of a consumer is required either same day or within a few days. For those occasions, there may not be time to complete the paperwork necessary to present a motion to the Board of Directors and complete the credentialing processes within the short time frame. Staff will contact all known providers to see if any provider is willing and appropriately trained to take our consumer immediately; this would be considered a sole source procured provider. HealthWest Staff will review documentation that the Provider's staff is trained to manage the special needs of the specific consumer and a site review visit must occur prior to the placement.

   For those emergent/urgent placement situations, it will be necessary to have the Provider sign a Single Case Agreement for up to forty-five (45) days at which time the HW Contract Staff will have presented a board motion, have the LRE credential the Provider (if not already in our system), and have a signed contract with the provider completed. If there are extenuating circumstances, a continuation Single Case Agreement may be necessary.

   Should this Provider not be willing to continue the placement beyond the forty-five (45- days, a thirty (30)-day notice is required from the Provider to HealthWest

Staff. HealthWest Staff will need to seek another appropriate placement right away.

B. Following the procurement process for new Provider(s) selection, the assigned HealthWest Contract Staff will check within the LRE Credentialing SharePoint system for information on the selected Provider(s) already received by another CMHSP in the region. If present in the LRE SharePoint system, the documentation will be downloaded into the Provider file in the Current Contracts section of the Contracts Department. Any other additional information from the Provider as applicable shall be requested, including HealthWest specific forms. If the Provider is not located in the LRE SharePoint, the HealthWest Contract Staff verifies the Provider is not pending with the LRE Credentialing Committee by contacting the LRE Credentialing Staff.

C. Application

1. All New Providers are required to complete a LRE Provider Application Packet prior to the issuing of a contract unless there is a current one already on file with the LRE.

2. LRE Credentialing will send out the Application Packet for all agency providers and complete their credentialing process. For Licensed Independent Practitioners (LIP), the HealthWest Contract Staff will send out the Provider Application Packet with instructions to return to HealthWest. LRE Credentialing Staff will be sent a copy of the LIP's credentialing packet for their records in case another Region 3 CMHSP is interested in the same provider service(s).

3. All Provider Applications for contracted services will be surveyed for compliance through a site review completed by the Lakeshore Regional Entity if within Region 3 or by a HealthWest Contract Staff if out of Region 3. Another alternative is to contact the Provider's "home" CMHSP for a copy of their Provider site review and any other information they may wish to share regarding the Provider.

D. Preparation for Monitoring Process

1. Contract Staff will forward the Application Packet to the LRE Credentialing Staff and will complete a review of the Packet submitted by the Provider.

2. Upon receipt of the Provider Application Packet, the Contract Staff will verify the packet is complete, and follow-up with the Provider to acquire missing content and proof documents.

3. Contract Staff will correct or add to the Application Packet any information sent or otherwise verified by the Provider. Information acquired by telephone will not be acceptable verification for license, insurance, accreditation, financial solvency, conflict of interest, and/or rate for service.

4. When the Provider Application Packet is complete, the LRE will initiate a site review or obtain a review from another CMHSP who is already contracting with the Provider.

5. Designated Credentialing Reviewer (LRE Staff or HW Staff) will document all full compliance categories. All non-compliance or partial compliance must be documented on the Site Review Forms with sufficient information to permit follow-up. Only when the Provider is in full compliance with HealthWest and LRE standards will a contract be issued to the Provider.

6. Once the Provider is in full compliance, the Site Review Forms will be filed in the Compliance Review section of the Provider's HealthWest contract file and/or stored on SharePoint.

7. Requests for Plans of Correction must be written by the Designated Reviewer, and copies sent to the LRE/Contract Staff to be filed in SharePoint/contract file. The Provider responses must also be filed in SharePoint/contract file.

8. LRE Designated Reviewer and/or HealthWest Contract Staff will monitor all corrective action plans and conduct follow-up site reviews as necessary to assure full compliance; copies of all reports will be forwarded to the LRE/HealthWest Contract Staff upon completion.

9. LRE Designated Reviewer and/or HealthWest Contract Staff must verify and document all corrective actions.

V. REVIEW PROCESS

A. Accreditation (Copy of Accreditation Letter/Certificate Must be Included in Returned Packet)

1. HealthWest Contract Staff must review all accreditation documents. If accredited without a plan of correction, Contract Staff will document the date he/she has verified full compliance on the Provider Application Review Form.

2. If the Provider is non-accredited, Contract Staff will document N/A on the Provider Application Review Form.

3. If the Provider is required to complete corrective actions by the accrediting body, Contract Staff will document such and the need for follow-up on the Provider Application Review Form.

B. Conflict of Interest (Conflict of Interest Compliance Certificate Form completed and signed)

1. Upon review, if a conflict of interest is not identified or is identified but corrective actions are sufficient to remediate the conflict, HealthWest Contract Staff will document full compliance (Provider Application Review Form). Contract Staff may seek Corporate Counsel opinion.

2. If a conflict of interest is identified, Contract Staff must submit a copy of the forms to the Executive Director. Executive Director/designee will schedule Corporate Counsel review and assure Corporate Counsel recommendations are implemented and documented.

Executive Director will notify the Contract Staff when full compliance can be documented.

C. Insurance (Insurance Requirement Form)

1. If the type, amount, and coverage dates of insurance meet Agency requirements, HealthWest Contract Staff will contact the Provider for the appropriate Insurance certificate. Coverage dates meet compliance if they cover the first day of the contract. A separate monitoring process is in place to identify coverage which expires during the contract year.

2. If type, amount, or coverage date(s) do not comply with Agency requirements, Contract Staff must initiate and document immediate follow-up with the Provider until full compliance can be documented and the contract initiated.

D. Financial Solvency (Contractor Fiscal Certification Form, W-9 Form, and Audits completed and signed)

1. The most current financial forms/audit reports will be forwarded to the HealthWest Chief Financial Officer for review and approval once received by the Contract Staff.

2. Financial forms/audit reports approved by the HealthWest Chief Financial Officer will be noted and documented as "in compliance". Formal audits returned by the Chief Financial Officer with questions or recommendations will be considered non-compliant and will be followed-up by the HealthWest Contract Staff until full compliance in this area can be verified and the contract initiated.

E. Disclosure of Ownership and Controlling Interest Statement (Completed and signed)
This form must be completed in its entirety for any individual in the Provider's organization with an ownership or controlling interest, including anyone with direct or indirect ownership of 5% or more, board members, or any managing employee such as general managers, business managers, administrators, and directors. This form is requested for new contracts, renewals, and when a provider has changes. LRE is the holder of this completed form.

F. Provider Facility or Other License (Copies of all Licenses, Registrations, etc., included.)

HealthWest Contract Staff will source-verify that the date of the license(s) cover(s) from the beginning contract date and will verify absence of sanctions or corrective action requirements. Licenses which expire during the contract year will be monitored by a separate monitoring process.

G. Policies and Procedures and Guidelines

Each policy must be separately monitored, including each Environment of Care policy.

1. All required HealthWest policies formally adopted by the Provider will be reported as in full compliance only when the Contract Staff and/or LRE staff has verified through the site review process that the Provider has evidence of procedures or processes in place for the policies.

2. HealthWest Contract Staff will request or review on-site the non-HealthWest policies which are included in the Provider Application Packet. The policies will be forwarded to the appropriate HealthWest staff member for formal approval or recommendations (e.g., Quality Improvement policy will be sent to HealthWest Quality Improvement Supervisor/Manager for review.) Contract Staff is responsible for tracking the flow of each document, follow-up, and documentation of any recommended changes, and final documentation of full compliance. (Attachment: Contract Provider Policy/Procedure Review and Approval Form) LRE Designated Reviewer will also review all required policies at their on-site review.

H. Delegation of Administrative Functions (See Form in Contract Packet

Provisions of the Balanced Budget Act (BBA) of 1997 allow for delegation of administrative functions through contracts between the PIHP and HealthWest, and HealthWest and Providers. For the purpose of HealthWest Provider contracts, HealthWest will not delegate Administrative Functions.

I. New Hire Employee Verification Form (For Substance Use Disorder (SUD) Treatment Staff Only)

Every SUD treatment staff member of the New Contracted Provider providing direct service must complete this form and ensure the staff's Supervisor and Program Director sign at the bottom of the last page. All forms must be returned with the LRE Application packet.

J. Staff Credentialing, Competency and Training (See Form)

1. Designated Reviewer (LRE Staff and/or HealthWest Contract Staff) will review the Provider's Credentialing and Re-credentialing policies and procedures to assure compliance with HealthWest Policy No. 10-004 and MDHHS Credentialing and Re-credentialing Processes. Accredited Providers are responsible for credentialing and re-credentialing their employees and subcontractors as part of the requirements for being accredited. HealthWest will credential and re-credential its contracted Licensed Independent Practitioners practicing independently or employed by a non-accredited agency. Designated Reviewer must verify each item in the Credentialing, Competency, and Training Section of the Site Review Form for all Providers.

2. For specialized residential services, Designated Reviewer must verify staff training in the Group Home Core Curriculum.

3. For any provider of clinical services to children and adolescents, Designated Reviewer must verify the annual documentation of twenty-four (24)-hours professional development training specific to children's issues.

4. For any site reported as having specialty medical equipment, Designated Reviewer must verify evidence of equipment-specific training by a qualified trainer and maintenance of that equipment by the manufacturer or other qualified maintenance provider.

5. Designated Reviewer must document any deficits on the Site Review Form.

6. Designated Reviewer will monitor until full compliance is achieved.

K. Background Check Authorization (Complete and sign form)

LRE staff or HealthWest Contract Staff will review the form for completion and have the background check completed by the HealthWest Human Resources Department or the LRE. These checks must be completed prior to Contract Providers working individually with HealthWest consumers.

L. Attestation Questions (Must be completed as part of the LRE Credentialing Packet)

This form is included in the LRE Credentialing packet and must be completed prior to a contract being issued to the Provider.

M. HCBS New Residential or Non-Residential Provider Survey (Must be completed and returned with the LRE Credentialing Packet)

The purpose of the provisional approval survey is to ensure that the settings in which new providers wish to provide Home and Community Based Services are not institutional or isolated in nature. LRE Staff must ensure all new providers complete this initial survey, and the LRE Staff will review and determine provisional approval.

N. Training Requirements for New and Ongoing Service Providers (See Attachment I list)

The training requirements are set up by services to be provided. Based upon the New Provider's services, there is a list for each service on the Training Requirements Form, Attachment I.

O. Compliance Tracking

1. Designated Reviewer will notify the Provider in writing of the results of the site review, noting that the Provider was found either in full compliance or out of compliance, and copy the report to the LRE and HealthWest Contract Staff.

2. If the Provider is found to be out of compliance, a letter of notification will require them to submit a Plan of Correction for approval within thirty days (30) of receipt of the letter identifying how the deficit(s) will be brought into compliance along with a target date when compliance will be achieved.

3. HealthWest Contract Staff will review the Plan of Correction once it is received from the LRE Designated Reviewer and assist the Provider with any corrections which fall under the CMHSP category for correction.

P. Latitude 43 (PCE) Account Access (Forms to be completed at Orientation of New Provider)

New Providers must choose the appropriate link below for their organization to request access to HealthWest's Electronic Health Record (EHR) system. Access will allow the

New Provider to view their consumers' clinical documentation, enter claims, and bill for rendering providers.

1. Behavioral Health Contracts-Provider Access Form

   BH Provider EHR User Account Form (#A261)

2. Substance Use Disorder Contracts-Provider Access and Credentialing Forms

   SUD New Hire Employee Verification Form
   SUD Provider EHR User Account Form
   SUD Providers Requiring ASAM Continuum Training- Online Course Required for SUD Clinical Staff that will be completing assessments.

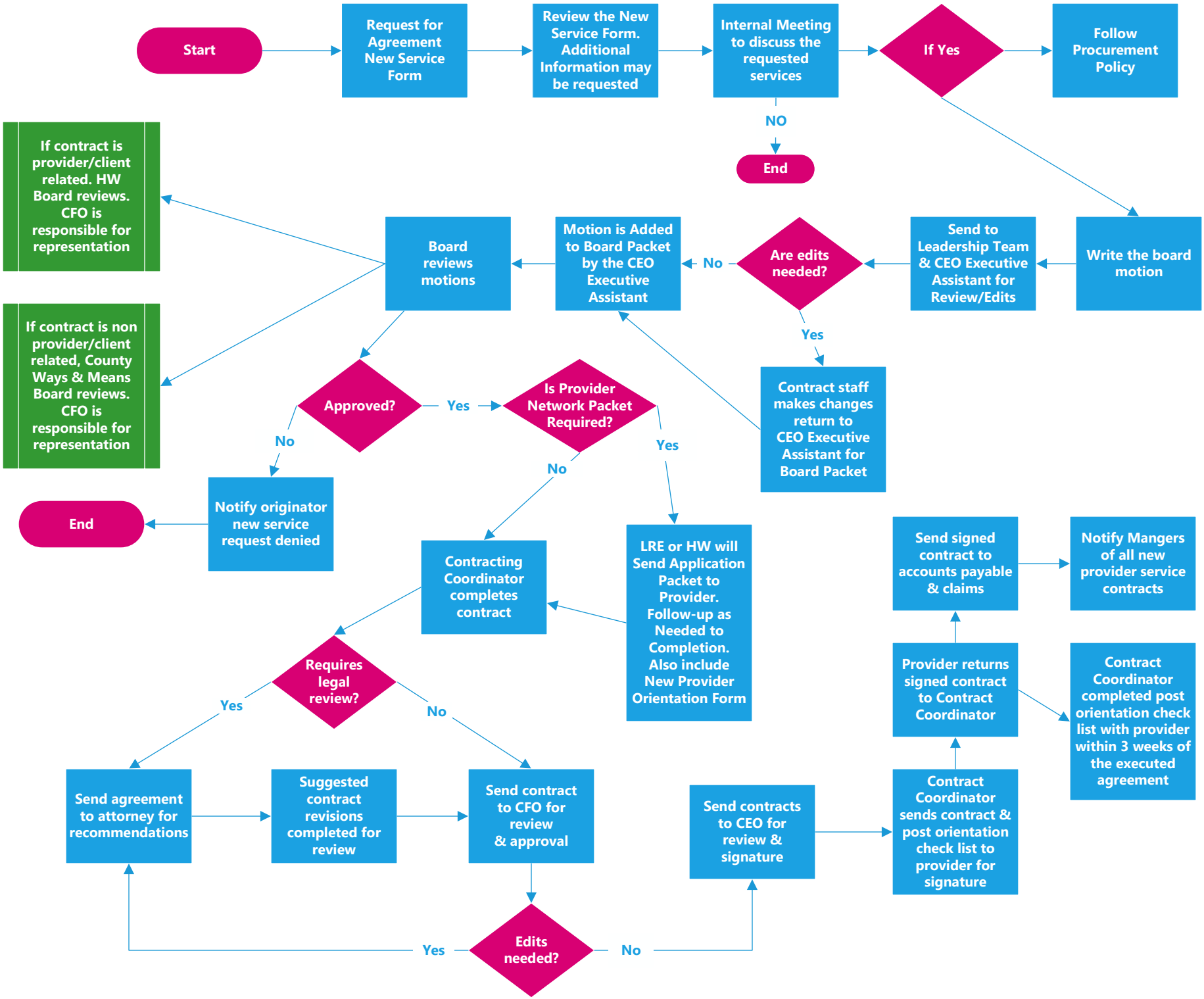
VI. ATTACHMENTS

Policy Flow Chart
Provider Application Review Form (Q071)
Action Transmittal Form (A098)
HealthWest Request for New Service Provider Form (#A259)
Contract Provider Policy/Procedure Review and Approval Form (Q071)
LRE/HealthWest Site Review Form (Need this form)
Background Check Authorization Form
HCBS New Residential Provider Survey
HCBS Non-Residential Provider Survey
Training Requirements for Providers: Attachment I
Conflict of Interest Form
Insurance Requirements Form
Contractor Fiscal Certification Form
W-9--Request for Taxpayer Identification Number and Certification Form
Disclosure of Ownership and Controlling Interest Statement Form
New Hire Employee Verification Form (For Substance Use Disorder (SUD) Treatment Staff Only)

VII. REFERENCES

MDHHS/HealthWest Contract (Current)
Lakeshore Regional Entity/HealthWest Contract (Current)
Medicaid Provider Manual: Mental Health/Substance Abuse Section (Current Revision)
CARF Behavioral Health Standards Manual (Current)
ASAM Continuum User Manual For Michigan Providers

/jec (Revised 8/17/23)



Updated
9/19/23

REQUEST FOR NEW PROVIDER SERVICES
HealthWest

Please fill out the entire Request for New Provider Services form. An incomplete form may result in a delay.

Request Date: Click here to enter a date.

Requestor Name: Enter First and Last name.

Date Needed: Click here to enter a date.

Contract Category: Choose a contract type.

Type of Service(s)

1. Choose an item.
2. Choose an item.
3. Choose an item.

Population:

☐MI Adult ☐MI Child
☐DD Adult ☐DD Child
☐SUD Adult ☐SUD Child

Additional Types of Service(s):
If there are more than three types of services requested, please add additional types here.

Rational for Service:
Please enter the rational for the services requested.

Potential Service Code(s)	Current CMH Rate	Estimated Rate for Service
Choose a service code.	Click here to enter rate.	Click here to enter rate.
Choose a service code.	Click here to enter rate.	Click here to enter rate.
Choose a service code.	Click here to enter rate.	Click here to enter rate.

Additional Service Code(s):
If there are more than three potential service codes, please add additional codes here.

Budgeted Item? ☐Yes ☐No

Annual Financial Expenses:
☐ $9,999 or less
☐ $10,000 to $24,999.99
☐ $25,000 to $149,999.99
☐ $150,000 or more

Funding Source: LRE

Service Location: Choose location where the service will be provided.

Identified Service Provider/Vendor: Enter name of Identified Service Provider.

Provider/Vendor Contact: Enter name of contact person for the provider/vendor.

Email: Click here to enter email.
Phone: Click here to enter phone number.

Systems Needed: ☐ Latitude 43

REQUEST FOR NEW PROVIDER SERVICES
HealthWest

Please fill out the entire Request for New Provider Services form. An incomplete form may result in a delay.

Notes:
Enter any additional notes (i.e. client information for single services).

Program Supervisor Signature:

Print and Sign here. _____

Manager of Procurement and Provider Network Signature:

Print and Sign here. _____

Chief Financial Officer Signature:

Print and Sign here. _____

Executive Director Signature:

Print and Sign here. _____

REQUEST FOR NEW PROVIDER SERVICES
HealthWest

Please fill out the entire Request for New Provider Services form. An incomplete form may result in a delay.

Notes:
Enter any additional notes (i.e. client information for single services).

Program Supervisor Signature:

Print and Sign here.

Manager of Procurement and Provider Network Signature:

Print and Sign here.

Chief Financial Officer Signature:

Print and Sign here.

Executive Director Signature:

Print and Sign here.

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE	BUDGETED	NON-BUDGETED	PARTIALLY BUDGETED
Program/Personnel Committee	X		

REQUESTING DIVISION	REQUEST DATE	REQUESTOR SIGNATURE
Administration	October 13, 2023	Randi Bennett, Director of Information Systems

SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)

HealthWest Board authorization is requested to make the below changes to HealthWest policy 05-026. These are also provided in detail in the attached, redlined document.

Changes Include:

1. A.3.C. Updated language to reflect current process and requirements.
2. A.3.D. Updated language to reflect current requirements.
3. A.3.F. Updated language to reflect current requirements.
4. B.3.A. Added language to provide clarification.
5. B.5.A. Added language to clarify that only licensing by legal means is permitted on HealthWest equipment, network, and systems.
6. B.6.D. Added language to provide clarification.
7. Section G, bullet point 1. Added language to provide clarification.
8. Section G, bullet point 2. Updated language to reflect current process and requirements and to add clarification.
9. Section G, bullet point 7. Updated language to reflect current HealthWest system.

SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)

I move to authorize the policy and procedural changes as described above and attached, effective October 27, 2023.

COMMITTEE DATE	COMMITTEE APPROVAL
10/13/2023	_____ Yes _____ No _____ Other
BOARD DATE	**BOARD APPROVAL**
10/27/2023	_____ Yes _____ No _____ Other

HWB 3-P

HEALTHWEST

Policy and Procedure

No. 05-026

Prepared By:

Randi Bennett
Director of Information Systems

Effective: June 1, 2020
Revised: ~~April 30, 2021~~July 11, 2023

Approved By:

~~Julia B. Rupp~~Rich Francisco
Executive Director

Subject: Information System Use

I. PURPOSE

The purpose of the Information System Use Policy is to ensure the proper use of workstations, devices, and computing facilities by the HealthWest workforce to protect the security of all agency-owned, captured, and/or stored information and data, including client- and staff-related personal and private information, as required by the HIPAA Privacy and Security Rules and other applicable regulations.

Compliance with the enclosed policies and directives will:

- Protect personal, private, proprietary, and other information contained within the HealthWest network infrastructure and systems, including, but not limited to, intellectual property.
- Protect the financial investment made in these systems.
- Protect HealthWest and its system users from unnecessary risk.

II. SCOPE

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy documents, pictures, videos, models, wireless, telecommunication, conversations, and systems either owned or chartered by HealthWest for its use as well as any other methods used to convey, capture, store, and/or share knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all HealthWest employees, interns, and temporary workers as well as by contracted providers working with HealthWest as subcontractors.

Each of the policies defined in this document is applicable to the task being performed, not to specific departments or job titles.

III. POLICY

The network infrastructure, computer systems, and computing equipment at HealthWest are provided to employees to perform their jobs. As such, HealthWest reserves the right to determine appropriate use of the equipment, software, and systems that employees use. No employee is allowed to employ these resources for personal gain. It is the responsibility of HealthWest supervisors, managers, and leadership to monitor the appropriate behavior of employees.

It is the policy of HealthWest that all employees, interns, contracted providers, and temporary workers shall comply with the requirements of applicable privacy and security standards and regulations. Compliance shall be ensured through the use of measures such as training, security reminders, policies and procedures, sanctions for policy violations, and monitoring of workforce activities.

Employees who are granted use of HealthWest-owned equipment, access to the network infrastructure, and use of computer systems at HealthWest agree to abide by the policies guiding the appropriate use of those devices and systems. Any employee found in violation of this policy may be subject to disciplinary action, up to and including termination. Some violations may also constitute a criminal offense and may result in legal action according to Federal and State laws.

This policy addresses a variety of issues that staff using HealthWest computers, as well as other technologically related devices, systems, and the HealthWest network must be aware of, as described in the following sections:

A. Gaining Access to Information Systems

B. Acceptable Use

C. The Internet and e-mail

D. Laptops, Portable Devices, and Removable Media

E. Remote Access or Use of Information

F. Information Security Incidents

G. Saving Files

H. Intimidating or Retaliatory Acts

I. Confidentiality Agreement

A. Gaining Access to Information Systems

HealthWest grants role-based access to the network, as well as other systems, and the organization's Intranet and the Internet at large. Access may also be granted based on assigned task. The purpose of this policy is to provide the minimum necessary access for employees to perform their job functions. Users may access only those computer systems and resources that are necessary to perform their assigned job duties. The IT Department or assigned designee is responsible for managing the process for the provision of access and passwords. Procedures shall include Access of Information, Network Access Changes, and Password Management.

1. Access to Information

    a. All workforce members working with personal or private information or working in areas where personal or private information is accessible must be authorized to do so.

    b. Network and system IDs and passwords are provided for individual use only and must not be shared with anyone. Activity in the system related to an employee's logon ID and password may be tracked. Use of a logon ID and password is the legal equivalent of a signature.

2. Network Access Changes

    Requests for new employee/user access must be made a minimum of 2 days prior to starting and must be made to the Information Technology (IT) Department by the Human Resources Department following the established process. The IT Department, or specified designee(s), shall be responsible for the administration of access controls to HealthWest computer systems. The IT Department, or specified designee(s), will process add, deletion, activation, inactivation, and change requests upon receipt of a written notification from the Human Resources Department, an individual's direct supervisor, or the manager over the department/team in which an individual works.

3. Password Management will adhere to the following policies:

    a. Passwords are to be treated as confidential information. Under no circumstances is any user who is provided access to HealthWest equipment and systems to give, tell, or hint at their password to another person. Passwords must not be disclosed under any conditions to other workforce members or individuals, including team or family members.

    b. No user who is provided access to HealthWest equipment and systems is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access environment, such as a safe or locked cabinet that only he/she has access to, if in hardcopy form, or in an encrypted file, if in electronic form.

c. ~~Users should not use the~~The only "Remember Password" feature ~~of applications.~~ that should be utilized within any HealthWest system and on any HealthWest equipment would be that of a password manager application provided by HealthWest Information Systems department.

d. Passwords must be changed at least every ~~45~~ 180 days.

e. A user cannot reuse previously used passwords.

f. Passwords must be at least ~~twelve~~ sixteen characters and contain three of these four characteristics: upper case letters, lower case letters, numbers, and special symbols.

g. Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

h. A password must be promptly changed if it is suspected of being disclosed or is known to have been disclosed.

B. Acceptable Use

Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, and for the care and security of any computer, device, or hardware assigned to them.

Users shall not knowingly engage in any activity that may be potentially harmful to any portion of the HealthWest network, HealthWest systems, HealthWest equipment, HealthWest users, or HealthWest consumers. They shall also take the necessary precautions to protect any confidential or sensitive information from inappropriate or unauthorized access by others.

1. Use of Computing Resources

a. Organizational computer resources must be used in a manner that complies with company policies and State and Federal laws and regulations.

b. Uses shall not interfere with the proper functioning or the ability of others to make use of HealthWest's networks, computer systems, applications, equipment, and other data and computing resources.

c. Use of HealthWest technological resources for personal gain is not permitted. Personal use of a limited nature is allowed but must not compromise the integrity of HealthWest's systems or workplace productivity.

d. Users are not permitted to connect any equipment to the agency network without prior approval from the IT Department. Users may connect equipment to the guest wireless network without prior approval.

2. Access of Information

a. Workforce members may not access systems, files, documents, or any data of other users or systems, files, documents, or other data to which they have not been properly granted access. Workforce members may not share their log-in, access codes, or passwords to the HealthWest network or the systems used in the course of HealthWest business activities, including the provision of care, with others.

b. Users leaving their work area should lock their computers (by logging off, using the ctrl-alt-delete/lock option, or Windows-L key combination) to prevent use of their login by others. The IT Department will implement an automatic password protected screen saver for all PCs connected to the network, which will activate after no more than 10 minutes of inactivity. In order to regain access to the computer, the user who is logged into that computer must enter their login id and password to unlock it. Staff may not take any action which would override this setting.

c. E-mail over the Internet shall not be used for the transmission of unencrypted protected health information (PHI) that is part of HealthWest's operations. To encrypt protected health information being sent to individuals, agencies, and/or systems outside of the HealthWest organization (outside of the healthwest.net domain), SECURE must be written in the subject line of the email message, along with any other subject information pertinent to the message being communicated.

d. Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate reason to access that information, to the extent practicable.

3. Hardware and Equipment

a. Only computer hardware owned by HealthWest is permitted to be connected to the network or to access HealthWest systems, unless other arrangements are made with the HealthWest IT Department, and only software owned by HealthWest may be installed on HealthWest equipment and devices, unless other arrangements are made with the HealthWest IT Department. Exceptions to this may be made on a case-by-case basis. Such exceptions will be considered by the IT Department, with the input of others that the department may deem necessary in the decision-making process. Consideration for exception(s) will be made after a written request for exception(s) is received by the IT Department. Computers supplied by HealthWest are to be primarily used for business purposes. Limited personal use is allowed. Guidelines regarding personal use is outlined in *C. The Internet and e-mail* section below. All individuals being provided access to the HealthWest network, systems, and equipment must read and understand the list of prohibited activities that

are outlined below. Modifications and/or configuration changes may only be made by the HealthWest IT Department, or specified designee(s) assigned by the IT Department, on computers supplied by HealthWest.

b. Computers and computer-related hardware belonging to HealthWest may not be removed from HealthWest premises without the knowledge and approval of the appropriate department manager and the IT Department.

c. Users must notify the HealthWest IT Department of any equipment provided by HealthWest that is missing or damaged. Workforce members shall promptly (within 2 hours of the discovery of the loss) report the loss or theft of any portable device, hardware, or electronic media that has been provided by HealthWest or that has accessed any HealthWest systems. Workforce members shall promptly (within 2 hours of the discovery of the loss) report the loss or theft of any PHI or other sensitive information. Report should be made to the worker's direct supervisor, the Information Technology department, and the HIPAA Privacy and Corporate Compliance Officers.

d. Employees or business associates may not bring computers from outside HealthWest and connect them to the HealthWest network without approval from the IT Department. Employees, business associates and other guests may connect computers to the HealthWest Guest Network without approval.

4. Technology

Adoption

It is the policy of HealthWest to protect the security of all agency-owned, captured, and/or stored information and data, including client-related personal or private information as new technologies and devices are adopted for use, so that any technologies or devices used do not jeopardize the security of such information and data.

Use of new or additional technologies and devices that may transmit or retain personal or private information must be subject to:

a. Explicit management and IT approval

b. Security procedures for the technology, including risk assessment

c. Maintenance of a list of all such devices and personnel with access

d. Audit of use by the HealthWest IT Department

e. Erasure of any retained data, which may require a reset to factory settings. Efforts to erase retained data may result in the loss of any and all data on the device.

5. Software Copying, Downloading, and Installation

   a. All software used on HealthWest computers must be appropriately licensed.

   b. The IT Department will coordinate the acquisition of commercial software.

   c. Software may not be downloaded and/or installed without prior approval from the IT Department. The approval process relating to any new software request shall include scanning for viruses or other malicious software. It is against company policy to install or run software requiring a license on any company-owned computer without a valid license.

   d. All software programs and documentation generated or provided by employees, temporary employees, interns, consultants, or contractors for the benefit of HealthWest are the property of HealthWest unless covered by a contractual agreement.

6. Uploading, Copying, Backing Up, and Disposing of Information

   a. Workforce members may not upload information into HealthWest systems except as part of an established business process.

   b. Workforce members may not copy information in HealthWest systems except as part of an established business process.

   c. The confidentiality of any data copied or removed from HealthWest premises must be maintained.

   d. Any data files generated by a user must be stored within network-based folders (designated by "I:" or "H:" drive). This ensures necessary backup, reduces the likelihood of data breach, and allows for the data to be utilized by other staff in the course of HealthWest business activities. Temporary storage on the local drive is allowed on a limited basis when access to the HealthWest network is not available. Guidelines outlining this is in section *G. Saving Files* below.

   e. Business information will not be deleted or otherwise removed from HealthWest systems except as in accordance with defined information disposal procedures and will not be deleted if it may be required for discovery proceedings related to lawsuit.

7. Wireless Networks

The use of non-HealthWest wireless networks for access to HealthWest systems shall be restricted to the greatest extent possible. When staff are working from their own home and utilizing a home wireless network, the network should be configured securely, utilizing at least the WPA2 encryption standard as well as a secure login and password.

When non-HealthWest and non-staff home wireless networks are utilized for access to HealthWest systems, the HealthWest VPN should be utilized in that process. When non-HealthWest and non-staff home networks must be used, the best effort should be made to utilize networks that are configured securely, utilizing at least the WPA2 encryption standard, and that require a secure login and password.

8. Instant Messaging, Direct Messaging, and Texting

Instant Messaging, Direct Messaging, and texting are not considered secure means of communication. Users are prohibited from including any confidential or protected health information in direct, instant, or text messages.

9. Teleconferencing Platforms

In order to ensure the security of proprietary and private agency information, as well as the protected health information (PHI) of individuals served by HealthWest, teleconferencing (aka video conferencing) must include the following:

- A Business Associate Agreement (BAA) between the meeting host/organization and the vendor of the platform being utilized for the teleconferencing session.
- The platform/solution being used is encrypted.
- If PHI is in any way involved during the meeting, the session must not be recorded to avoid being stored by the solution provider.
- Participation in the meeting should be controlled so that only authorized individuals are allowed to join and/or observe. This may be accomplished by utilizing such measures as requiring meeting passwords or a host-managed waiting room, as well as other similar options for regulation of participation offered by the platform being used.

If the above security and control components pertaining to the platform being used by a host inviting a HealthWest representative to a teleconference session cannot be verified, a HealthWest teleconferencing platform must be used or the HealthWest representative may not participate in the meeting.

10. Unacceptable Use

Use of network, Internet, and e-mail services at HealthWest shall comply with all applicable law, all applicable HealthWest policies, and all HealthWest contracts. Employees must not use the Internet and e-mail for purposes that are illegal, immoral, unethical, harmful to the company, harmful to other HealthWest workforce members, harmful to individuals receiving services by HealthWest, or is otherwise nonproductive. The use of programs or connection to the Internet that compromises the privacy of others and/or damages the integrity of HealthWest computer systems, data, or programs is forbidden.

Examples of unacceptable use are:

- Illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, forgery, impersonation, and computer tampering (e.g., spreading viruses).
- Internet and e-mail services may not be used in any way that violates HealthWest policies, rules or administrative orders. Use of email services in a manner which is not consistent with the mission and values of HealthWest, misrepresents HealthWest or violates any HealthWest policy, is prohibited.
- Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive.
- Opening or forwarding any email attachments (executable files) from unknown sources and/or that may contain viruses.
- Sending or forwarding chain letters of other mass mailing communications.
- Downloading any data that is inappropriate or not HealthWest-specifically approved.
- Sending communications anonymously.
- Conducting a personal business using company resources.
- Product or business advertisements, and/or sales of goods for personal gain.
- Lobbying for a cause; political, religious, or otherwise.
- Communication containing ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on their race, sex, national origin, sexual orientation, age, disability, or religious or political beliefs.
- Transmitting any content that is obscene, offensive, threatening, harassing, or fraudulent.

The following are among the prohibited activities:

- Crashing an information system. Deliberately crashing an information system is strictly prohibited unless specifically part of some HealthWest business function like system testing.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system. Exception: Authorized information system support personnel, or others authorized by IT Department, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. HealthWest has access to client level private health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited. Further, the purposeful attempt to look at or access information to which you have been granted appropriate access, but you have no business-related need to access that information at a given time, is also strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited unless given prior approval by the IT Department. All software installed on HealthWest computers must be approved by the IT Department.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by HealthWest is strictly prohibited.

C. <u>The Internet and e-mail</u>

Internet access is provided for HealthWest users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by HealthWest should be used judiciously. While seemingly trivial to a single user, the company-wide use of non-business Internet resources can consume a significant amount of Internet bandwidth, which is therefore not available for business uses.

As a productivity enhancement tool, HealthWest encourages the business use of electronic communications. However, all electronic communication systems and all

messages generated on or handled by HealthWest-owned communication software are considered the property of HealthWest – not the property of individual users. Consequently, this policy applies to all HealthWest workforce members and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voicemail, text messaging, direct messaging, instant messaging, Internet, fax, personal computers, technological devices and systems, and servers.

HealthWest provides resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services, which are intended for business purposes. However, limited personal use is permissible as long as:

1. It does not consume more than a trivial amount of employee time or resources;

2. It does not interfere with staff productivity;

3. It does not preempt any business activity;

4. It does not violate any of the following;

    a. Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

    b. Illegal activities – Use of HealthWest information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.

    c. Commercial use – Use of HealthWest information resources for personal or commercial profit is strictly prohibited.

    d. Political Activities – All political activities are strictly prohibited on HealthWest premises. HealthWest encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using HealthWest assets or resources.

    e. Harassment – HealthWest strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, HealthWest prohibits the use of computers, e-mail, voicemail, direct messaging, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but are not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f. Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is not the policy of HealthWest to monitor the content of any electronic communication, HealthWest is responsible for servicing and protecting HealthWest's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

HealthWest reserves the right, at its discretion, to review any files stored or created on HealthWest equipment or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as HealthWest policies.

Employees are reminded that HealthWest electronic communications systems are not encrypted by default. Email is subject to the confidentiality policy and therefore should include only minimal confidential data. If confidential information must be sent over the Internet by electronic communications systems, encryption or similar technologies to protect the data (including authentication of the receiving party) must be employed.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others or may even be audited by overseeing or regulating entities as well as be subpoenaed in legal situations.

D. <u>Laptops, Portable Devices, and Removable Media</u>

It is the responsibility of any staff member who is using PHI outside of HealthWest offices or connecting to the organizational network with a laptop, portable USB-based memory device, iPad, smart phone, or any other device to ensure that all components of his/her connection remain as secure as his/her network access within the office and to ensure that all security protocols normally used in the management of data are also applied. Employees must take proper care to protect laptops, portable devices, and removable

media from loss, theft, or damage, and must protect the confidentiality of any agency or client information or data held or viewed on such devices.

The IT Department reserves the right to refuse the ability to connect portable devices to organizational and organizational-connected infrastructure. The IT Department will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, clients, and other organizational equipment at risk.

The IT Department reserves the right to audit any portable device used for HealthWest business to ensure that it continues to conform to this policy. The IT Department will deny network access to any laptop that has not been properly configured.

The user of the portable device is responsible for physical and system security of the device whether they are on site, at home, or on the road.

- Users must physically secure all portable devices that are used for HealthWest interests and/or purposes.
- Such devices must not be accessed or used by unauthorized individuals.
- When off-site, equipment must be kept secure in locked buildings or vehicles and kept out of sight when unattended. If traveling by public transportation, equipment must be kept with the employee and cannot be checked as baggage.
- No sensitive data should ever be stored on portable media unless absolutely necessary. If deemed absolutely necessary to do so, the data must be maintained in an encrypted format. For instructions to encrypt a file, staff should enter a Track It work order for IT assistance.
- Do not connect HealthWest devices to non-HealthWest workstations except in the case of trusted HealthWest partners. Example: Data provided to auditors via USB drive during the course of an audit.
- Do not connect non-HealthWest devices to HealthWest workstations except in the case of trusted HealthWest partners.

Power-on passwords and encryption of stored personal or private information must be used, as possible and practicable. Passwords and other confidential data are not to be stored on portable devices or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and other similar storage media) unless encrypted using a method approved by the IT Department. Note that if a portable device is lost or stolen, information not encrypted using an approved method is considered to be breached and must be reported under state and federal laws. This is a very serious and expensive process. All users must be in compliance with encryption requirements.

All users must always allow update processes to fully complete. Various protections are available on/to all HealthWest computers, as well as other technological devices (iPhones, iPads, etc.), and these protections require updates to occur as they become available to remain as protected and secure as possible. For example, the operating system on each computer is setup to download and install updates, on a regular basis. These updates are critical to the security of all data and must be allowed to complete.

HealthWest network resources may be accessed only via an approved VPN connection, using approved hardware and software. Disabling a virus scanner or firewall may be reason for termination.

The user of a portable device which contains HealthWest data, has accessed HealthWest systems, or potentially has access to HealthWest systems agrees to immediately report to his/her supervisor, as well as to HealthWest's Privacy Officer the loss of any portable device, or any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

No matter what location, always lock the screen before walking away from a workstation. The data on the screen may be protected by HIPAA or may contain confidential or proprietary information.

When an employee leaves HealthWest, all portable media and equipment in their possession must be returned to the IT Department for appropriate data erasure that conforms to HIPAA requirements.

When no longer in productive use, all HealthWest laptops, workstations, portable devices or media, printers, fax machines, servers, and technological devices must be wiped of any existing data in a manner which conforms to HIPAA regulations. All portable media must be returned to the IT Department for appropriate data erasure when no longer in use.

E. Remote Access or Use of Information

Any and all HealthWest data or information, including but not limited to agency, service, and client data, being accessed remotely shall be protected from improper access, view, or modification in transit through encryption approved by the IT Department and shall be subject to other sections of this policy. Strong cryptography and/or encryption techniques must be used to safeguard sensitive personal or private information during transmission over public networks. Personal or private information may not be sent via unencrypted e-mail. Information not encrypted using an approved method may potentially be considered to be breached and reportable under State and Federal laws. This is a very serious, expensive process; all users must be incompliance with encryption requirements.

Confidential information may not be maintained outside HealthWest systems, network infrastructure, and facilities without a valid business reason and approval by the Privacy Officer, and any such stored confidential information must be encrypted by a means that is approved by the IT Department.

Computers used outside of HealthWest facilities by employees, interns, temporary workers, and contracted providers to access, store, or transmit HealthWest information must be used solely by the employee (not shared with other household members and not a public Internet access point) and must be configured with up-to-date virus protection, security patches, operating system and software updates, and firewall software. Such configuration will be performed personally by IT Department staff or a

designee, or by automated, scheduled processes setup by the IT Department or a designee.

If wireless networks outside of HealthWest facilities must be used by HealthWest workforce members for the transmission of any confidential information, and the configuration of the network to be used cannot be verified to be setup according to best practices for purposes of security, the HealthWest VPN should be utilized to protect the HealthWest organization's data as well as the agency's clients' information and data.

Any access or use of HealthWest information and data outside of HealthWest offices must be performed in such a way that onlookers and passers-by cannot see or overhear any PHI.

Remote Data Security Protection

1. Data Backup: Information stored on the HealthWest network and within HealthWest systems is automatically backed up on a regular basis to preserve data. Information and data must always be stored within these media. Where situations occur that access to the HealthWest network and systems is not possible but data must be captured, the information may be stored on the HealthWest-owned device being used, but that data must be transferred to the appropriate HealthWest network and/or system as soon as possible. In the event that PHI or other sensitive information must be temporarily retained locally to a device, workforce members shall be responsible for the protection from improper use or disclosure of all PHI or other sensitive information. At the earliest time that the HealthWest network becomes available, all data is to be moved from the device's local drive to the agency network, ensuring no PHI remains on the device's local storage, including in the "trash bin". As described in the policies above, portable media, including but not limited to laptops, should be protected at all times to avoid loss, theft, or damage causing potential loss or breach of data.
2. Transferring Data to HealthWest: When working remotely, transferring data to HealthWest requires the use of an approved secure connection (VPN) to ensure the confidentiality of the data being transmitted. Do not circumvent established procedures nor create your own method when transferring data to HealthWest. External System Access: If you require access to an external system, contact the IT Department. The IT Department or a designee will assist in establishing a secure method of access to the external system.
3. E-mail: Do not send any personal health information (PHI) via e-mail to individuals or organizations outside of HealthWest unless it is encrypted. This is done by including the word "secure" in the subject line of the email message, along with any other appropriate subject information pertaining to the email message. If you need assistance with this, contact the Privacy Officer or IT Department to ensure approved encryption is utilized for transmission through e-mail.

4. Non-HealthWest Networks: Extreme care must be taken when connecting HealthWest equipment to a home or public network. Although HealthWest actively monitors its security status and maintains organization-wide protection policies and procedures to protect its data and systems, HealthWest has no ability to monitor or control the security procedures on non-HealthWest networks.
5. Protect Data in Your Possession: View or access only the information that you have a need to see in the course of performing job duties assigned to you. Regularly review the data you have stored to ensure that client data is as accurate and up to date as possible and that old data is eliminated or archived, as appropriate, as soon as possible. Electronic data should only be stored on the HealthWest network or within HealthWest systems. It should not be permanently stored on portable devices, including but not limited to laptops.
6. Hard Copy Reports or Work Papers: Never leave paper records displaying PHI around your work area. Lock all paper records in a file cabinet at night and put all paper records away or turn over when you leave your work area. PHI in your possession is your responsibility and should not be available where others have access or are able to otherwise view the data.
7. Data Entry When in a Public Location: To the greatest extent possible, do not perform work tasks which require the use of sensitive organizational or client level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you. If working in a public area becomes necessary, ensure that others are not able to view the organizational or client information with which you are working.
8. Sending Data Outside HealthWest: All external transfers of patient data must be associated with an official contract, appropriate Business Associate Agreement, and/or existing, current release of information signed by the client(s) whose data will be shared.

F. Information Security Incidents

All users must immediately report to the IT Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc. If the incident involves client data, the Privacy Officer must also be notified.

An incident may be any event that affects the confidentiality, integrity, or availability of agency or client information based in any electronic systems or networks. Reportable incidents may include known or suspected breaches of security, unusually slow or improper workstation or system operation, unusual or repeated system crashes, or other out-of-the-ordinary workstation or system behaviors.

Examples of information security incidents may include (but are not limited to):

- An employee, intern, temporary worker, or contracted individual or organization viewing protected information in a database the individual is not authorized to access under HealthWest policy.

- An employee, intern, temporary worker, or contracted individual or organization downloading software which is not permitted under the Information System User Policy.
- Intrusion of a HealthWest system by an unauthorized third party (“hacker”) within which Patient Health Information (PHI) resides. In this situation, there would be an assumption that there was a probable access or loss of confidential patient information.
- An unauthorized third party ("hacker") using a falsified username and password to gain access to HealthWest Information Systems.
- An unauthorized third party seeking HealthWest Information System access control or other information by pretending to be an individual authorized to obtain such information ("Social Engineering").
- An unauthorized third party ("hacker") who acquires access to any HealthWest system or device by any means or method.
- An email or other communication purporting to be from an authorized party seeking Protected Information or information potentially useful in obtaining Information System access ("phishing").
- A software virus or worm ("malware") interfering with the functioning of HealthWest-owned computers which are part of an Information System and which may also result in a compromise of the infected system by a remote “hacker”, etc.

G. Saving Files

- All PHI or other sensitive information must be stored in secure server environments only, as in a directory on a HealthWest secure network file server. PHI and other sensitive information should not be stored on hard drives or portable drives/media when the HealthWest network, or other appropriate HealthWest system, is accessible. The only exception to allowing PHI or other sensitive information to be saved on a local hard drive is when staff must work in a situation, ~~at a remote site~~ where there is no capability of connecting to the HealthWest network, or appropriate HealthWest system, such as when Wi-Fi and cell service/hotspot are not available. In the event that PHI or other sensitive information must be temporarily retained locally to a device, workforce members shall be responsible for the protection from improper use or disclosure of all PHI or other sensitive information. At the earliest time that the HealthWest network or appropriate system becomes available, all data is to be moved from the device’s local drive to the agency network / system, ensuring no PHI remains on the device’s local storage, including in the “trash bin”.
- Any file that is created outside of the HealthWest Electronic Health Record (EHR) system, and contains an individual client’s PHI, must be uploaded to the HealthWest EHR system in its final format at the earliest time that access to the EHR is available. If there is a question or concern about a file being appropriate for EHR storage, the Client Information Manager or Director of Health Information Services should be consulted. If it is determined the file is not

appropriate for EHR storage, but it contains an individual's PHI, the file must be saved to the network drive denoted by the letter H:, within the directory entitled "client," then within the subdirectory titled with the client ID number relating to the file being saved.

- ~~Any file that needs to be saved in its original format, and contains an individual client's PHI, must be saved to the network drive denoted by the letter H:, within the directory entitled "client", then within the subdirectory titled with the client ID number relating to the file being saved.~~
- ~~Any file that does not need to be saved in its original format but does contain the PHI of one specific client, and needs to be part of that client's record, should be submitted to the Clerical department to be included in the client's Laserfiche record. The electronic file used to create the document does not need to be saved in this case.~~
- Any file that needs to be saved in its original format, and that contains the PHI of multiple clients, must be saved to the network drive denoted by the letter H:, within the appropriate directory/subdirectory hierarchy of that network drive. In this case, the appropriate "save location" will vary depending on the purpose of the file as well as who needs access to it. For example, there are various teams and programs that utilize shared lists containing multiple clients and those individuals' associated data. Case in point, if "Team X" has a list of clients and points of data important to that teams' "ABC Project", they must save that file on the H: drive but have options of where to save within that network drive. Based on the purpose in this example case, those staff may choose to save the file within the "Team X" folder, then within the "ABC Project" folder from there. Good judgment should be used in the file save process. If a staff questions where a file should be saved, he/she should consult with his/her supervisor. If technical questions or needs are involved, the Information Technology department may also be sought out for advice and assistance.
- In the case that a file needs to be saved, but does not contain client-related PHI, and you are the only individual who needs access to the file, that file should be saved to the network drive denoted by the letter I:. Each staff person is allotted server file storage space for his/her specific work purposes. Since data and information stored in the "I: drive" is intended for only your specific use, you may utilize your preferred file storage method within this network drive/location (folders, file names, etc.). Even though this network location is provided for each person's own, individual use, it should be understood that any file, of any type, in any location on the HealthWest network, is available and accessible to the appropriate agency personnel for such reasons as audit, supervision, corporate compliance, security, and FOIA, among others.
- No file should be stored directly beneath the network drive denoted by the letter "H:". Files should be stored in an appropriate directory/subdirectory hierarchy described in the points above.
- In cases where there are existing Business Associate Agreements (BAA) between HealthWest and outside entities for purposes of collaborative work, and there is a need to share files, including the potential for PHI, secure,

encrypted storage locations/methods will be utilized where appropriate rights to the data can be managed. Examples of this include, but may not be limited to, HealthWest's managed SharePoint site, the HealthWest Google Suite, and File Transfer Protocol (FTP).

The only cloud-based storage that should be utilized for housing PHI or other sensitive information relating to HealthWest business would be under contract for HealthWest use. Under contract, this would be considered part of the HealthWest network and/or the HealthWest system to which the storage relates to, and therefore, acceptable for storage of this information. Typically, a cloud-based storage situation for HealthWest purposes would be through the use of a vendor-hosted system. For example, the HealthWest ~~cx360~~ Latitude43/Peter Chang Enterprises (PCE) Electronic Health Record (EHR) offers the options of self-hosting or cloud. HealthWest chose the cloud option for its purposes. This would fall under the umbrella of the term cloud-based storage as well as "under contracted use by" HealthWest. In the case of housing PHI, HealthWest would also have a BAA in place for the system/storage being utilized. For any other situation, the Corporate Compliance Officer, HIPAA Officer, and Director of Information Systems should be consulted to determine appropriateness and acceptability of that specific situation.

H. Intimidating or Retaliatory Acts

Any individual who provides assistance with HIPAA compliance and any regulatory officials or investigations, shall not be subjected to intimidation or retaliatory acts by HealthWest, per HIPAA Privacy Rule §164.530(g).

Any individual who provides assistance with regulatory compliance (aka corporate compliance), and any regulatory officials or investigations, shall not be subjected to intimidation or retaliatory acts by HealthWest.

I. Confidentiality Agreement

Users of HealthWest Information ~~resources~~ resources understand that abiding by this agreement is a condition of employment. If breach of any provision of this agreement shall occur, the individual may be subject to civil or criminal liability and/or disciplinary action consistent with applicable HealthWest policies, contracts, and processes. Temporary workers and third-party employees (i.e., contracted individuals and organizations) must also abide by this agreement and may also be subject to civil or criminal liability, as well as termination of any employment, work agreement, or contract that exists between the worker and the HealthWest agency.

IV. ENFORCEMENT

Any employee, vendor, client, intern, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

V. POLICY REVIEW AND APPROVAL

HealthWest management performs a periodic review of this policy. Based on the review, HealthWest management may change this policy to reflect its intentions and compliance requirements.

HEALTHWEST

DRAFT

Policy and Procedure

No. 05-026

Prepared By:

Effective: June 1, 2020
Revised: July 11, 2023

Randi Bennett
Director of Information Systems

Approved By:

Subject: Information System Use

_____
Rich Francisco
Executive Director

I. PURPOSE

The purpose of the Information System Use Policy is to ensure the proper use of workstations, devices, and computing facilities by the HealthWest workforce to protect the security of all agency-owned, captured, and/or stored information and data, including client- and staff-related personal and private information, as required by the HIPAA Privacy and Security Rules and other applicable regulations.

Compliance with the enclosed policies and directives will:

- Protect personal, private, proprietary, and other information contained within the HealthWest network infrastructure and systems, including, but not limited to, intellectual property.
- Protect the financial investment made in these systems.
- Protect HealthWest and its system users from unnecessary risk.

II. SCOPE

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy documents, pictures, videos, models, wireless, telecommunication, conversations, and systems either owned or chartered by HealthWest for its use as well as any other methods used to convey, capture, store, and/or share knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all HealthWest employees, interns, and temporary workers as well as by contracted providers working with HealthWest as subcontractors.

Each of the policies defined in this document is applicable to the task being performed, not to specific departments or job titles.

III. POLICY

The network infrastructure, computer systems, and computing equipment at HealthWest are provided to employees to perform their jobs. As such, HealthWest reserves the right to determine appropriate use of the equipment, software, and systems that employees use. No employee is allowed to employ these resources for personal gain. It is the responsibility of HealthWest supervisors, managers, and leadership to monitor the appropriate behavior of employees.

It is the policy of HealthWest that all employees, interns, contracted providers, and temporary workers shall comply with the requirements of applicable privacy and security standards and regulations. Compliance shall be ensured through the use of measures such as training, security reminders, policies and procedures, sanctions for policy violations, and monitoring of workforce activities.

Employees who are granted use of HealthWest-owned equipment, access to the network infrastructure, and use of computer systems at HealthWest agree to abide by the policies guiding the appropriate use of those devices and systems. Any employee found in violation of this policy may be subject to disciplinary action, up to and including termination. Some violations may also constitute a criminal offense and may result in legal action according to Federal and State laws.

This policy addresses a variety of issues that staff using HealthWest computers, as well as other technologically related devices, systems, and the HealthWest network must be aware of, as described in the following sections:

A. Gaining Access to Information Systems

B. Acceptable Use

C. The Internet and e-mail

D. Laptops, Portable Devices, and Removable Media

E. Remote Access or Use of Information

F. Information Security Incidents

G. Saving Files

H. Intimidating or Retaliatory Acts

I. Confidentiality Agreement

A. Gaining Access to Information Systems

HealthWest grants role-based access to the network, as well as other systems, and the organization's Intranet and the Internet at large. Access may also be granted based on assigned task. The purpose of this policy is to provide the minimum necessary access for employees to perform their job functions. Users may access only those computer systems and resources that are necessary to perform their assigned job duties. The IT Department or assigned designee is responsible for managing the process for the provision of access and passwords. Procedures shall include Access of Information, Network Access Changes, and Password Management.

1. Access to Information

    a. All workforce members working with personal or private information or working in areas where personal or private information is accessible must be authorized to do so.

    b. Network and system IDs and passwords are provided for individual use only and must not be shared with anyone. Activity in the system related to an employee's logon ID and password may be tracked. Use of a logon ID and password is the legal equivalent of a signature.

2. Network Access Changes

    Requests for new employee/user access must be made a minimum of 2 days prior to starting and must be made to the Information Technology (IT) Department by the Human Resources Department following the established process. The IT Department, or specified designee(s), shall be responsible for the administration of access controls to HealthWest computer systems. The IT Department, or specified designee(s), will process add, deletion, activation, inactivation, and change requests upon receipt of a written notification from the Human Resources Department, an individual's direct supervisor, or the manager over the department/team in which an individual works.

3. Password Management will adhere to the following policies:

    a. Passwords are to be treated as confidential information. Under no circumstances is any user who is provided access to HealthWest equipment and systems to give, tell, or hint at their password to another person. Passwords must not be disclosed under any conditions to other workforce members or individuals, including team or family members.

    b. No user who is provided access to HealthWest equipment and systems is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access environment, such

as a safe or locked cabinet that only he/she has access to, if in hardcopy form, or in an encrypted file, if in electronic form.

c. The only “Remember Password” feature that should be utilized within any HealthWest system and on any HealthWest equipment would be that of a password manager application provided by HealthWest Information Systems department.

d. Passwords must be changed at least every 180 days.

e. A user cannot reuse previously used passwords.

f. Passwords must be at least sixteen characters and contain three of these four characteristics: upper case letters, lower case letters, numbers, and special symbols.

g. Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

h. A password must be promptly changed if it is suspected of being disclosed or is known to have been disclosed.

B. <u>Acceptable Use</u>

Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, and for the care and security of any computer, device, or hardware assigned to them.

Users shall not knowingly engage in any activity that may be potentially harmful to any portion of the HealthWest network, HealthWest systems, HealthWest equipment, HealthWest users, or HealthWest consumers. They shall also take the necessary precautions to protect any confidential or sensitive information from inappropriate or unauthorized access by others.

1. Use of Computing Resources

a. Organizational computer resources must be used in a manner that complies with company policies and State and Federal laws and regulations.

b. Uses shall not interfere with the proper functioning or the ability of others to make use of HealthWest's networks, computer systems, applications, equipment, and other data and computing resources.

c. Use of HealthWest technological resources for personal gain is not permitted. Personal use of a limited nature is allowed but must not compromise the integrity of HealthWest’s systems or workplace productivity.

d. Users are not permitted to connect any equipment to the agency network without prior approval from the IT Department. Users may connect equipment to the guest wireless network without prior approval.

2. Access of Information

a. Workforce members may not access systems, files, documents, or any data of other users or systems, files, documents, or other data to which they have not been properly granted access. Workforce members may not share their log-in, access codes, or passwords to the HealthWest network or the systems used in the course of HealthWest business activities, including the provision of care, with others.

b. Users leaving their work area should lock their computers (by logging off, using the ctrl-alt-delete/lock option, or Windows-L key combination) to prevent use of their login by others. The IT Department will implement an automatic password protected screen saver for all PCs connected to the network, which will activate after no more than 10 minutes of inactivity. In order to regain access to the computer, the user who is logged into that computer must enter their login id and password to unlock it. Staff may not take any action which would override this setting.

c. E-mail over the Internet shall not be used for the transmission of unencrypted protected health information (PHI) that is part of HealthWest's operations. To encrypt protected health information being sent to individuals, agencies, and/or systems outside of the HealthWest organization (outside of the healthwest.net domain), SECURE must be written in the subject line of the email message, along with any other subject information pertinent to the message being communicated.

d. Workstations shall only be used in such a manner that the information displayed thereon is not made visible to others who do not have a legitimate reason to access that information, to the extent practicable.

3. Hardware and Equipment

a. Only computer hardware owned by HealthWest is permitted to be connected to the network or to access HealthWest systems, unless other arrangements are made with the HealthWest IT Department, and only software owned by HealthWest may be installed on HealthWest equipment and devices, unless other arrangements are made with the HealthWest IT Department. Exceptions to this may be made on a case-by-case basis. Such exceptions will be considered by the IT Department, with the input of others that the department may deem necessary in the decision-making process. Consideration for exception(s) will be made after a written request for exception(s) is received by the IT Department.

Computers supplied by HealthWest are to be primarily used for business purposes. Limited personal use is allowed. Guidelines regarding personal use is outlined in *C. The Internet and e-mail* section below. All individuals being provided access to the HealthWest network, systems, and equipment must read and understand the list of prohibited activities that are outlined below. Modifications and/or configuration changes may only be made by the HealthWest IT Department, or specified designee(s) assigned by the IT Department, on computers supplied by HealthWest.

b. Computers and computer-related hardware belonging to HealthWest may not be removed from HealthWest premises without the knowledge and approval of the appropriate department manager and the IT Department.

c. Users must notify the HealthWest IT Department of any equipment provided by HealthWest that is missing or damaged. Workforce members shall promptly (within 2 hours of the discovery of the loss) report the loss or theft of any portable device, hardware, or electronic media that has been provided by HealthWest or that has accessed any HealthWest systems. Workforce members shall promptly (within 2 hours of the discovery of the loss) report the loss or theft of any PHI or other sensitive information. Report should be made to the worker's direct supervisor, the Information Technology department, and the HIPAA Privacy and Corporate Compliance Officers.

d. Employees or business associates may not bring computers from outside HealthWest and connect them to the HealthWest network without approval from the IT Department. Employees, business associates and other guests may connect computers to the HealthWest Guest Network without approval.

4. Technology

Adoption

It is the policy of HealthWest to protect the security of all agency-owned, captured, and/or stored information and data, including client-related personal or private information as new technologies and devices are adopted for use, so that any technologies or devices used do not jeopardize the security of such information and data.

Use of new or additional technologies and devices that may transmit or retain personal or private information must be subject to:

a. Explicit management and IT approval

b. Security procedures for the technology, including risk assessment

c. Maintenance of a list of all such devices and personnel with access

d. Audit of use by the HealthWest IT Department

e. Erasure of any retained data, which may require a reset to factory settings. Efforts to erase retained data may result in the loss of any and all data on the device.

5. Software Copying, Downloading, and Installation

a. All software used on HealthWest computers must be appropriately licensed.

b. The IT Department will coordinate the acquisition of commercial software.

c. Software may not be downloaded and/or installed without prior approval from the IT Department. The approval process relating to any new software request shall include scanning for viruses or other malicious software. It is against company policy to install or run software requiring a license on any company-owned computer without a valid license.

d. All software programs and documentation generated or provided by employees, temporary employees, interns, consultants, or contractors for the benefit of HealthWest are the property of HealthWest unless covered by a contractual agreement.

6. Uploading, Copying, Backing Up, and Disposing of Information

a. Workforce members may not upload information into HealthWest systems except as part of an established business process.

b. Workforce members may not copy information in HealthWest systems except as part of an established business process.

c. The confidentiality of any data copied or removed from HealthWest premises must be maintained.

d. Any data files generated by a user must be stored within network-based folders (designated by “I:” or “H:” drive). This ensures necessary backup, reduces the likelihood of data breach, and allows for the data to be utilized by other staff in the course of HealthWest business activities. Temporary storage on the local drive is allowed on a limited basis when access to the HealthWest network is not available. Guidelines outlining this is in section *G. Saving Files* below.

e. Business information will not be deleted or otherwise removed from HealthWest systems except as in accordance with defined information

disposal procedures and will not be deleted if it may be required for discovery proceedings related to lawsuit.

7. Wireless Networks

The use of non-HealthWest wireless networks for access to HealthWest systems shall be restricted to the greatest extent possible. When staff are working from their own home and utilizing a home wireless network, the network should be configured securely, utilizing at least the WPA2 encryption standard as well as a secure login and password.

When non-HealthWest and non-staff home wireless networks are utilized for access to HealthWest systems, the HealthWest VPN should be utilized in that process. When non-HealthWest and non-staff home networks must be used, the best effort should be made to utilize networks that are configured securely, utilizing at least the WPA2 encryption standard, and that require a secure login and password.

8. Instant Messaging, Direct Messaging, and Texting

Instant Messaging, Direct Messaging, and texting are not considered secure means of communication. Users are prohibited from including any confidential or protected health information in direct, instant, or text messages.

9. Teleconferencing Platforms

In order to ensure the security of proprietary and private agency information, as well as the protected health information (PHI) of individuals served by HealthWest, teleconferencing (aka video conferencing) must include the following:

- A Business Associate Agreement (BAA) between the meeting host/organization and the vendor of the platform being utilized for the teleconferencing session.
- The platform/solution being used is encrypted.
- If PHI is in any way involved during the meeting, the session must not be recorded to avoid being stored by the solution provider.
- Participation in the meeting should be controlled so that only authorized individuals are allowed to join and/or observe. This may be accomplished by utilizing such measures as requiring meeting passwords or a host-managed waiting room, as well as other similar options for regulation of participation offered by the platform being used.

If the above security and control components pertaining to the platform being used by a host inviting a HealthWest representative to a teleconference session cannot be verified, a HealthWest teleconferencing platform must be used or the HealthWest representative may not participate in the meeting.

10. Unacceptable Use

Use of network, Internet, and e-mail services at HealthWest shall comply with all applicable law, all applicable HealthWest policies, and all HealthWest contracts. Employees must not use the Internet and e-mail for purposes that are illegal, immoral, unethical, harmful to the company, harmful to other HealthWest workforce members, harmful to individuals receiving services by HealthWest, or is otherwise nonproductive. The use of programs or connection to the Internet that compromises the privacy of others and/or damages the integrity of HealthWest computer systems, data, or programs is forbidden.

Examples of unacceptable use are:

- Illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, forgery, impersonation, and computer tampering (e.g., spreading viruses).
- Internet and e-mail services may not be used in any way that violates HealthWest policies, rules or administrative orders. Use of email services in a manner which is not consistent with the mission and values of HealthWest, misrepresents HealthWest or violates any HealthWest policy, is prohibited.
- Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive.
- Opening or forwarding any email attachments (executable files) from unknown sources and/or that may contain viruses.
- Sending or forwarding chain letters of other mass mailing communications.
- Downloading any data that is inappropriate or not HealthWest-specifically approved.
- Sending communications anonymously.
- Conducting a personal business using company resources.
- Product or business advertisements, and/or sales of goods for personal gain.
- Lobbying for a cause; political, religious, or otherwise.
- Communication containing ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on their race, sex, national origin, sexual orientation, age, disability, or religious or political beliefs.
- Transmitting any content that is obscene, offensive, threatening, harassing, or fraudulent.

The following are among the prohibited activities:

- Crashing an information system. Deliberately crashing an information system is strictly prohibited unless specifically part of some HealthWest business function like system testing.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system. Exception: Authorized information system support personnel, or others authorized by IT Department, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. HealthWest has access to client level private health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited. Further, the purposeful attempt to look at or access information to which you have been granted appropriate access, but you have no business-related need to access that information at a given time, is also strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited unless given prior approval by the IT Department. All software installed on HealthWest computers must be approved by the IT Department.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by HealthWest is strictly prohibited.

C. <u>The Internet and e-mail</u>

Internet access is provided for HealthWest users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by HealthWest should be used judiciously. While seemingly trivial to a single user, the company-wide use of non-business Internet resources can consume a significant amount of Internet bandwidth, which is therefore not available for business uses.

As a productivity enhancement tool, HealthWest encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by HealthWest-owned communication software are considered the property of HealthWest – not the property of individual users. Consequently, this policy applies to all HealthWest workforce members and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voicemail, text messaging, direct messaging, instant messaging, Internet, fax, personal computers, technological devices and systems, and servers.

HealthWest provides resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services, which are intended for business purposes. However, limited personal use is permissible as long as:

1. It does not consume more than a trivial amount of employee time or resources;

2. It does not interfere with staff productivity;

3. It does not preempt any business activity;

4. It does not violate any of the following;

    a. Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

    b. Illegal activities – Use of HealthWest information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.

    c. Commercial use – Use of HealthWest information resources for personal or commercial profit is strictly prohibited.

    d. Political Activities – All political activities are strictly prohibited on HealthWest premises. HealthWest encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using HealthWest assets or resources.

    e. Harassment – HealthWest strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, HealthWest prohibits the use of computers, e-mail, voicemail, direct messaging, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but are not limited to, ethnic slurs, racial comments, off-color jokes, or anything

that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f. Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is not the policy of HealthWest to monitor the content of any electronic communication, HealthWest is responsible for servicing and protecting HealthWest's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

HealthWest reserves the right, at its discretion, to review any files stored or created on HealthWest equipment or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as HealthWest policies.

Employees are reminded that HealthWest electronic communications systems are not encrypted by default. Email is subject to the confidentiality policy and therefore should include only minimal confidential data. If confidential information must be sent over the Internet by electronic communications systems, encryption or similar technologies to protect the data (including authentication of the receiving party) must be employed.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others or may even be audited by overseeing or regulating entities as well as be subpoenaed in legal situations.

D. <u>Laptops, Portable Devices, and Removable Media</u>

It is the responsibility of any staff member who is using PHI outside of HealthWest offices or connecting to the organizational network with a laptop, portable USB-based memory

device, iPad, smart phone, or any other device to ensure that all components of his/her connection remain as secure as his/her network access within the office and to ensure that all security protocols normally used in the management of data are also applied. Employees must take proper care to protect laptops, portable devices, and removable media from loss, theft, or damage, and must protect the confidentiality of any agency or client information or data held or viewed on such devices.

The IT Department reserves the right to refuse the ability to connect portable devices to organizational and organizational-connected infrastructure. The IT Department will engage in such action if it feels such equipment is being used in such a way that puts the company's systems, data, users, clients, and other organizational equipment at risk.

The IT Department reserves the right to audit any portable device used for HealthWest business to ensure that it continues to conform to this policy. The IT Department will deny network access to any laptop that has not been properly configured.

The user of the portable device is responsible for physical and system security of the device whether they are on site, at home, or on the road.

- Users must physically secure all portable devices that are used for HealthWest interests and/or purposes.
- Such devices must not be accessed or used by unauthorized individuals.
- When off-site, equipment must be kept secure in locked buildings or vehicles and kept out of sight when unattended. If traveling by public transportation, equipment must be kept with the employee and cannot be checked as baggage.
- No sensitive data should ever be stored on portable media unless absolutely necessary. If deemed absolutely necessary to do so, the data must be maintained in an encrypted format. For instructions to encrypt a file, staff should enter a Track It work order for IT assistance.
- Do not connect HealthWest devices to non-HealthWest workstations except in the case of trusted HealthWest partners. Example: Data provided to auditors via USB drive during the course of an audit.
- Do not connect non-HealthWest devices to HealthWest workstations except in the case of trusted HealthWest partners.

Power-on passwords and encryption of stored personal or private information must be used, as possible and practicable. Passwords and other confidential data are not to be stored on portable devices or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and other similar storage media) unless encrypted using a method approved by the IT Department. Note that if a portable device is lost or stolen, information not encrypted using an approved method is considered to be breached and must be reported under state and federal laws. This is a very serious and expensive process. All users must be in compliance with encryption requirements.

All users must always allow update processes to fully complete. Various protections are available on/to all HealthWest computers, as well as other technological devices

(iPhones, iPads, etc.), and these protections require updates to occur as they become available to remain as protected and secure as possible. For example, the operating system on each computer is setup to download and install updates, on a regular basis. These updates are critical to the security of all data and must be allowed to complete.

HealthWest network resources may be accessed only via an approved VPN connection, using approved hardware and software. Disabling a virus scanner or firewall may be reason for termination.

The user of a portable device which contains HealthWest data, has accessed HealthWest systems, or potentially has access to HealthWest systems agrees to immediately report to his/her supervisor, as well as to HealthWest's Privacy Officer the loss of any portable device, or any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

No matter what location, always lock the screen before walking away from a workstation. The data on the screen may be protected by HIPAA or may contain confidential or proprietary information.

When an employee leaves HealthWest, all portable media and equipment in their possession must be returned to the IT Department for appropriate data erasure that conforms to HIPAA requirements.

When no longer in productive use, all HealthWest laptops, workstations, portable devices or media, printers, fax machines, servers, and technological devices must be wiped of any existing data in a manner which conforms to HIPAA regulations. All portable media must be returned to the IT Department for appropriate data erasure when no longer in use.

E. Remote Access or Use of Information

Any and all HealthWest data or information, including but not limited to agency, service, and client data, being accessed remotely shall be protected from improper access, view, or modification in transit through encryption approved by the IT Department and shall be subject to other sections of this policy. Strong cryptography and/or encryption techniques must be used to safeguard sensitive personal or private information during transmission over public networks. Personal or private information may not be sent via unencrypted e-mail. Information not encrypted using an approved method may potentially be considered to be breached and reportable under State and Federal laws. This is a very serious, expensive process; all users must be incompliance with encryption requirements.

Confidential information may not be maintained outside HealthWest systems, network infrastructure, and facilities without a valid business reason and approval by the Privacy Officer, and any such stored confidential information must be encrypted by a means that is approved by the IT Department.

Computers used outside of HealthWest facilities by employees, interns, temporary workers, and contracted providers to access, store, or transmit HealthWest information must be used solely by the employee (not shared with other household members and not a public Internet access point) and must be configured with up-to-date virus protection, security patches, operating system and software updates, and firewall software. Such configuration will be performed personally by IT Department staff or a designee, or by automated, scheduled processes setup by the IT Department or a designee.

If wireless networks outside of HealthWest facilities must be used by HealthWest workforce members for the transmission of any confidential information, and the configuration of the network to be used cannot be verified to be setup according to best practices for purposes of security, the HealthWest VPN should be utilized to protect the HealthWest organization's data as well as the agency's clients' information and data.

Any access or use of HealthWest information and data outside of HealthWest offices must be performed in such a way that onlookers and passers-by cannot see or overhear any PHI.

Remote Data Security Protection

1. Data Backup: Information stored on the HealthWest network and within HealthWest systems is automatically backed up on a regular basis to preserve data. Information and data must always be stored within these media. Where situations occur that access to the HealthWest network and systems is not possible but data must be captured, the information may be stored on the HealthWest-owned device being used, but that data must be transferred to the appropriate HealthWest network and/or system as soon as possible. In the event that PHI or other sensitive information must be temporarily retained locally to a device, workforce members shall be responsible for the protection from improper use or disclosure of all PHI or other sensitive information. At the earliest time that the HealthWest network becomes available, all data is to be moved from the device's local drive to the agency network, ensuring no PHI remains on the device's local storage, including in the "trash bin". As described in the policies above, portable media, including but not limited to laptops, should be protected at all times to avoid loss, theft, or damage causing potential loss or breach of data.
2. Transferring Data to HealthWest: When working remotely, transferring data to HealthWest requires the use of an approved secure connection (VPN) to ensure the confidentiality of the data being transmitted. Do not circumvent established procedures nor create your own method when transferring data to HealthWest. External System Access: If you require access to an external system, contact the IT Department. The IT Department or a designee will assist in establishing a secure method of access to the external system.

3. E-mail: Do not send any personal health information (PHI) via e-mail to individuals or organizations outside of HealthWest unless it is encrypted. This is done by including the word “secure” in the subject line of the email message, along with any other appropriate subject information pertaining to the email message. If you need assistance with this, contact the Privacy Officer or IT Department to ensure approved encryption is utilized for transmission through e-mail.
4. Non-HealthWest Networks: Extreme care must be taken when connecting HealthWest equipment to a home or public network. Although HealthWest actively monitors its security status and maintains organization-wide protection policies and procedures to protect its data and systems, HealthWest has no ability to monitor or control the security procedures on non-HealthWest networks.
5. Protect Data in Your Possession: View or access only the information that you have a need to see in the course of performing job duties assigned to you. Regularly review the data you have stored to ensure that client data is as accurate and up to date as possible and that old data is eliminated or archived, as appropriate, as soon as possible. Electronic data should only be stored on the HealthWest network or within HealthWest systems. It should not be permanently stored on portable devices, including but not limited to laptops.
6. Hard Copy Reports or Work Papers: Never leave paper records displaying PHI around your work area. Lock all paper records in a file cabinet at night and put all paper records away or turn over when you leave your work area. PHI in your possession is your responsibility and should not be available where others have access or are able to otherwise view the data.
7. Data Entry When in a Public Location: To the greatest extent possible, do not perform work tasks which require the use of sensitive organizational or client level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you. If working in a public area becomes necessary, ensure that others are not able to view the organizational or client information with which you are working.
8. Sending Data Outside HealthWest: All external transfers of patient data must be associated with an official contract, appropriate Business Associate Agreement, and/or existing, current release of information signed by the client(s) whose data will be shared.

F. Information Security Incidents

All users must immediately report to the IT Department any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc. If the incident involves client data, the Privacy Officer must also be notified.

An incident may be any event that affects the confidentiality, integrity, or availability of agency or client information based in any electronic systems or networks. Reportable incidents may include known or suspected breaches of security, unusually slow or

improper workstation or system operation, unusual or repeated system crashes, or other out-of-the-ordinary workstation or system behaviors.

Examples of information security incidents may include (but are not limited to):

- An employee, intern, temporary worker, or contracted individual or organization viewing protected information in a database the individual is not authorized to access under HealthWest policy.
- An employee, intern, temporary worker, or contracted individual or organization downloading software which is not permitted under the Information System User Policy.
- Intrusion of a HealthWest system by an unauthorized third party (“hacker”) within which Patient Health Information (PHI) resides. In this situation, there would be an assumption that there was a probable access or loss of confidential patient information.
- An unauthorized third party ("hacker") using a falsified username and password to gain access to HealthWest Information Systems.
- An unauthorized third party seeking HealthWest Information System access control or other information by pretending to be an individual authorized to obtain such information ("Social Engineering").
- An unauthorized third party ("hacker") who acquires access to any HealthWest system or device by any means or method.
- An email or other communication purporting to be from an authorized party seeking Protected Information or information potentially useful in obtaining Information System access ("phishing").
- A software virus or worm ("malware") interfering with the functioning of HealthWest-owned computers which are part of an Information System and which may also result in a compromise of the infected system by a remote “hacker”, etc.

G. Saving Files

- All PHI or other sensitive information must be stored in secure server environments only, as in a directory on a HealthWest secure network file server. PHI and other sensitive information should not be stored on hard drives or portable drives/media when the HealthWest network, or other appropriate HealthWest system, is accessible. The only exception to allowing PHI or other sensitive information to be saved on a local hard drive is when staff must work in a situation where there is no capability of connecting to the HealthWest network, or appropriate HealthWest system, such as when Wi-Fi and cell service/hotspot are not available. In the event that PHI or other sensitive information must be temporarily retained locally to a device, workforce members shall be responsible for the protection from improper use or disclosure of all PHI or other sensitive information. At the earliest time that the HealthWest network or appropriate system becomes available, all data is to be

moved from the device's local drive to the agency network / system, ensuring no PHI remains on the device's local storage, including in the "trash bin".

- Any file that is created outside of the HealthWest Electronic Health Record (EHR) system, and contains an individual client's PHI, must be uploaded to the HealthWest EHR system in its final format at the earliest time that access to the EHR is available. If there is a question or concern about a file being appropriate for EHR storage, the Client Information Manager or Director of Health Information Services should be consulted. If it is determined the file is not appropriate for EHR storage, but it contains an individual's PHI, the file must be saved to the network drive denoted by the letter H:, within the directory entitled "client," then within the subdirectory titled with the client ID number relating to the file being saved.
- Any file that needs to be saved in its original format, and that contains the PHI of multiple clients, must be saved to the network drive denoted by the letter H:, within the appropriate directory/subdirectory hierarchy of that network drive. In this case, the appropriate "save location" will vary depending on the purpose of the file as well as who needs access to it. For example, there are various teams and programs that utilize shared lists containing multiple clients and those individuals' associated data. Case in point, if "Team X" has a list of clients and points of data important to that teams' "ABC Project", they must save that file on the H: drive but have options of where to save within that network drive. Based on the purpose in this example case, those staff may choose to save the file within the "Team X" folder, then within the "ABC Project" folder from there. Good judgment should be used in the file save process. If a staff questions where a file should be saved, he/she should consult with his/her supervisor. If technical questions or needs are involved, the Information Technology department may also be sought out for advice and assistance.
- In the case that a file needs to be saved, but does not contain client-related PHI, and you are the only individual who needs access to the file, that file should be saved to the network drive denoted by the letter I:. Each staff person is allotted server file storage space for his/her specific work purposes. Since data and information stored in the "I: drive" is intended for only your specific use, you may utilize your preferred file storage method within this network drive/location (folders, file names, etc.). Even though this network location is provided for each person's own, individual use, it should be understood that any file, of any type, in any location on the HealthWest network, is available and accessible to the appropriate agency personnel for such reasons as audit, supervision, corporate compliance, security, and FOIA, among others.
- No file should be stored directly beneath the network drive denoted by the letter "H:". Files should be stored in an appropriate directory/subdirectory hierarchy described in the points above.
- In cases where there are existing Business Associate Agreements (BAA) between HealthWest and outside entities for purposes of collaborative work, and there is a need to share files, including the potential for PHI, secure,

encrypted storage locations/methods will be utilized where appropriate rights to the data can be managed. Examples of this include, but may not be limited to, HealthWest's managed SharePoint site, the HealthWest Google Suite, and File Transfer Protocol (FTP).

- The only cloud-based storage that should be utilized for housing PHI or other sensitive information relating to HealthWest business would be under contract for HealthWest use. Under contract, this would be considered part of the HealthWest network and/or the HealthWest system to which the storage relates to, and therefore, acceptable for storage of this information. Typically, a cloud-based storage situation for HealthWest purposes would be through the use of a vendor-hosted system. For example, the HealthWest Latitude43/Peter Chang Enterprises (PCE) Electronic Health Record (EHR) offers the options of self-hosting or cloud. HealthWest chose the cloud option for its purposes. This would fall under the umbrella of the term cloud-based storage as well as "under contracted use by" HealthWest. In the case of housing PHI, HealthWest would also have a BAA in place for the system/storage being utilized. For any other situation, the Corporate Compliance Officer, HIPAA Officer, and Director of Information Systems should be consulted to determine appropriateness and acceptability of that specific situation.

H. Intimidating or Retaliatory Acts

Any individual who provides assistance with HIPAA compliance and any regulatory officials or investigations, shall not be subjected to intimidation or retaliatory acts by HealthWest, per HIPAA Privacy Rule §164.530(g).

Any individual who provides assistance with regulatory compliance (aka corporate compliance), and any regulatory officials or investigations, shall not be subjected to intimidation or retaliatory acts by HealthWest.

I. Confidentiality Agreement

Users of HealthWest Information Resources understand that abiding by this agreement is a condition of employment. If breach of any provision of this agreement shall occur, the individual may be subject to civil or criminal liability and/or disciplinary action consistent with applicable HealthWest policies, contracts, and processes. Temporary workers and third-party employees (i.e., contracted individuals and organizations) must also abide by this agreement and may also be subject to civil or criminal liability, as well as termination of any employment, work agreement, or contract that exists between the worker and the HealthWest agency.

IV. ENFORCEMENT

Any employee, vendor, client, intern, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

V. POLICY REVIEW AND APPROVAL

HealthWest management performs a periodic review of this policy. Based on the review, HealthWest management may change this policy to reflect its intentions and compliance requirements.

HEALTHWEST

RECIPIENT RIGHTS ADVISORY COMMITTEE MEETING MINUTES

Friday, October 13, 2023
8:00 a.m.
376 E. Apple Ave., Muskegon, MI 49442

CALL TO ORDER

The regular meeting of the Recipient Rights Advisory Committee was called to order by Chair Hardy at 8:49 a.m.

ROLL CALL

Members Present:	Janet Thomas, Tamara Madison, Cheryl Natte, Thomas Hardy
Members Absent:	Janice Hilleary
HealthWest Staff Present:	Gina Post, Shannon Morgan, Cyndi Blair, Amber Berndt, Rich Francisco, Linda Wagner, Christy LaDronka, Heather Wiegand, Brian Speer, Gary Ridley, Randi Bennett, Mike Kimble, Chelsea Kirksey, Pam Kimble, Melina Barrett
Guest Present:	Kristen Wade, John Weerstra

APPROVAL OF MINUTES

It was moved by Ms. Madison, seconded by Ms. Thomas, to approve the minutes of the August 11, 2023 meeting as written.

MOTION CARRIED.

ITEMS FOR CONSIDERATION

A. Motion to Accept Recipient Rights Reports for August 2023 / September 2023

It was moved by Ms. Thomas, seconded by Ms. Madison, to approve the Recipient Rights Reports for August 2023 / September 2023.

MOTION CARRIED.

For the months of August 2023 / September 2023, there were 64 HealthWest and 28 provider employees trained:

Rights Updates HealthWest	45
Rights Updates Provider	1
New Employee Training HealthWest/Contracted	13
New Employee Training Provider	14
SUD Recipient Rights Orientation Employee	1
SUD Recipient Rights Orientation Provider	2

For the months of August 2023 / September 2023 there were 737 incident reports and 35 rights allegations.

Statistical data showing type and code was provided in the enclosed report.

There were a total of 8 deaths reported in August 2023 / September 2023.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATIONS

There was no communication.

DIRECTOR'S COMMENTS

There was no Director's Comments.

AUDIENCE PARTICIPATION / PUBLIC COMMENT

There was no audience participation.

ADJOURNMENT

There being no further business to come before the committee, the meeting adjourned at 9:11 a.m.

Respectfully,

Thomas Hardy
HealthWest Rights Advisory Committee Chair

TH/hb

PRELIMINARY MINUTES
To be approved at the Rights Advisory Committee Meeting of
December 1, 2023

HealthWest
Muskegon's Behavioral Wellness Connection

RECIPIENT RIGHTS ADVISORY COMMITTEE

October 13, 2023 – 8:00 a.m.

376 E. Apple Ave. Muskegon, MI 49442
Zoom: https://healthwest.zoom.us/j/92247046543?pwd=ZXY0QnFPVGc5UVZENlRwcExTTmdvdz09
Join by Phone: (312) 626-6799, 92718779426#

Recipient Rights Committee Chair: Thomas Hardy
Recipient Rights Committee Vice-Chair: Vacant

AGENDA

1)	Call to Order	Quorum
2)	Approval of Agenda	Action
3)	Approval of the Minutes of August 11, 2023 (Attachment #1 – pg. 1-2)	Action
4)	Public Comment (on an agenda item)	
5)	Items for Consideration	
	A) Motion to Accept Recipient Rights Bi-Monthly Report for August 2023 / September 2023 (Attachment #2 – pg. 3-12)	Action
6)	Old Business	
7)	New Business	
8)	Communication / Director's Report	
	A) Training Recipient Rights Complaint Process and Appeal - Linda Wagner, Recipient Rights Officer (Attachment #3 – pg. 13-19)	Information
	B) Director's Report – Rich Francisco, Executive Director	Information
9)	Audience Participation / Public Comment	
10)	Adjournment	Action

/hb

HEALTHWEST

RECIPIENT RIGHTS ADVISORY COMMITTEE MEETING MINUTES

Friday, August 11, 2023
8:00 a.m.
376 E. Apple Ave., Muskegon, MI 49442

CALL TO ORDER

The regular meeting of the Recipient Rights Advisory Committee was called to order by Vice Chair Hardy at 8:26 a.m.

ROLL CALL

Members Present: Janice Hilleary, Janet Thomas, Tamara Madison, Cheryl Natte, Thomas Hardy

HealthWest Staff Present: Holly Brink, Tasha Percy, Shannon Morgan, Cyndi Blair, Amber Berndt, Melina Barrett, Rich Francisco, Linda Wagner, Suzanne Beckeman, Gordon Peterman, Justine Belvitch, Justine Tufts

Guest Present: Kristen Wade, John Weerstra

APPROVAL OF MINUTES

It was moved by Ms. Natte, seconded by Ms. Hilleary, to approve the minutes of the June 9, 2023 meeting as written.

MOTION CARRIED.

ITEMS FOR CONSIDERATION

A. Motion to Accept Recipient Rights Reports for June 2023 / July 2023

It was moved by Ms. Thomas, seconded by Ms. Hilleary, to approve the Recipient Rights Reports for June 2023 / July 2023.

MOTION CARRIED.

For the months of June 2023 / July 2023, there were 91 HealthWest and 24 provider employees trained:

Rights Updates HealthWest	64
Rights Updates Provider	1
New Employee Training HealthWest/Contracted	19
New Employee Training Provider	18
SUD Recipient Rights Orientation Employee	8
SUD Recipient Rights Orientation Provider	5

For the months of June 2023 / July 2023 there were 791 incident reports and 23 rights allegations.

Statistical data showing type and code was provided in the enclosed report.

There were a total of 8 deaths reported in June 2023 / July 2023.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATIONS

There was no communication.

DIRECTOR'S COMMENTS

Rich Fracisco, Executive Director, gave an update regarding the recent completion of his Recipient Rights training required by MDHHS. His completion of this training maintains our compliance with MDHHS.

AUDIENCE PARTICIPATION / PUBLIC COMMENT

Mr. John Weerstra questioned if there were any investigation open past 90 days. Our Recipient Rights Officer, Linda Wagner, confirmed that we do not have any investigations still open past 90 days.

ADJOURNMENT

There being no further business to come before the committee, the meeting adjourned at 8:38 a.m.

Respectfully,

Thomas Hardy
HealthWest Rights Advisory Committee Vice Chair

TH/hb

PRELIMINARY MINUTES
To be approved at the Rights Advisory Committee Meeting of
October 13, 2023

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE	BUDGETED	NON-BUDGETED	PARTIALLY BUDGETED
Recipient Rights Advisory Committee	X		

REQUESTING DIVISION	REQUEST DATE	REQUESTOR SIGNATURE
Administration	October 13, 2023	Linda Wagner, Recipient Rights Officer

SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)

Approval is requested to accept the Recipient Rights Reports of August 2023 and September 2023. The report includes:

- Training sessions conducted by the Rights Office from August 1, 2023 through September 30, 2023.
- Site Reviews from August 8, 2023 through September 15, 2023.
- Incident Reports and Rights Allegations for August 1, 2023 through September 30, 2023.
- Formal Complaints and Interventions for August 1, 2023 through September 30, 2023.
- Deaths reported for July 31, 2023 through September 21, 2023.

SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)

I move to approve the Recipient Rights Reports for the months of August 1, 2023 through September 30, 2023.

COMMITTEE DATE	COMMITTEE APPROVAL
October 13, 2023	_____ Yes _____ No _____ Other
BOARD DATE	**BOARD APPROVAL**
October 27, 2023	_____ Yes _____ No _____ Other

HWB 5-R

BI-MONTHLY RECIPIENT RIGHTS REPORT

Date: **October 13, 2023**

To: **Recipient Rights Advisory Committee**

From: **The Office of Recipient Rights**

Subject: **Recipient Rights Report for August and September**

I. TRAINING

A. August 3-4, 2023, Recipient Rights Officers Association of Michigan Training provided, 7.25 Category IV CEU's for Lawrence O. Spataro, Linda K. Wagner and Amanda M. Absher.

B. August 8, 2023, Rights Update for 11 Muskegon Recovery Center SUD Cherry Health employees.

C. August 9, 2023, New Employee Training for 6 HealthWest and 5 Provider employees.

D. August 11, 2023, Rights Update for 15 HealthWest employees.

E. August 23, 2023, New Employee Training for 1 HealthWest and 4 Provider employees.

F. August 23, 2023, Rights Update for 11 HealthWest employees.

G. September 6, New Employee Training for 1 HealthWest and 2 Provider employees.

H. September 8, 2023, Rights Update for 19 HealthWest and 1 Provider employees.

I. MDHHS-ORR Conference Training, 9.75 CEU's category I, 5 CEU's category III, 4.5 CEU's category IV, 11 Social Work CEU's for Linda K. Wagner, RRO and for Amanda M. Absher, RRA, 9.75 CEU's category I, 5 CEU's category III, 1.5 Category II, 3 CEU's category IV.

J. September 25, 2023, SUD Orientation for 1 HealthWest and 2 Provider employees.

K. September 27, 2023, New Employee Training for 5 HealthWest and 3 Provider employees.

64 HealthWest and **28** Provider employees were trained for the months of August and September.

II. SITE REVIEWS

A. August 8, 2023, Terra Nova residential DD MOKA Non-Profit Services Corp.

B. August 14, 2023, DayBreak Adult Day Services, Adult CLS Services, Day Springs Inc.

C. August 22, 2023, Kelly's Kare AFC, residential DD, Kelly's Kare Inc .

D. August 22, 2023, Kelly's Kare Community Program, Adult CLS Services, Kelly's Kare Inc .

E. August 24, 2023, Beacon Home at Morton Terrace, residential mixed, Beacon Specialized Living Services.

F. August 25, 2023, Beacon Home at Lakeview Mannor, residential mixed, Beacon Specialized Living Services.

G. August 25, 2023, Graceland residential DD MOKA Non-Profit Services Corp.

H. September 14, 2023, Brookmere, residential DD MOKA Non-Profit Services Corp.

I. September 15, 2023, Superior Care, residential mixed, Greatlakes Regional Care Inc.

III. STATISTICAL INFORMATION

The Office of Recipient Rights received **737** incident reports and **35** rights allegations for the months of August and September. Provided for your review is the statistical data showing type and location.

IV. FORMAL INVESTIGATIONS

Old Business:

A. July10, 2023, Wraparound outpatient HealthWest during a Wraparound meeting on June 22, 2023, Community Living Supports was not offered to the family or discussed as an option even when it was brought up as an SED service array. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The staff received additional training.**

B. July10, 2023, Wraparound outpatient HealthWest on June 29, 2023, the family requested therapeutic foster care which is an SED Waiver service. The family was told therapeutic foster care is not an available service. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

C. July10, 2023, Wraparound outpatient HealthWest residential treatment was recommended by the HealthWest team. A referral to Psychiatric Residential Treatment Facility (PRTF) was requested. The Recipient's mother was told that PRTFs do not exist in Michigan. Although this is true, PRTF is a Medicaid covered level of care when it is medically necessary. When a provider is not available in network, the CMH must look out of network and even out of state in order to secure services. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

D. July10, 2023, Wraparound outpatient HealthWest during a Wraparound meeting on June 22, 2023, family was told Medicaid does not provide transportation to medical appointments to minors. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

E. July10, 2023, Wraparound outpatient HealthWest during a Wraparound meeting on June 22, 2023, the family was told HealthWest does not have available respite providers. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

F. July10, 2023, Wraparound outpatient HealthWest the family lacks a Person Centered Plan that addresses the needs for this family in all life domains. The Recipient could be released from detention after violently attacking his mother. There is no plan to ensure his psychiatric stability or the safety of the youth or the family. The family is in crisis after experiencing significant trauma. The needs of siblings after experience family trauma must also be considered. Current IPOS does not address known risks or aggression, violence, emotional deregulation, elopement, threats of violence in the community, property destruction, or symptoms which could be considered psychotic in nature. The intensity and severity of needs are not addressed with appropriate amount, scope, and duration, because of the lack of clarity around severity of need, interventions are not appropriate to condition, For example, interventions such as jumping jacks and ripping phone books discussed in June 22, 2023, Wraparound meeting are not adequate interventions 1) when the mom has stated they have not worked in the past and 2) youth can quickly deregulate to the point of no longer being able to maintain emotional control. **The investigation into the allegation of WRITTEN PLAN OF SERVICE (PERSON-CENTERED PLANNING) is not substantiated.**

G. July 10, 2023, Wraparound outpatient HealthWest the family lacks a Safety Plan/Crisis Plan that addresses the needs of this family. The Recipient could be released from detention after violently attacking his mother. The family is in crisis after experiencing trauma. The needs of the youth, the younger siblings, and the mother must be considered especially after they experience significant family trauma. There were many unsafe situations that led to hospitalizations and placement in detention. The safety plan does not address known risks or aggression, violence, emotional deregulation, elopement, threats of violence in the community, property destruction, or

symptoms which could be considered psychotic in nature. The family needs a Safety Plan/Crisis plan that takes into account: -The triggers (situations, circumstances) that have resulted in the consumer/family experiencing a crisis in the past -Past signs, symptoms, prodromal, behaviors, observations, changes that have served as indicators of a potential crisis -What has been effective in reducing the severity of the crisis in the past -What could lead to a crisis and what supports could be provided to prevent or assist the consumer/family with the crisis -How to ensure safety of younger siblings during risk of violence. **The investigation into the allegation of WRITTEN PLAN OF SERVICE (PERSON-CENTERED PLANNING) is not substantiated.**

H. July 10, 2023, Wraparound outpatient HealthWest the CANS/CAFAS scoring is lower than what is documented in the comments sections of each category. The scoring of the CAFAS is unclear. There were many unsafe situations that led to hospitalizations and placement in detention. Risks include aggression, violence, safety of younger siblings, emotional deregulation, elopement, threats of violence in the community and at school, property destruction, or symptoms which could be considered psychotic in nature. In many circumstances, even when these risks are documented in comments, the scoring remained a 0 or 1 even though there are extreme behaviors and significant needs. **The investigation into the allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

I. July10, 2023, Wraparound outpatient HealthWest Independent Facilitation was not offered to the family as required even though it is an essential element of the person centered planning process per the MDHHS BEHAVIORAL HEALTH AND DEVELOPMENT DISABILITIES ADMINISTRATION PERSON-CENTERED PLANNING PRACTICE GUIDELINE. When the family requested independent facilitation, the family was told by wraparound facilitator. The family was told by HealthWest Staff that HealthWest does not have services that allow families to utilize the choice voucher to hire their own employees, however wraparound is not a service that can be vouchered. **The investigation into the allegation of WRITTEN PLAN OF SERVICE (PERSON-CENTERED PLANNING) is not substantiated.**

J. July 21, 2023, Muskegon Merriam Launch Pad DD Day Program MOKA Non-Profit Services Corp. the Recipient was on an outing in Rockford at the Rockford Dam Overlook under the care of two Staff. The Recipient was in a wheelchair for his outing for unknown reasons as the Recipient is able to walk and does not usually use a wheelchair. Staff had parked the Recipient at the top of an incline with his brakes locked. While Staff were assisting the others, another Recipient unlocked the Recipient's brakes, and he rolled down the incline and fell into the reeds and water getting the Recipient wet and dirty. **The allegation of SAFE, SANITARY AND HUMANE TREATMENT ENVIRONMENT is SUBSTANTIATED. All MOKA employees working with the person served will review their plan prior to working with them. Persons served will use only medical equipment that is assigned to them in accordance with their plan. Employee Staff 1 will receive a written reprimand for not following a person's served plan which will include coaching on; only using**

medical equipment that is in the person served plan and only MOKA employees can assist persons served with the medical equipment Employee Staff 2 received a documented verbal coaching about medical equipment usage requirements to include only using medical equipment that is in the person served plan and only MOKA employees can assist persons served with the medical equipment.

New Business:

A. August 8, 2023, Morton Terrace mixed residential Beacon Specialized Living Services. Staff left their shift without approval, leaving the home out of staff to recipient ratio. **The allegation of NEGLECT III is SUBSTANTIATED. The staff voluntarily resigned from her position with Beacon Specialized Living.**

B. August 8, 2023, out of county Maple Cottage, Turning Leaf Residential Rehabilitation Services during a group the Recipient told Staff that he and another Staff argued because the Recipient asked the other Staff for a glass of milk. The argument escalated to the point the Other Staff told the Recipient, 'to shut up and leave her alone.' I told Will I would talk to him later about it when the group was over. **The investigation into the allegation of DIGNITY AND RESPECT is substantiated. Staff was removed from this location and were given a written reprimand.**

C. August 8, 2023, Riverwood residential DD Pioneer Resources the Recipient was videotaped and you could hear the staff person call out her name. Staff was also heard saying that if she threw a glove box at her she would harm her and called the Recipient a b--ch. **The investigation into the allegation of ABUSE III is substantiated**. **The staff was terminated.** During the investigation a secondary complaint was discovered for **Disclosure of Confidential Information that is substantiated. The staff left employment with Pioneer Resources.**

D. August 11, 2023, ABA Playground other Pioneer Resources a Staff had a hard grip on a Recipient. The Staff would have been facing the Recipient holding on to her left forearm pulling with her body weight. The Recipient was verbally distressed. **The allegation of MENTAL HEALTH SERVICES SUITED TO CONDITION is SUBSTANTIATED. The staff received additional training.**

E. August 11, 2023, Community Living Supports Services provided by Preferred Employment and Living Services CLS Services CLS Staff and the Recipient had made plans to meet the Recipient's friend in the parking lot to pass off some movies that she was selling on FB. The CLS Staff began screaming at the Recipient saying, "you can't go out of my sight". **The investigation into the allegation of DIGNITY AND RESPECT is substantiated. The staff was removed from working with the Recipient and received additional training.**

F. August 22, 2023, Sophia Home residential DD MOKA Non-Profit Services Corp. Recipient went missing from the group of his housemates and staff while exiting the Unity

Christian Music Festival. He was later found by Police and returned to the group. **The investigation into Safe, Sanitary, and Humane Treatment Environment is substantiated. Staff received a written reprimand, additional training on Individual Plans of Service and is enrolled to repeat his Recipient Rights Training.**

G. August 25, 2023, Black Creek Cove residential DD HGA Support Services. Recipient was seen by HealthWest RN because it appeared that she had a significant weight loss and malnutrition. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The staff were retrained on the proper documentation requirements.** During the investigation it was discovered that staff had falsified food acceptance logs. Therefore, **the investigation into NEGLECT-CLASS III was also substantiated. The staff was counseled on proper documentation requirements and received a written reprimand.**

H. August 29, 2023, Crescent Home, residential DD MOKA Non-Profit Services Corp. Two recipients were at the IHOP with one staff person. The staff person took one recipient to the restroom, leaving the other man sitting at the table alone. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

I. September 1, 2023, Recipient Receiving Adult Outpatient Services from HealthWest stated he was wrongfully discharged from the Crisis Residential Unit. (CRU) because he was still a danger to himself. Staff at the CRU became angry with him which made him feel uncomfortable. When he later met criteria for readmission, they stated he was not allowed to come back because he did not participate in groups of which he was not aware of and stated the only group's flyer he had seen was from May 19. Then he had informed CRU staff that he had meetings at Muskegon Family Care; originally they approved these appointments but when he was leaving, they told him he was not allowed to leave because he had an appointment with the HealthWest Doctor in "two minutes. **The investigation of DIGNITY AND RESPECT is not substantiated. The investigation of SERVICES OF MENTAL HEALTH PROFESSIONAL is not substantiated.** During the investigation it was discovered that it was not made clear to the Recipient that group attendance was expected while at CRU. Therefore, **there was an investigation into MENTAL HEALTH SERVICES SUITED TO CONDION and this was substantiated. Staff will be retrained and a new system for alerting recipients of expectations was put in place.**

J. September 5, 2023, JBC Home, residential mixed, The RN was looking into the Recipients meds and contacted the pharmacy to verify last time med was sent to home. The Recipient's med has not been refilled since January, but the home has been marking it passed on the MAR. The Doctor sent in new refills in June 2023. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The corrective action plan is pending.**

K. September 5, 2023, JBC Home, residential mixed, September 5, 2023. The nurse received an email from the Home Supervisor at JBC on 9/1/2023 at 3:14pm stating that she needed

a refills for the Recipient. The nurse reviewed the chart, and this Recipient has not been seen for a medication review since 4/19/2023 where medications were sent with 2 refills. This nurse reviewed when these medications were last filled, which was on 6/23/23 for a 30 day supply. This means that the last dosage the Recipient would have received would have been around 7/23/2023. The nurse emailed the Home Supervisor back that a medication review would need to be scheduled. The nurse then called the home and asked that documentation be provided to show when the last time these medications were passed with the current cartages it is being dispensed from. This information was discussed with the HealthWest IDD Supervisor and reported to the appropriate agencies. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. Home manager/staff will cross check all medications to ensure all medications are accounted for and properly documented according to administration. Provide staff with required trainings for medication administration and Rights training. Change their system of medication administration, cross check each medication to MARS daily/weekly. Consult with HW nurses monthly to ensure medications to MARs are accurate. Communicate with HW nurses and SC when appointments are missed or have not been scheduled.**

L. September 5, 2023. A Recipient receiving Adult IDD Services, at HealthWest stated that a HealthWest Staff is taking his check and giving it away to some kid. He says that HealthWest is the representative payee. **The investigation of Abuse, Class II – Exploitation is not substantiated.**

M. September 7, 2023, Recipient receiving Adult Outpatient Services complained because his HealthWest Staff did not inform him that there would be a person shadowing her during his appointment. He does not like the way that his HealthWest Staff speaks to him and does not feel that she is listening to him. **The investigation of DIGNITY AND RESPECT is not complete.**

N. September 7, 2023, Grand Street Home, residential mixed, Cornerstone AFC, Van Buren CMH's ORR reported they were told that a staff person slept in the same bed as a female resident at Cornerstone AFC. The staff's last day was August 26 and Cornerstone has been unable to reach her since. HealthWest's Recipient is no longer staying in the home; she is now living in a SIL. **The investigation of DIGNITY AND RESPECT is not substantiated.**

O. September 7, 2023, JBC Home, residential mixed, The RN received the MARs from the home manager for the Recipients. There were discontinued meds signed for and still on the MAR and med order was not correct on the MAR. One Recipient had almost 2 months' worth of meds when he should have had 90 for the month For all the residents in the home, it seems they are not following the 5 r's when passing meds and making sure that they are utilizing the MAR while the med pass is happening instead, they are signing for the meds at the end of their shift. For another Recipient, he missed meds for 3 days because the medication was not refilled in a timely manner and utilizing a med box for

passing medications. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The corrective action plan is pending.**

P. September 12, 2023, Crescent Home, residential DD MOKA Non-Profit Services Corp. A Staff working with another Staff on second shift at the Crescent home reported that the when she was in the office charting the other Staff went out into the garage to get something out for dinner. The first Staff said that she overheard the second Staff provoked the Recipient about dinner. Then later the first Staff observed the second Staff hit the Recipient on his hand/arm area. **The investigation of ABUSE CLASS II-UNREASONABLE FORCE is not substantiated.**

Q. September 13, 2023, Anchor Pointe, residential mixed, A Home Staff alleges that two staff members frequently call the recipients in the home names, including, "stupid" and "retard". **The investigation of DIGNITY AND RESPECT is not complete.**

R. September 14, 2023, Crescent Home, residential DD MOKA Non-Profit Services Corp. Two staff took 6 recipients out for lunch and inadvertently left one of the recipients behind when they left. The restaurant called the police, and they contacted the home and staff went back and picked up the Recipient. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The corrective action is pending.**

S. September 15, 2023, Crescent Home, residential DD MOKA Non-Profit Services Corp. A family member alleges that Staff did not follow Recipients Individual Plan of Service. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITION is not complete.**

T. September 28, 2023, Slocum Home, residential DD MOKA Non-Profit Services Corp. Staff were outside vaping while a recipient was left alone in the bathroom with no gait belt which violates his IPOS. **The investigation of MENTAL HEALTH SERVICES SUITED TO CONDITON is not complete.**

V. INTERVENTIONS

Old Business: None

New Business:

A. August 25, 2023, Lakeview Mannor residential mixed Beacon Specialized Living Services. Staff was upset and hit a glass off the table, and it went flying. He then through a menu book. Neither was directed at the recipient. **This was not a code protected right and will be addressed by the Home Manger.**

B. September 25, 2023, Mararebecah Home, residential mixed, Samaritas. A family member arranged a trip for a Recipient and sent a check to be cashed for funds for

the trip. The check was never cashed. When the staff transported the Recipient for the trip she told the family member that she put her own money in to gas up the vehicle. **This is not a code protected right. Contact was made with the Regional Director of Samaritas and the family member. The Regional Director for Samaritas said that they will address the families concerns.**

VI. SUBSTANCE USE DISORDER

Old Business: None

New Business: None

VII. DEATHS

A. July 31, 2023, a 37 year old female recipient receiving IDD Adult Supports Coordination case management HealthWest died of Cancer while on Hospice.

B. August 11, 2023, a 68 year old male recipient receiving MI Adult Community Based Services, died from Chronic COPD.

C. August 16, 2023, a 62 year old male recipient living at the Lilac Home, residential DD, HGA Support Services, died at Trinity Health from natural causes after being removed from life support.

D. August 26, 2023, a 33 year old male recipient living in the community, receiving SUD Services from HealthWest, died at Trinity Health from Cardiac Arrest, secondary to a Fentanyl drug overdose.

E. August 31, 2023, a 62 year old male recipient who was homeless who received HealthWest Services with the LEAD team died in the community from exposure.

F. September 5, 2023, a 48 year old female recipient living in the community who received HealthWest Services with the LEAD team died in her home of a unknown cause.

G. August 19, 2023, a 68 year old male recipient MI Adult Supports Coordination case management HealthWest died of an unknown cause.

H. September 21, 2023, a 58 year old female recipient living at the Riverwood Home residential DD, Pioneer Resources died at Trinity Health after a choking incident.

HEALTHWEST

Policy and Procedure

No. 04-022

Prepared By:

Effective: February 2, 1988
Revised: January 20, 2022

The Office of Recipient Rights

Approved By:

Subject: Recipient Rights Complaint Process and Appeals

Julia B. Rupp

Julia B. Rupp, Executive Director

I. POLICY

The Office of Recipient Rights of HealthWest will ensure that all rights complaints are responded to within 5 business days, investigated when appropriate and that all those with a right to appeal will be notified of the right to appeal or choose mediation.

II. PURPOSE

To ensure that rights complaints and appeals are responded to in accordance with the requirements of the Mental Health Code and Administrative Rules.

III. APPLICATION

All mental health programs, services and facilities operated by or under contract with HealthWest.

IV. DEFINITIONS

A. **Allegation:** An assertion of fact made by an individual that has not yet been proved or supported with evidence.

B. **Appeals Committee:** The Recipient Rights Advisory Committee as appointed by the Board of HealthWest to hear appeals.

C. **Appellant:** The recipient, complainant, parent, or guardian who appeals a recipient rights finding or a respondent's action to the Appeals Committee.

D. **Complainant:** An individual who files a rights complaint.

E. **Intervention:** To act on behalf of a recipient to obtain resolution of an allegation of a rights violation contained in a complaint, through processes other than investigation, as defined by the Mental Health Code. Interventions are not allowed in allegations of abuse,

neglect, serious injury, or death of a recipient involving an apparent or suspected rights violation.

F. **Investigation:** A detailed inquiry into and systematic examination of an allegation raised in a rights complaint.

G. **Mediation:** A private, informal dispute resolution process in which an impartial, neutral individual, in a confidential setting, assists parties in reaching their own settlement of issues in a dispute and has no authoritative decision-making power.

H. **Not Substantiated:** A determination by the Recipient Rights Officer/Advisor that an allegation was not able to be proved based on the preponderance of evidence.

I. **Preponderance of Evidence:** The greater weight of evidence, not as to quantity but as to quality.

J. **Remedial Action:** If, through investigation, a right has been determined to have been violated, the respondent shall take appropriate remedial action that corrects or provides a remedy for the rights violation, is implemented in a timely manner and attempts to prevent a recurrence of the rights violation.

K. **Rights Complaint:** A written or oral statement that contains all of the following information: A statement of allegations that give rise to the dispute; A statement of the right or rights that may have been violated; the outcome that the complainant is seeking as a resolution to the complaint.

L. **Substantiated:** A determination by the Recipient Rights Officer/Advisor that an alleged violation of a right was proven to have occurred by the preponderance of the evidence.

V. COMPLAINT PROCEDURES

A. The Recipient Rights Officer/Advisor will ensure that recipients, parents of minors, guardians and others have ready access to complaint forms.

B. Each rights complaint shall be recorded upon receipt by the Office of Recipient Rights on a complaint log and each rights complaint shall be date stamped.

C. An acknowledgment of the recording in V.B. shall be sent along with a copy of the complaint to the complainant within five (5) business days.

D. Within five (5) business days after the Office of Recipient Rights receives a complaint, it shall notify the complainant if it determines that no investigation of the rights complaint is warranted.

E. The Office of Recipient Rights shall assist the recipient or other individual with the complaint process as necessary.

1. The Office of Recipient Rights shall advise the recipient or other individual that there are advocacy organizations available to assist in preparation of a written rights complaint and shall offer to refer the recipient or other individual to those organizations.

2. In the absence of assistance from an advocacy organization, the Office of Recipient Rights shall assist in preparing a written rights complaint, which will contain a statement of the allegation, the right allegedly violated, and the outcome desired by the complainant.

3. The Office of Recipient Rights shall inform the recipient or other individual of the option of mediation and that it is available at any time after the Office of Recipient Rights completes the investigative report.

F. If a rights complaint has been filed regarding the conduct of the Executive Director, the rights investigation shall be conducted by the Recipient Rights Office of another community mental health services program or by the state office of recipient rights as decided by the Board.

G. The Office of Recipient Rights shall initiate investigation of apparent or suspected rights violations in a timely and efficient manner.

1. Subject to delays involving pending action by external agencies (law enforcement, MDHHS), The Office of Recipient Rights shall complete the investigation not later than ninety (90) days after it receives the rights complaint.

2. Investigation shall be initiated immediately in cases involving alleged abuse, neglect, serious injury, or the death of a recipient involving an apparent or suspected rights violation.

H. Investigation activities for each rights complaint shall be accurately recorded by the Office of Recipient Rights on the complaint log.

I. The Office of Recipient Rights shall determine whether a right was violated by using the preponderance of the evidence as its standard of proof.

J. The Office of Recipient Rights shall issue a written report every thirty (30) calendar days during the course of the investigation. The report shall be submitted to the complainant, the respondent, and the Executive Director. A status report shall include all of the following:

1. Statement of the allegations.

2. Statement of the issues involved.

3. Citations to relevant provisions of the Mental Health Code, rules, policies, and guidelines.

4. Investigative progress to date.

5. Expected date for completion of the investigation.

K. Upon completion of the investigation, the Office of Recipient Rights shall submit a written investigative report to the respondent and to the Executive Director. Issuance of the written investigative report may be delayed pending completion of investigations that

involve external agencies (law enforcement, DHHS). The report shall include all of the following:

1. Statement of the allegations.

2. Statement of the issues involved.

3. Citations to relevant provisions of the Mental Health Code, rules, policies, and guidelines.

4. Investigative Findings.

5. Conclusions.

6. Recommendations, if any.

L. On substantiated rights violations, the respondent shall take appropriate remedial action that meets all of the following requirements:

1. Corrects or provides a remedy for the rights violation.

2. Is implemented in a timely manner.

3. Attempts to prevent a recurrence of the rights violation.

M. The remedial action shall be documented and made a part of the record maintained by the Office of Recipient Rights.

N. The Executive Director or her designee shall submit a written summary report to the complainant and recipient, if different than the complainant, or his/her legal representative within 10 business days after the Executive Director receives a copy of the investigative report. The summary report shall include all of the following:

1. Statement of allegations.

2. Statement of issues involved.

3. Citations to relevant provisions of the Mental Health Code, rules policies, and guidelines.

4. Summary of investigative findings.

5. Conclusions.

6. Recommendations made by the Office of Recipient Rights.

7. Action taken, or plan of action proposed, proposed by the respondent.

8. If the summary report contains a plan of action the Executive Director will send a letter indicating when the action was completed and include the recipient rights appeal process.

9. A statement describing the complainant's, the recipient's if different than the complainant, or his/her legal representative's right to appeal and the grounds for appeal.

O. Information in the summary report shall be provided within the constraints of the confidentiality/privileged communications sections (748, 750) of the Mental Health Code.

P. Information in the summary report shall not violate the rights of any employee (ex. Bullard-Plawecki Employee Right To Know Act).

Q. HealthWest and each service provider under contact with it shall ensure that appropriate disciplinary action is taken against those who have engaged in abuse or neglect.

R. Administrative action will be taken if either HealthWest or provider personnel fail to report suspected violations of rights.

S. The Office of Recipient Rights shall comply with Muskegon County Personnel Rules and contracts to assure that investigations are conducted in a manner that did not violate employee rights.

T. The Office of Recipient Rights will ensure that rights complaints filed by recipients or anyone on their behalf were received in a timely manner.

VI. APPEAL/DISPUTE RESOLUTION PROCEDURES

A. The Recipient Rights Advisory Committee has been appointed by the Board to act as the Appeals Committee.

B. A member of the Appeals Committee who has a personal or professional relationship with an individual involved in an appeal shall abstain from participating in that appeal as a member of the committee.

C. The complainant, the recipient if different than the complainant, or her/his legal representative in the summary report from the Executive Director/designee, will be informed of the following:

1. The complainant, recipient if different than the complainant, or her/his legal representative may file a written appeal with the Appeals Committee not later than forty-five (45) days after the receipt of the summary report.

2. An appeal shall be based on one of the following grounds:

a. The investigative findings of the Office of Recipient Rights are not consistent with the facts or with law, rules, policies, or guidelines.

b. The action taken or plan of action proposed by the respondent does not provide an adequate remedy.

c. An investigation was not initiated on a timely basis.

D. The Office of Recipient Rights shall advise the appellant there are advocacy organizations available to assist the appellant in preparing the written appeal and shall offer to refer the complainant to those organizations.

E. In the absence of assistance from an advocacy organization, the Office of Recipient Rights shall assist the appellant in meeting the procedural requirements of a written appeal.

F. The Office of Recipient Rights shall inform the appellant of the option of mediation.

G. Within five (5) business days after the receipt of the written appeal, members of the Appeals Committee shall review the appeal to determine whether it meets the criteria described above.

H. If the appeal is denied because the criteria were not met, the appellant shall be notified in writing within the five (5) business day period.

I. If the appeal is accepted, written notice shall be provided to the appellant within the five (5) business day period.

J. If the appeal is accepted, a copy of the appeal shall be provided to the respondent and the Executive Director within the five (5) business day period.

K. Within thirty (30) days after receipt of a written appeal, the Appeals Committee shall meet and review the facts as stated in all complaint investigation documents and shall do one of the following:

1. Uphold the investigative findings of the Office of Recipient Rights and the action taken or plan of action proposed by the respondent.

2. Return the investigation to the Office of Recipient Rights and request that it be reopened or reinvestigated.

3. Uphold the investigative findings of the Office of Recipient Rights but recommend that the respondent take additional or different action to remedy the violation.

4. Recommend that the Board request an external investigation by the State Office of Recipient Rights.

L. The Appeals Committee shall document its decision in writing.

M. Within ten (10) working days after reaching its decision, it shall provide copies of the decision to the respondent, appellant, recipient if different than the appellant, or his/her legal representative the Executive Director and the Office of Recipient Rights.

N. Copies of the Appeals Committee's decision shall include a notice of the appellant's right to appeal to MDHHS within forty-five (45) days from the receipt of their decision and include the grounds for further appeal, which consist of the investigative findings of the

Office of Recipient Rights are not consistent with the facts or with law, rules, policies, or guidelines.

O. If an investigation is returned to the appeals committee for reinvestigation, upon receipt of the Report of Investigative Findings (RIF), the Executive Director will take appropriate remedial action and will submit a written summary report to the complainant, recipient, if different than the complainant, parent or guardian, and the appeals committee within 10 business days.

P. If a request for additional or different action is sent to the Executive Director, a response will be sent within 30 days as to the action taken or justification as to why it was not taken. The response will be sent to the complainant, recipient, if different than the complainant, parent or guardian, and the appeals committee.

Q. If the committee notifies the CMH Board Chair of a recommendation to seek an external investigation from MDHHS-ORR, the Board will send a letter of request to the Director of MDHHS-OOR within 5-business days of receipt of the request from the appeals committee. The Director of the CMH making the request will be responsible for the issuance of the summary report, which will include information on the grounds for appeal, the time frame for submission for the appeal, advocacy organizations that may assist and an offer of assistance by the ORR in the absence of assistance from an advocacy organization.

VII. REFERENCES

M.C.L. 330.1722, 330.1752, 330.1774, 330.1776, 330.1780, 330.1782, 330.1784 330.1788 and 330.1788.

Bullard-Plawecki Employee Right to Know Act, Act No. 397 of the Public Acts of 1978, M.C.L. 423.501 et. seq.

LS/ab