

HEALTHWEST

PROGRAM/PERSONNEL MEETING MINUTES

**April 12, 2024
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, Tamara Madison, Thomas Hardy, John Weerstra

Members Absent: Janice Hilleary

Staff Present: Holly Brink, Gina Post, Amber Berndt, Rich Francisco, Brandy Carlson, Susan Plotts, Linda Wagner, Gary Ridley, Kristi Chittenden, Tasha Kuklewski, Jennifer Hoeker, Justine Belvitch, Mickey Wallace, Gary Ridley, Gordon Peterman, Anissa Goodno, Jackie Farrar, Melina Barrett, Gina Kim, Lakshmee Persuad

Guests Present: Kristen Wade

MINUTES

It was moved by Mr. Hardy, seconded by Ms. Thomas, to approve the minutes of the February 12th 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 approve the HealthWest Policy and Procedure for Background Checks effective April 26, 2024.

MOTION CARRIED.

It was moved by Mr. Hardy, seconded by Ms. Thomas, to approve the policy and procedural changes as described above and attached, effective April 29, 2024.

MOTION CARRIED.

It was moved by Mr. Hardy, seconded by Ms. Thomas, to approve the policy and procedural changes as described above and attached for 05-025 Information System Use, effective April 29, 2024.

MOTION CARRIED.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATION

There was no communication.

DIRECTOR'S COMMENTS

Executive Director, Rich Francisco, provided an update:

Mr. Francisco share that that him and Cyndi met with MDHHS director, Donata Kidd, to touch base on projects that overlapped with them. One is an update on the MichiCANS soft launch, MDHHS is now doing their soft launch and pilot and are not doing the MichiCANS prescreen. They are completing MichiCANS for kids entering the foster care system, and if a referral is made to HW it will be routed to us via CC360. Upon the completion of their assessment, we will be keeping our eye on the prescreens referred to our CMH. The other discussion we had was surrounding the Medicaid enrollment process, and Donata was going to look more into the various cases where we have individuals that are dropping off from DAB to other fund sources. She is going to look for systemic issues on their end. In the meantime, she wants HW to escalate cases to her to investigate further.

Staff are busy preparing for CARF now that we have a date set for May 15 to 17th. Policies are being reviewed and sent out for updates and as you saw we are taking new and significantly changed policies to the board for approval as well.

I have been working with the County and Foster Swift (corporate counsel) on developing a countywide HIPAA policy and that is now completed. I have sent it to Mark Eisenbarth and other county directors for review. This would allow the different departments to be on the same page for various requests that we receive for PHI. This should define some of the parameters about what we can and cannot share and should make the sharing of information more efficient as we coordinate care with these departments.

Lastly, I am currently working with staff and the communications team on updating the Annual Plan and the Strategic Plan. I will be taking that to the full board at the end of the month for updates.

AUDIENCE PARTICIPATION

There was no audience participation.

ADJOURNMENT

There being no further business to come before the board, the meeting adjourned at 8:10 a.m.

Respectfully,

Cheryl Natte
Program/Personnel Committee Chair

CN/hb

***PRELIMINARY MINUTES
To be approved at the Program/Personnel Committee Meeting on
June 14th, 2024***



PROGRAM AND PERSONNEL COMMITTEE

**Friday, April 12, 2024
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 February 9, 2024
(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 Procedure for
Background Checks
(Attachment #2 – pg. 3 – 11) | Action |
| | B) Authorization to Approve the HealthWest Policy and Procedure
Changes to Policy 10-005 Provider Conflict of Interest
(Attachment #3– pg. 12 –16) | Action |
| | C) Authorization to Approve the HealthWest Policy and Procedure
Changes to Policy 05-026 Information System Use Policy
(Attachment #2 – pg. 17 – 66) | Action |
| 6) | Old Business | |
| 7) | New Business | |
| 8) | Communication | |
| | A) Director's Update – Rich Francisco | Information |
| 9) | Audience Participation / Public Comment | |
| 10) | Adjournment | Action |

/hb

Main Office

376 E. Apple Ave. | Muskegon, MI 49442 | P (231) 724-1111 | F (231) 724-3659

HealthWest.net

HEALTHWEST
PROGRAM/PERSONNEL MEETING MINUTES

February 9, 2024
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, Tamara Madison, Thomas Hardy, Janice Hilleary, John Weerstra

Staff Present: Holly Brink, Shannon Morgan, Amber Berndt, Rich Francisco, Gary Ridley, Kristi Chittenden, Tasha Kuklewski, Jennifer Hoeker, Kim Davis, Gina Kim, Cyndi Blair

Guests Present: Kristen Wade

MINUTES

It was moved by Mr. Hardy, seconded by Ms. Hilleary, to approve the minutes of the December 1, 2023 meeting as written.

MOTION CARRIED.

PUBLIC COMMENT (ON AN AGENDA ITEM)

There was no public comment.

ITEMS FOR CONSIDERATION

It was moved by Mr. Hardy, seconded by Ms. Hilleary, to approve the HealthWest Network Procurement Plan that was created on September 29, 2023.

MOTION CARRIED.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATION

There was no communication.

DIRECTOR'S COMMENTS

Executive Director, Rich Francisco, provided an update:

The MichiCANS soft launch is progressing well and will place HealthWest in a good position for the hard launch. The soft launch site has completed over 150 assessments, utilizing MichiCANS and our staff currently participating in the soft launch has completed the training. HealthWest has also submitted a total number of staff to be trained prior to Hard Launch of MichiCANS for Oct. 1, 2024:

- Combined with Adult (depending on how the 18-21 old population is defined):
 - Clinical-92
 - Supervisor-20
 - Leadership-9

The submission of the CCBHC renewal grant has been submitted thanks to the finance team grants division and CCBHC leads in getting this submitted. This is the 3rd year continuation of this CCBHC grant. On top of the CCBHC demonstration status HealthWest has, we still get additional grant funding from SAMHSA for the CCBHC expansion grant for about 1M to help support and continue our efforts with CCBHC.

AUDIENCE PARTICIPATION

There was no audience participation.

ADJOURNMENT

There being no further business to come before the board, the meeting adjourned at 8:06 a.m.

Respectfully,

Cheryl Natte
Program/Personnel Committee Chair

CN/hb

PRELIMINARY MINUTES
To be approved at the Program/Personnel Committee Meeting on
April 12, 2024

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE Program/Personnel Committee	BUDGETED X	NON-BUDGETED	PARTIALLY BUDGETED
REQUESTING DIVISION Administration	REQUEST DATE April 12, 2024	REQUESTOR SIGNATURE Susan Plotts, HR Manager	
<u>SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)</u>			
<p>HealthWest Board authorization is requested to approve the HealthWest Policy and Procedure for Background Checks.</p> <p>HealthWest will not employ, independently contract with, allow volunteer/student observer/intern access, or grant clinical privileges to an individual with a criminal conviction disclosed through a criminal background check required by law, if the individual will regularly have direct access to or provide direct services to clients, and the individual is prohibited by law from having access or performing services due to a criminal conviction. Criminal background checks will occur prior to date of hire or contract initiation, and minimally every two years thereafter. HealthWest may employ, independently contract with, or grant clinical privileges to an individual who has been convicted of a felony or misdemeanor if: (a) the individual is not prohibited by law from having direct access to or performing direct services for clients due to the criminal conviction, and (b) HealthWest has determined the criminal record is not substantially related to the position. HealthWest shall require all providers who employ staff to have policies outlining the completion of required background checks. The policies and procedures shall meet personnel selection criteria required by law, and other universal requirements for all staff that deliver services to individuals served within the HealthWest network. During quarterly reviews, HealthWest will verify background checks are completed and maintained by Provider Agencies.</p> <p>The purpose of this policy is to ensure HealthWest and its contracted providers conduct both criminal and exclusionary background checks as required by law and as required under contracts with the Michigan Department of Health and Human Services (MDHHS), the Lakeshore Regional Entity, and as required by specific funding sources.</p>			
<u>SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)</u>			
I move to authorize and approve the HealthWest Policy and Procedure for Background Checks, effective April 29, 2024.			
COMMITTEE DATE April 12, 2024	COMMITTEE APPROVAL _____ Yes _____ No _____ Other		
BOARD DATE April 26, 2024	BOARD APPROVAL _____ Yes _____ No _____ Other		

HWB 66-P

HEALTHWEST
POLICY / PROCEDURE

No. (Insert number)

Prepared by: _____ Effective: April ____, 2024

Susan Plotts, Human Resources Manager

Approved by: _____ Subject: Background Checks

Rich Francisco, Executive Director

I. POLICY

HealthWest will not employ, independently contract with, allow volunteer/student observer/intern access, or grant clinical privileges to an individual with a criminal conviction disclosed through a criminal background check required by law, if the individual will regularly have direct access to or provide direct services to clients, and the individual is prohibited by law from having access or performing services due to a criminal conviction. Criminal background checks will occur prior to date of hire or contract initiation, and minimally every two years thereafter. HealthWest may employ, independently contract with, or grant clinical privileges to an individual who has been convicted of a felony or misdemeanor if: (a) the individual is not prohibited by law from having direct access to or performing direct services for clients due to the criminal conviction, and (b) HealthWest has determined the criminal record is not substantially related to the position. HealthWest shall require all providers who employ staff to have policies outlining the completion of required background checks. The policies and procedures shall meet personnel selection criteria required by law, and other universal requirements for all staff that deliver services to individuals served within the HealthWest network. During quarterly reviews, HealthWest will verify background checks are completed and maintained by Provider Agencies.

II. PURPOSE

To ensure HealthWest and its contracted providers conduct both criminal and exclusionary background checks as required by law and as required under contracts with the Michigan Department of Health and Human Services (MDHHS), the Lakeshore Regional Entity, and as required by specific funding sources.

III. APPLICATION

This policy applies to HealthWest employees, volunteers, student interns/observers, and licensed independent contractors who provide direct services.

IV. PROCEDURE

A. Definitions

1. Staff – employees, interns, volunteers, students, and contractors

B. Required Background Checks

1. Background checks required for all staff:
 - a) State Criminal Record Background Check, using ICHAT (Internet Criminal History Access Tool System)
 - b) National Criminal Background Check (requires fingerprints) – anyone who has lived outside of Michigan anytime during the 5 years prior to starting at HealthWest.
 - c) Sanctions Checks
 - ii. Office of Inspector General (OIG)
 - iii. Systems for Awards Management (SAM)
 - iv. Medicaid/Medicare Sanction Provider List (MSP)
 - d) Recipient Rights Checks
 - e) Michigan Driving Record Check
 - f) Michigan Sex Offender Registry
 - g) National Sex Offender Registry
2. Additional background checks required for specialty areas:
 - a) Workforce Background Check - for employees working in the Crisis Residential Unit
 - b) Central Registry Checks – for staff working under the MI Kids Now Grant

C. Criminal Background Checks

1. Upon a formal offer, the applicant will fill out form [A158](#) Background Check Information Consent Form to grant permission for formal background checks to be ran.
2. State Criminal History Record Check
HealthWest and its contracted providers shall complete and maintain criminal and exclusionary background checks for all employees, potential employees, and independently contracted staff that provide direct services to individuals, have access to the records or money of individuals served through the provider network, and/or are responsible for billing services within the Provider Network. Criminal background checks will be ran through the state's Internet Criminal History Access Tool (iCHAT) system before hire and minimally every two (2) years for all staff.
3. National Criminal History Record Check
If a potential employee or contractor has lived outside of Michigan within the last five (5) years, a national background check shall be conducted by the provider. This will require fingerprinting.
4. Workforce Background Check

Adult Foster Care Provider initial criminal background checks shall be in accordance with State of Michigan licensing requirements. Criminal background checks for employees and applicants of adult foster care facilities (AFC) and homes for the aged facilities are conducted in the Michigan Workforce Background Check Program. Notice of new criminal records are provided automatically for those checks conducted in the Michigan Workforce Background Check Program. HealthWest requires Crisis Residential staff to be re-fingerprinted through a Workforce Background Check approved vendor every five (5) years.

5. Determination of Outcome of Criminal Background Check

The information obtained from criminal background checks will be used to evaluate a person's qualifications to provide approved services for individuals. If a conviction appears in the criminal background check, it may mean that the prospective or current staff member is precluded from performing the essential functions of the services purchased by HealthWest.

The following precludes the staff from providing services to individuals served by HealthWest:

- a) Has been convicted of any of the following felonies:
 - i. Medicaid/Medicare fraud
 - ii. Convicted of any of the following felonies, attempt or conspiracy to commit the following felonies – unless 15 years have lapsed since all the terms and conditions of sentencing, parole and probation are completed:
 - Intent to cause death or serious impairment of a body function, that results in death or serious impairment of body function, involves use of force or violence, or involves the threat of the use of force or violence.
 - Cruelty or torture
 - Felonies under MCL 750.145m to 750.145r (definitions of adult foster care and vulnerable adults)
 - Criminal sexual conduct
 - Abuse or neglect
 - Use of a firearm or dangerous weapon
 - Diversion or adulteration of a prescription drug or other medications
- b) A felony, attempt, or conspiracy to commit a felony other than Medicaid/Medicare fraud or a felony listed above – unless 10 years have lapsed since the terms and conditions of sentencing, parole and probation are completed.
- c) Has been convicted of any of the following misdemeanors:
 - i. Convicted of any misdemeanors involving the following – unless 10 years have lapsed since all the terms and conditions of sentencing, parole and probation are completed:
 - Use of a firearm or dangerous weapon with the intent to injure, the use of a firearm or dangerous weapon that results in a personal injury or a misdemeanor involving the use of force or violence or the threat of the use of force or violence.
 - Misdemeanors under MCL 750.145m to 750.145r (definitions of adult foster care and vulnerable adults)

- Criminal sexual conduct
 - Cruelty or torture
 - Abuse or neglect
- ii. Convicted of any misdemeanors involving the following – unless 5 years have lapsed since all the terms and conditions of sentencing, parole and probation are completed:
- Cruelty if committed by an individual who is less than 16 years old
 - Home invasion
 - Embezzlement
 - Negligent homicide or a violation of MCL 257.601d of Michigan vehicle code
 - Larceny if committed over age of 16
 - Retail fraud in second degree if committed over age of 16
 - Assault, fraud, theft or the possession or delivery of a controlled substance if committed over the age of 16
- iii. Convicted of any misdemeanors involving the following – if committed within the last 3 years:
- Assault if there was no use of a firearm or dangerous weapon and no intent to commit murder or inflict great bodily injury
 - Retail fraud in third degree if committed over age of 16
 - Misdemeanors under MCL 333.7401 to 333.7461 (drugs such as controlled substances, narcotics, etc.)
- iv. Convicted of any misdemeanors involving the following – if committed within the year immediately preceding application for employment or independent contract:
- Misdemeanors under MCL 333.7401 to 333.7461 (drugs such as controlled substances, narcotics, etc.) if conviction before age of 18
 - Larceny or retail fraud in second or third degree if conviction before age 16
- d) Is the subject of an order or disposition under the code of criminal procedure with a finding of “not guilty by reason of insanity”.
- e) Had a substantiated finding of neglect, abuse, or misappropriation of property by a state or federal agency in a nursing facility or skilled nursing facility.
- f) Individuals providing applied behavior analysis services must not have any felony or misdemeanor convictions.

If the results of the criminal and exclusionary background investigation show no criminal record identified, the employment process may proceed.

If the results of the criminal check show a finding that does not fit within the identified exclusionary findings above, the results will be brought forward to a HealthWest Executive Team Member for review and approval or denial.

HealthWest may employ, independently contract with, or grant clinical privileges to an individual who has been convicted of a felony or misdemeanor if: (a) the individual is not prohibited by law from having direct access to or performing direct services for clients due to the criminal conviction, and (b) HealthWest has determined that the

criminal record is not substantially related to the position. HealthWest shall document the review and determination which may be requested during quality monitoring reviews.

D. Medicaid/Medicare Sanctioned Provider List (MSP), Office of Inspector General (OIG), and System for Award Management (SAM) Exclusion Checks

1. HealthWest shall complete and maintain Medicaid/Medicare Exclusion background checks by conducting an examination of Federal and State databases of excluded parties and litigation checks from SAM, OIG, and MSP. Such examinations must take place prior to time of hiring or contract and at least monthly thereafter. HealthWest performs these checks through EPStaffCheck.
2. Determination of Outcome of Medicaid/Medicare Exclusion Background
Individuals presently excluded from participation in Medicaid/Medicare, or any other Federal health care program, may not provide services within the HealthWest Provider Network. The HealthWest Human Resources Manager and/or Provider Network Manager must be notified, in writing, of exclusion as soon as it is identified.

E. Recipient Rights Background Check

1. HealthWest will complete and maintain recipient rights checks for all employees, potential employees, and contracted staff (independent contractors) that provide direct services to individuals. This is done through the HealthWest Recipient Rights Main Database (or equivalency). Recipient Rights checks must be completed at the time of hire or contracting.
2. Rights checks done through HealthWest are completed by submitting the background consent form to the Recipient Rights Office, who then checks the Recipient Rights Main Database. Results are then returned to Human Resources staff.
3. Determination of Outcome of Recipient Rights Background
 - a) Individuals with substantiated Abuse I, Abuse II, Neglect I, or Neglect III violations may not provide services to Individuals served by a provider in the HealthWest Network without a formal review of circumstances and timeframe of the violation, and without the written consent of either the HealthWest Executive Director if the individual is a HealthWest staff or the appropriate approving staff from the Provider Agency.
 - b) If an employee of a provider agency starts services with a consumer of HealthWest prior to completion of background checks and it is found that the employee has a record with Recipient Rights that prohibits employee from working with a HealthWest consumer, claims submitted will not be paid.

F. Driving Record Check

1. HealthWest shall complete initial driving record checks prior to start date for all individuals that may transport individuals served by HealthWest. HealthWest uses the Secretary of State subscription service for continuous driving record monitoring.
2. Determination of Outcome of Driving Record Check.

The information obtained from driving record checks will be used to evaluate an individual provider's qualifications to provide approved transportation for Individuals. If certain offenses appear on the driving record check, it may mean that the prospective or current provider is precluded from transporting individuals served by HealthWest.

- a) One or more of the following offenses in the past three years may preclude one from providing transportation:
 - Any alcohol or drug related violation including driving or operating under the influence, driving with an open container, minor in possession of alcohol or any drug crime.
 - Reckless driving
 - Careless driving
 - Speed contest (Illegal Racing)
 - Hit and run
 - Permitting an unlicensed person to drive
 - Aggravated assault with a motor vehicle
 - Driving while license is suspended or revoked
 - Operating a motor vehicle for the commission of a felony
 - Fleeing or evading police or roadblock or resisting arrest
 - Manslaughter or negligent homicide using a motor vehicle
 - Failure to report an accident
 - Illegal passing of a school bus
3. Employees must have a valid license to be employed at HealthWest. If their license is suspended while employed, the employee must inform Human Resources immediately. They must also inform Human Resources if any of the above infractions occur while employed or contracted. The infraction will be reviewed, and further action will be determined by human resources and executive leadership.

G. Michigan and National Sex Offender Registry

1. Sex offender registry checks will be done for HealthWest staff and minimally for licensed, certified and/or registered provider Agency staff per the MDHHS Credentialing and Recredentialing requirements using both the Michigan Sex Offender Registry and the United States Department of Justice National Sex Offender Public website.
2. Determination of the Outcome of the Registry Check
 - a) Results of the registry checks that come back with a hit that do not already fall under the convictions listed in 1. b. above will be sent to the Human Resources Manager for review. If necessary, they will then be sent on to the Chief Clinical Director and/or Executive Director for review and approval/denial.

H. Standard Operation Procedures

Human Resources maintains Standard Operating Procedures explaining the process for conducting background checks and they are available for view upon request.

V. REPORTING

All HealthWest staff are required to report to their Department Head as soon as possible after an incident occurs but no later than five (5) days of a charge, arrest, conviction, or assessment imposition. The Department Head will forward the notice to the HealthWest Human Resources Manager who will forward the report to the Muskegon County Human Resources Director for review. Any Department Head who is arrested or charged for a violation of criminal law will notify the County Administrator. Employees are also required to notify the Department Head, or as appropriate, the Administrator, of any conviction for a violation of criminal law. The Department Head will also provide notice to the Human Resource Manager. Notification by the employee must occur as soon as possible after the incident but no later than five (5) business days after the charge, arrest, or conviction. Conviction includes a plea of guilty and a plea of no contest.

- A. Any criminal conviction, felony, misdemeanor or being placed on any of the violator registries while employed will result in an immediate Group 3 offense per Muskegon County Personnel Rules.
- B. The imposition of civil money penalties or assessments imposed under section 1128 A of the Social Security Act.

HealthWest Human Resources must report offenses as defined in 1128(a) and 1128(b)(1), (2), or (3) of the Social Security Act, or that have had civil money penalties or assessments imposed under section 1128A of the Act to the Lakeshore Regional Entity pursuant to LRE Policy 9.11.

VI. ATTACHMENTS

- A. Background Check Information Consent Form (A158) – [Laserfiche Forms](#)
- B. HR SOP 1 – Background Checks
- C. HR SOP 2 – Secretary of State Subscription Service
- D. HR SOP 4 – Driver License Tracking
- E. HR SOP 5 – Hiring Process
- F. HR SOP 10 – Access to CHRIS System and CHRI

VII. REFERENCES

- A. [Michigan Medicaid Provider Manual](#)
- B. MDHHS Contract Attachment – [Credentialing and Re-credentialing Processes](#)
- C. Lakeshore Regional Entity Policy 9.11 – [Criminal History Checks](#)
- D. [State of Michigan Contract](#)
- E. [Social Security Act Sec. 1128](#)
- F. [Michigan Sex Offender Registry](#)
- G. [United States Department of Justice National Sex Offender Public website](#)
- H. Public Health Code Act 368 of 1978 ([MCL 333.20173a](#))
- I. [42 U.S. Code 1320a-7](#)
- J. Mental Health Code Act 258 of 1974 section ([MCL 330.1134a](#))
- K. [Code of Federal Regulations Title 42, Chapter V, Subchapter B section 1001.101](#)
- L. Public Health Code 368 of 1978 ([MCL 333.18263](#)) specific to behavior technicians providing ABA services.

(SP/ab)

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE Program/Personnel Committee	BUDGETED X	NON-BUDGETED	PARTIALLY BUDGETED
REQUESTING DIVISION Provider Network Management	REQUEST DATE April 12, 2024	REQUESTOR SIGNATURE Anissa Goodno, Provider Network Specialist	
<u>SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)</u>			
<p>HealthWest Board authorization is requested to approve the revisions of Policy and Procedure 10-005 (Provider Conflict of Interest). The revised sections are listed below and redlined in the attached Policy.</p> <p>Revisions Include:</p> <ol style="list-style-type: none"> 1. Section II Purpose: Expanded on the purpose of the policy. 2. Section IV Definitions: Added definitions for Interested Person and Financial Interest. 3. Section V Procedures: Under B, added number three. 			
<u>SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)</u>			
I move the HealthWest Board of Directors to authorize the policy and procedural changes as described above and attached, effective April 29, 2024.			
COMMITTEE DATE April 12, 2024	COMMITTEE APPROVAL _____ Yes _____ No _____ Other		
BOARD DATE April 26, 2024	BOARD APPROVAL _____ Yes _____ No _____ Other		

HWB 67-P

HEALTHWEST
Policy and Procedure
No. 10-005

Prepared by:

Effective: December 27, 2001

~~2018~~ April 3, 2024

Revised: February 28,

~~Judith E. Cohen~~ Jackie Farrar, Network Manager

Formatted: Highlight

Approved by:

Subject: Provider Conflict of Interest

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

Formatted: Highlight

Formatted: Highlight

I. POLICY

It is the policy of HealthWest to assure all contracted Providers disclose actual and potential conflict of interest and, when actual or potential conflict of interest is identified, assure affected contracted Provider will refrain from further participation in matter(s) to which the conflict relates until the question of conflict has been resolved.

II. PURPOSE

To assure no undisclosed conflict of interest exists in any contractual relationship entered into by HealthWest.

It is important for HealthWest directors, officers, and staff to be aware that both real and apparent conflicts of interest or dualities of interest sometimes occur in the course of conducting the affairs of the agency and that the appearance of conflict can be troublesome even if there is in fact no conflict whatsoever.

Conflicts are undesirable because they potentially or eventually place the interests of others ahead of the corporation's obligations to its purposes and to the public interest. The policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to government organizations.

Formatted: Not Highlight

III. APPLICATION

All contracted Providers of HealthWest.

IV. DEFINITION

Conflict of Interest: All business interests, affiliations, and/or relationships which could have an existing or potential financial or other interest which impairs or might appear to impair that person's independent unbiased judgement when performing responsibilities to HealthWest.

Interested Person: Any director, principal officer, or member of a committee with governing board delegated powers, who has a direct or indirect financial interest, as defined below, is an interested person.

Formatted: Not Highlight
Formatted: Underline, Not Highlight
Formatted: Indent: Left: 0.5", No bullets or numbering

Financial Interest: A person has a financial interest if the person has, directly or indirectly, through business, investment, or family: a. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement, b. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement, or c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement. Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

Formatted: Not Highlight
Formatted: Underline, Not Highlight
Formatted: Indent: Left: 0.5", No bullets or numbering

V. PROCEDURE

- A. HealthWest Network Development staff will assure contract requirements include disclosure of conflict of interest at the time of Provider application/re-application.
- B. HealthWest Administrative staff will:
 - 1. Review contract provider disclosure statements, and
 - 2. Obtain Executive Director and/or Corporate Counsel recommendation for disposition.
 - 3. If it is determined a Conflict of Interest exists, Executive Director with the assistance of Corporate Counsel will decide whether the partnership can occur with an alternative arrangement or should be denied. This determination decision will occur in writing by Executive Director.

Formatted: Not Highlight

~~fee~~JF/hb

HEALTHWEST
Policy and Procedure
No. 10-005

Prepared by:
Jackie Farrar, Network Manager

Effective: December 27, 2001
Revised: April 3, 2024

Approved by:

Subject: Provider Conflict of Interest

Rich Francisco, Executive Director

I. POLICY

It is the policy of HealthWest to assure all contracted Providers disclose actual and potential conflict of interest and, when actual or potential conflict of interest is identified, assure affected contracted Provider will refrain from further participation in matter(s) to which the conflict relates until the question of conflict has been resolved.

II. PURPOSE

To assure, no undisclosed conflict of interest exists in any contractual relationship entered into by HealthWest.

It is important for HealthWest directors, officers, and staff to be aware that both real and apparent conflicts of interest or dualities of interest sometimes occur in the course of conducting the affairs of the agency and that the appearance of conflict can be troublesome even if there is in fact no conflict whatsoever.

Conflicts are undesirable because they potentially or eventually place the interests of others ahead of the corporation's obligations to its purposes and to the public interest. The policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to government organizations.

III. APPLICATION

All contracted Providers of HealthWest.

IV. DEFINITION

Conflict of Interest: All business interests, affiliations, and/or relationships which could have an existing or potential financial or other interest which impairs or might appear to impair that person's independent unbiased judgement when performing responsibilities to HealthWest.

Interested Person: Any director, principal officer, or member of a committee with governing board delegated powers, who has a direct or indirect financial interest, as defined below, is an interested person.

Financial Interest: A person has a financial interest if the person has, directly or indirectly, through business, investment, or family: a. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement, b. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement, or c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement. Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

V. PROCEDURE

- A. HealthWest Network Development staff will assure contract requirements include disclosure of conflict of interest at the time of Provider application/re-application.
- B. HealthWest Administrative staff will:
 - 1. Review contract provider disclosure statements, and
 - 2. Obtain Executive Director and/or Corporate Counsel recommendation for disposition.
 - 3. If it is determined a Conflict of Interest exists, Executive Director with the assistance of Corporate Counsel will decide whether the partnership can occur with an alternative arrangement or should be denied. This determination decision will occur in writing by Executive Director.

JF/hb

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE Program Personnel	BUDGETED X	NON-BUDGETED	PARTIALLY BUDGETED
REQUESTING DIVISION Administration	REQUEST DATE April 12, 2024	REQUESTOR SIGNATURE Randi Bennett, Director of Information Systems	
<u>SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)</u>			
<p>HealthWest Board authorization is requested to make the below changes to HealthWest policy 05-026.</p> <p>Changes Include:</p> <ol style="list-style-type: none"> 1. III., paragraph 2, Updated language to include volunteers as part of the HealthWest workforce required to comply with requirements. 2. III, A.1.b. Added language to reflect requirements for staff who have access to criminal record history information (CHRI). 3. III, A.3.e. Added language to reflect current password requirements (cannot reuse any of the past 24 passwords). 4. III, A.3.i. Added language to reflect current password requirements (cannot contain characters matching 3 or more consecutive characters of username). 5. III, A.3.j. Added language to reflect current password requirements (cannot be changed more than once in any 24-hour period). 6. III, B, paragraph 2, added language to reflect requirements of protecting HealthWest data. 7. III, B.2.d., Added language to reflect current requirements regarding transmission of criminal history record information (CHRI). 8. III, B.2.e., Added language to reflect current requirements regarding communication of criminal history record information (CHRI). 9. III, B.3.b., Added language to provide clarification regarding HealthWest equipment taken offsite. 10. III, B.3.c., Added language to reflect current requirements, and to also provide clarification regarding theft or loss of equipment and reporting of such. 11. III, B.4, paragraph 1 and 2, Added language to clarify protection of applicant and staff criminal history record information (CHRI). 12. III, B.5.d., Updated language to include volunteers as part of the HealthWest workforce under agreement that generated documentation and work is the property of HealthWest. 13. III, B.6.d., Added language to provide clarification as well as add requirements regarding saving of data files. 14. III, B.8., Added language to reflect current requirements regarding certain methods of communication involving criminal history record information (CHRI). 15. III, B.10., Added language within prohibitive activities section to identify that access to criminal history record information (CHRI) is limited to authorized individuals only. 16. III, D., paragraph 1, Added language to include protection of employee/workforce data. 17. III, D., paragraph 7, Added language for clarification of using VPN when working remotely. 18. III, D., paragraph 8, Added language to prohibit storage of criminal history record information (CHRI) on portable devices and to identify reporting requirements when unauthorized access to criminal history record information (CHRI) is suspected. 19. III, D., paragraph 9, Added language for clarification. 20. III, D., paragraph 10, Added language to include physical destruction as a means of destroying protected data. 21. III, D., paragraph 11, Added language for clarification. 22. III, E., paragraph 1, Added language to include workforce as a protected category of information and to also include requirements regarding communication of criminal history record information (CHRI). 23. III, E., paragraph 2, Added language to clarify storage of criminal history record information (CHRI). 24. III, E., paragraph 3, Updated language to include volunteers as part of the HealthWest workforce required to comply with requirements. 25. III, E., paragraph 5, Added language to include criminal history record information (CHRI) as information to be protected. 26. III, D.1., Added language to clarify unacceptable storage locations for criminal history record information (CHRI). 27. III, D.3., Added language to clarify unacceptable use of email for communication of criminal history record information (CHRI). 28. III, D.5., Added language to clarify portable devices as unacceptable means for storing criminal history record information (CHRI). 			

29. III, D.7., Added language to include workforce as a protected category of information.
30. III, D.8., Added language to identify the HealthWest CHRI Security Policy as a resource.
31. III, F., paragraph 1, Added language to reflect requirement to notify LASO in case of suspected security incident involving criminal history record information (CHRI).
32. III, F. paragraph 2, Added definition of criminal history record information (CHRI).
33. III, F., paragraph 3, Added language to include workforce and criminal record history to the description of an incident.
34. III, F., paragraph 4, bullet point 2, Updated language to include volunteers as part of the HealthWest workforce required to comply with requirements.
35. III, F., paragraph 4, bullet point 4, Added language to identify example of criminal history record information (CHRI) security incident.
36. III, G., paragraph 1, Added language to include criminal history record information (CHRI) as a protected category of data and to clarify unacceptable means of storing CHRI.
37. III, G., paragraph 7, Added language for clarification regarding cloud-based storage of data.
38. III, I., Updated language to include volunteers and interns as part of the HealthWest workforce required to comply with requirements.
39. IV. Paragraph 1, Updated language to include volunteers as part of the HealthWest workforce required to comply with requirements.

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 for 05-025 Information System Use, effective April 29, 2024

COMMITTEE DATE April 12, 2024	COMMITTEE APPROVAL _____ Yes _____ No _____ Other
BOARD DATE April 26, 2024	BOARD APPROVAL _____ Yes _____ No _____ Other

HWB 70-P

HEALTHWEST
Policy and Procedure
No. 05-026

Prepared By:

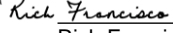
Effective: June 1, 2020

Revised: ~~July 11, 2023~~ April 5, 2024

Randi Bennett
Director of Information Systems

Approved By:

Subject: Information System Use

DocuSigned by:

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, volunteers, 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.

a.B. All workforce members working with criminal history record information or working in areas where criminal history record information is accessible must be authorized to do so.

b.c. 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

Formatted: Indent: Hanging: 0.56"

Formatted: Indent: Left: 1.56", Hanging: 0.56", Right: 0", Space Before: 0 pt, After: 10 pt, Don't add space between paragraphs of the same style, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 2.14" + 2.14"

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 3 + Alignment: Left + Aligned at: 1.58" + Indent at: 2.14"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 2 + Alignment: Left + Aligned at: 1.08" + Indent at: 1.58"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 2 + Alignment: Left + Aligned at: 1.08" + Indent at: 1.58"

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 one of their past 24 passwords. 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.
- i. Passwords cannot contain characters which match 3 or more consecutive characters of the username.
- h-j. Passwords cannot be changed more often than once in any 24-hour period.

B-C. Acceptable Use

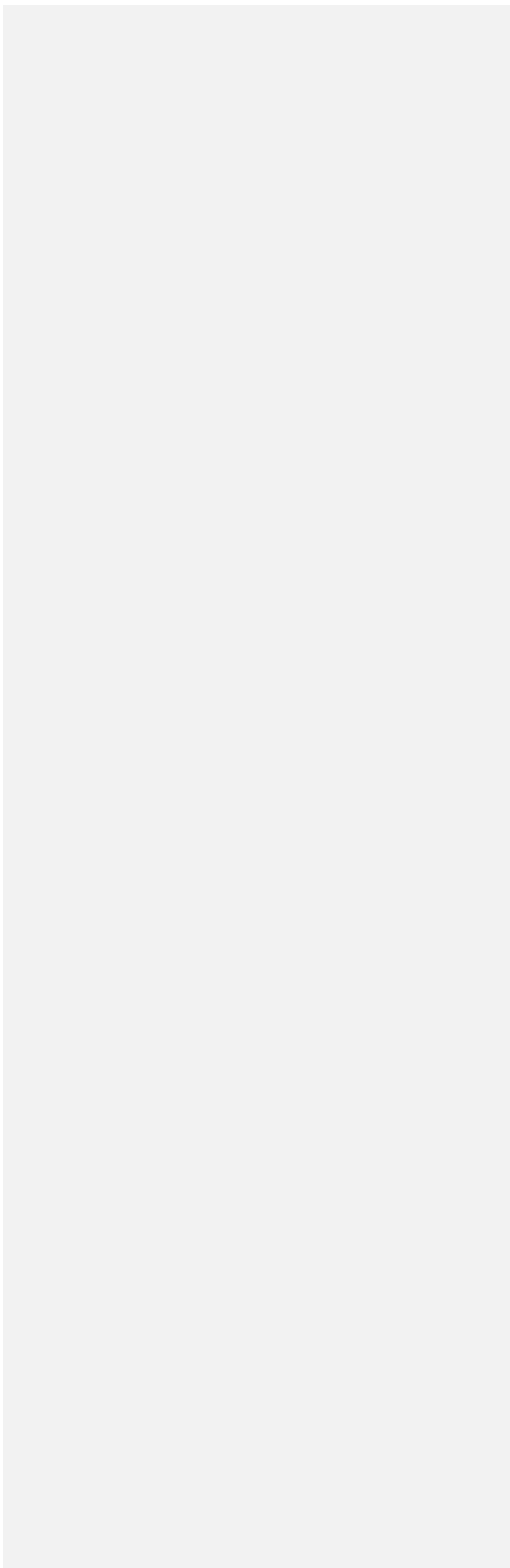
Each employee shall be responsible for all computer transactions that are made with his/her User ID and password, and for the care and security of any computer, device, or hardware assigned to them.

Users shall not knowingly engage in any activity that may be potentially harmful to any portion of the HealthWest network, HealthWest systems, HealthWest data, 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

Formatted: Indent: Left: 1.58", Hanging: 0.42", Right: 0", Space Before: 0 pt, Line spacing: single, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 10 + Alignment: Left + Aligned at: 1.58" + Indent at: 1.83", Tab stops: Not at 2.08" + 2.08"

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.~~ E-mail over the Internet shall not be used for the transmission of criminal record history information (CHRI).

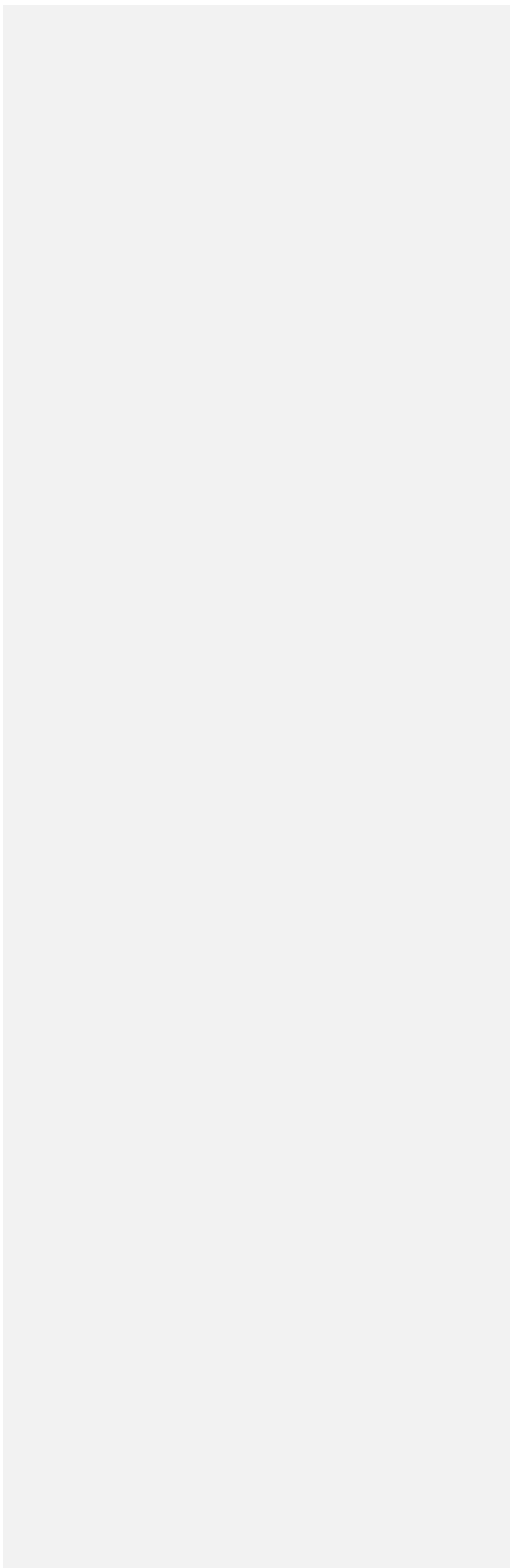
- ~~e-e.~~ Office 365 Suite of products shall not be used to communicate CHRI.

- ~~e-f.~~ 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 that is not intended and used for mobile or approved remote work may not be removed from HealthWest premises without the knowledge and approval of the appropriate department manager and the IT Department. Equipment removed from HealthWest premises for approved remote work and intended to remain offsite for an extended period of time also needs prior approval from 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, CHRI, 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. Where PHI is involved, the HIPAA Privacy Officer must also be notified and where CHRI is involved, the LASO must also be notified.
- 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 and staff criminal record history 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, or criminal record history 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, [volunteers](#), 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) [and/or appropriate HealthWest data storage systems](#). 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. [Criminal history record information \(CHRI\) is never to be stored on the local drive.](#)
 - 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 information, or protected health information, or criminal record history 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 [the](#) 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 ~~that~~[which](#) is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. [HealthWest has access to criminal record history information which is protected by CJIS security policy that limits access to CHRI to only authorized individuals.](#) 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.D. The Internet and e-mail

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-E. Laptops, Portable Devices, and Removable Media

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, [employee/workforce](#), 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.

When working remotely, 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. Criminal record history information should never be stored on a portable device. Unauthorized access, or suspected unauthorized access, to CHRI must be reported to HealthWest's LASO.

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 otherwise confidential, or proprietary, or regulated 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 or physical destruction.

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 or destruction when no longer in use.

E.F. Remote Access or Use of Information

Any and all HealthWest data or information, including but not limited to agency, service, workforce, 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 in compliance with encryption requirements. Criminal record history information must never be transmitted over email and Office 365 Suite of products must never be used to communicate CHRI.

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.

Criminal record history information may never be maintained outside of HealthWest systems or facilities.

Formatted: Indent: Left: 1.13"

Formatted: Indent: Left: 0.06", Right: 0", Space Before: 0 pt, Line spacing: Multiple 1.15 li

Computers used outside of HealthWest facilities by employees, [volunteers](#), 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 [or CHRI](#).

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. [Criminal record history information \(CHRI\) must never be stored outside of appropriate HealthWest systems or identified network locations. Local device storage must never be used for CHRI.](#) 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. [Never send criminal record history information \(CHRI\) via email.](#)
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. [Criminal record history information should never be stored on portable devices for any length of time, even temporarily.](#)
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, [workforce](#), 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. [For purposes of sharing criminal record history information, see HealthWest Criminal Record History Information \(CHRI\) Security Policy.](#)

F-G. 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. [If the incident involves criminal record history information \(CHRI\), the LASO must also be notified.](#)

[Criminal History Record Information \(CHRI\) is information, collected by criminal justice agencies on individuals, which consists of identifiable descriptions and notations of](#)

arrests, indictments, detention, complaints, information, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release, any of which relates to an identifiable person. An incident may be any event that affects the confidentiality, integrity, or availability of agency, criminal history record information, 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.

An incident may be any event that affects the confidentiality, integrity, or availability of agency, workforce, criminal record history, 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, volunteer, 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.
- Intrusion of a HealthWest system by an unauthorized third party within which Criminal Record History Information (CHRI) resides. In this situation, there would be an assumption that there was a probable access or loss of CHRI relating to job applicants and/or staff, current or past.
- 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.

Formatted: Not Expanded by / Condensed by

G-H. Saving Files

- All PHI, CHRI, 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. CHRI should never be stored on hard drives or portable drives/media. 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 [for the intended purpose under which the contract exists](#). 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.I. 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.

H.J. 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, [volunteers](#), [interns](#), 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, [volunteer](#), intern, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

Policy and Procedure
Information System Use
No. 05-026
Page 20 of 19

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

Policy and Procedure

No. 05-026

Prepared By:

Effective: June 1, 2020

Revised: April 5, 2024

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, volunteers, 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. All workforce members working with criminal history record information or working in areas where criminal history record information is accessible must be authorized to do so.
- c. 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 one of their past 24 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.
- i. Passwords cannot contain characters which match 3 or more consecutive characters of the username.
- j. Passwords cannot be changed more often than once in any 24-hour period.

C. 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 data, 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. Personal₄₈ use of a limited nature is allowed but must not

compromise the integrity of HealthWest's systems or workplace productivity.

Policy and Procedure
Information System Use
No. 05-026
Page 5 of 19

- 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. E-mail over the Internet shall not be used for the transmission of criminal record history information (CHRI).
- e. Office 365 Suite of products shall not be used to communicate CHRI.
- f. 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.

Policy and Procedure
Information System Use
No. 05-026
Page 6 of 19

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 that is not intended and used for mobile or approved remote work may not be removed from HealthWest premises without the knowledge and approval of the appropriate department manager and the IT Department. Equipment removed from HealthWest premises for approved remote work and intended to remain offsite for an extended period of time also needs prior approval from 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, CHRI, or other sensitive information. Report should be made to the worker's direct supervisor, the Information Technology department, and the Corporate Compliance Officer. Where PHI is involved, the HIPAA Privacy Officer must also be notified and where CHRI is involved, the LASO must also be notified.
- 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 and staff criminal record history 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, private, or criminal record history 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, volunteers, 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) and/or appropriate HealthWest data storage systems. 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. Criminal₁ history record information (CHRI) is never to be

stored on the local drive.

- 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 information, protected health information, or criminal record history 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 the 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 that is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. HealthWest has access to criminal record history information which is protected by CJIS security policy that limits access to CHRI to only authorized individuals. 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.

D. The Internet and e-mail

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.

E. Laptops, Portable Devices, and Removable Media

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, employee/workforce, 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.

When working remotely, 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. Criminal record history information should never be stored on a portable device. Unauthorized access, or suspected unauthorized access, to CHRI must be reported to HealthWest's LASO.

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 otherwise confidential, proprietary, or regulated 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 or physical destruction.

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 or destruction when no longer in use.

F. Remote Access or Use of Information

Any and all HealthWest data or information, including but not limited to agency, service, workforce, 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 in compliance with encryption requirements. Criminal record history information must never be transmitted over email and Office 365 Suite of products must never be used to communicate CHRI.

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. ⁵⁹

Criminal record history information may never be maintained outside of HealthWest systems or facilities.

Policy and Procedure Information System Use

No. 05-026

Page 15 of 19

Computers used outside of HealthWest facilities by employees, volunteers, 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 set up 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 or CHRI.

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. Criminal record history information (CHRI) must never be stored outside of appropriate HealthWest systems or identified network locations. Local device storage must never be used for CHRI. 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. Never send criminal record history information (CHRI) via email.
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. Criminal record history information should never be stored on portable devices for any length of time, even temporarily.
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, workforce, 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. For purposes of sharing criminal record history information, see HealthWest Criminal Record History Information (CHRI) Security Policy.

G. 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. If the incident involves criminal record history information (CHRI), the LASO must also be notified.

Criminal History Record Information (CHRI) is information, collected by criminal justice agencies on individuals, which consists of identifiable descriptions and notations of

arrests, indictments, detention, complaints, information, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release, any of which relates to an identifiable person. An incident may be any event that affects the confidentiality, integrity, or availability of agency, criminal history record information, 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.

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

Policy and Procedure
Information System Use
No. 05-026
Page 17 of 19

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, volunteer, 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.
- Intrusion of a HealthWest system by an unauthorized third party within which Criminal Record History Information (CHRI) resides. In this situation, there would be an assumption that there was a probable access or loss of CHRI relating to job applicants and/or staff, current or past.
- 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.

All PHI, CHRI, 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. CHRI should never be stored on hard drives or portable drives/media. 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 for the intended purpose under which the contract exists. 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.

I. 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.

J. 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, volunteers, interns, 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, volunteer, intern, or contractor found to have violated this policy may be subject to disciplinary and/or legal action.

Policy and Procedure
Information System Use
No. 05-026
Page 20 of 19

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.

RB/hb

HEALTHWEST

RECIPIENT RIGHTS ADVISORY COMMITTEE MEETING MINUTES

**Friday, February 12, 2024
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 8:11 a.m.

ROLL CALL

Members Present: Janet Thomas, Tamara Madison, Cheryl Natte, Thomas Hardy, John Weerstra

Members Absent: Janice Hilleary

HealthWest Staff Present: Rich Francisco, Holly Brink, Gina Post, Brandy Carlson, Kristi Chittenden, Susan Plotts, Anissa Goodno, Linda Wagner, Tasha Kuklewski, Lakshmee Persaud, Mickey Wallace, Melina Barrett, Gordon Peterman, Amber Berndt, Jackie Farrar, Justin Belvitch, Gina Kim, Gary Ridley, Jennifer Hoeker

Guest Present: Kristen Wade

APPROVAL OF MINUTES

It was moved by Ms. Natte, seconded by Ms. Thomas, to approve the minutes of the February 9, 2024 meeting as written.

MOTION CARRIED.

ITEMS FOR CONSIDERATION

A. Motion to Accept Recipient Rights Reports for February 2024 / March 2024

It was moved by Ms. Natte, seconded by Ms. Thomas, to approve the Recipient Rights Reports for February 2024 / March 2024.

MOTION CARRIED.

For the months of February 2024 / March 2024, there were 61 HealthWest and 44 provider employees trained:

Rights Updates HealthWest	44
Rights Updates Provider	1
New Employee Training HealthWest/Contracted	16
New Employee Training Provider	23
SUD Recipient Rights Orientation Employee	0
SUD Recipient Rights Orientation Provider	20

For the months of February 2024 / March 2024 there were 685 incident reports and 23 rights allegations.

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

There were a total of 5 deaths reported in February 2024 / March 2024.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATIONS

Recipient Rights Advisor, Tasha Kuklewski, provided training on Confidentiality.

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 8:27 a.m.

Respectfully,

Thomas Hardy
HealthWest Rights Advisory Committee Chair

TH/hb

PRELIMINARY MINUTES
To be approved at the Rights Advisory Committee Meeting of
June 14, 2024



RECIPIENT RIGHTS ADVISORY COMMITTEE

April 12, 2024 – 8:00 a.m.

376 E. Apple Ave. Muskegon, MI 49442

Zoom: <https://healthwest.zoom.us/j/92247046543?pwd=ZXY0QnFPVGc5UVZENIRwcExTTmdvdz09>

Join by Phone: (312) 626-6799, 92718779426#

Recipient Rights Committee Chair: Thomas Hardy
Recipient Rights Committee Vice-Chair: Tamara Madison

AGENDA

- | | | |
|-----|---|-------------|
| 1) | Call to Order | Quorum |
| 2) | Approval of Agenda | Action |
| 3) | Approval of the Minutes of February 9, 2024
(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
February 2024 / March 2024 2024
(Attachment #2 – pg. 3-10) | Action |
| 6) | Old Business | |
| 7) | New Business | |
| 8) | Communication | |
| | A) Training Recipient Rights: Confidentiality
Tasha Kuklewski, Recipient Rights Advisor
(Attachment #3 – pg. 11-19) | Information |
| 9) | Audience Participation / Public Comment | |
| 10) | Adjournment | Action |

/hb

Main Office

376 E. Apple Ave. | Muskegon, MI 49442 | P (231) 724-1111 | F (231) 724-3659

[HealthWest.net](https://healthwest.net)

HEALTHWEST**RECIPIENT RIGHTS ADVISORY COMMITTEE MEETING MINUTES**

Friday, February , 2024
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 8:07 a.m.

ROLL CALL

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

HealthWest Staff Present: Holly Brink, Shannon Morgan, Amber Berndt, Rich Francisco, Gary Ridley, Kristi Chittenden, Tasha Kuklewski, Jennifer Hoeker, Gina Kim, Cyndi Blair, Kim Davis

Guest Present: Kristen Wade

APPROVAL OF MINUTES

It was moved by Ms. Natte, seconded by Ms. Hilleary, to approve the minutes of the December 1, 2023 meeting as written.

MOTION CARRIED.

ITEMS FOR CONSIDERATION***A. Motion to Accept Recipient Rights Reports for December 2023 / January 2024***

It was moved by Ms. Hilleary, seconded by Ms. Natte, to approve the Recipient Rights Reports for December 2023 / January 2024.

MOTION CARRIED.

For the months of December 2023 / January 2024, there were 108 HealthWest and 26 provider employees trained:

Rights Updates HealthWest	90
Rights Updates Provider	2
New Employee Training HealthWest/Contracted	15
New Employee Training Provider	25
SUD Recipient Rights Orientation Employee	0
SUD Recipient Rights Orientation Provider	0

For the months of December 2023 / January 2024 there were 593 incident reports and 12 rights allegations.

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

There were a total of 7 deaths reported in December 2023 / January 2024.

OLD BUSINESS

There was no old business.

NEW BUSINESS

There was no new business.

COMMUNICATIONS

Recipient Rights Advisor, Tasha Kuklewski, provided training on Abuse & Neglect.

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 8:23 a.m.

Respectfully,

Thomas Hardy
HealthWest Rights Advisory Committee Chair

TH/hb

***PRELIMINARY MINUTES
To be approved at the Rights Advisory Committee Meeting of
April 12, 2024***

REQUEST FOR HEALTHWEST BOARD CONSIDERATION AND AUTHORIZATION

COMMITTEE Recipient Rights Advisory Committee	BUDGETED X	NON-BUDGETED	PARTIALLY BUDGETED
REQUESTING DIVISION Administration	REQUEST DATE April 12, 2024	REQUESTOR SIGNATURE Linda Wagner, Recipient Rights Officer	
SUMMARY OF REQUEST (GENERAL DESCRIPTION, FINANCING, OTHER OPERATIONAL IMPACT, POSSIBLE ALTERNATIVES)			
<p>Approval is requested to accept the Recipient Rights Reports of February 2024 and March 2024. The report includes:</p> <ul style="list-style-type: none"> • Training sessions conducted by the Rights Office from February 15, 2024 through March 28, 2024. • Site Reviews from February 1, 2024 through March 31, 2024. • Incident Reports and Rights Allegations for February 1, 2024 through March 31, 2024. • Formal Complaints and Interventions for February 1, 202 through March 31, 2024. • Deaths reported for January 30, 2024 through March 23, 2024. 			
SUGGESTED MOTION (STATE EXACTLY AS IT SHOULD APPEAR IN THE MINUTES)			
<p>I move to approve the Recipient Rights Reports for the months of February 1, 2024 through March 31, 2024.</p>			
COMMITTEE DATE April 12, 2024	COMMITTEE APPROVAL _____ Yes _____ No _____ Other		
BOARD DATE April 26, 2024	BOARD APPROVAL _____ Yes _____ No _____ Other		



BI-MONTHLY RECIPIENT RIGHTS REPORT

Date: April 12, 2024
To: Recipient Rights Advisory Committee
From: The Office of Recipient Rights
Subject: Recipient Rights Report for February 2024 and March 2024

I. TRAINING

February 15, 2024 New Employee Training for 4 HealthWest and 3 Provider employees.

February 16, 2024, Rights Update Training for 23 HealthWest and 1 Provider employees.

February 20, 2024, Rights Update Training for 4 HealthWest employees.

February 22, 2024, New Employee Training for 6 HealthWest and 6 Provider employees.

March 8, 2024, Rights Update Training for 17 HealthWest employees.

March 13, 2024, Received notice that Tasha Kuklewski completed and passed Basic Skills I and II.

March 14, 2024, New Employee Training for 4 HealthWest and 8 Provider employees.

March 26, 2024, SUD Update for 20 Provider employees.

March 28, 2024, New Employee Training for 2 HealthWest and 6 Provider employees.

61 HealthWest and **44** Provider employees for a total of **105** people were trained for the months of February and March.

II. SITE REVIEW

February 22, 2024, Beacon Home at Leslie, residential mixed, out of county. Beacon Specialized Living, Leslie Michigan.

February 23, 2024, Beacon Home at Wolf Lake, residential mixed, out of county. Beacon Specialized Living, Kalamazoo, Michigan.

March 8, 2024, Harbor Pines, residential I/DD, MOKA, Norton Shores Michigan.

March 8, 2024, Forest Trail, residential I/DD, MOKA, Fruitport Michigan.

March 13, 2024, Organic Care Home, residential mixed, Muskegon, Michigan.

III. STATISTICAL INFORMATION

The Office of Recipient Rights reviewed **685** incident reports and received **23** rights allegations for the months of February and March. Provided below for your review is the statistical data showing type and location for all rights allegations for the past review period.

IV. FORMAL INVESTIGATIONS

Old Business:

- A. November 20, 2023, a Recipient served by HealthWest, MI Adult Case Management, said that staff at HealthWest did not treat her with Dignity and Respect by accusing her that she was “gaming the system.” **The investigation into DIGNITY AND RESPECT is not substantiated. During the investigation, it was found that the Recipient was given a Notice of Adverse Benefit Determination (NABD) without proper documented support. The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The Staff involved is no longer employed by HealthWest.**
- B. November 20, 2023, Walker Home, residential I/DD, HGA. A HealthWest Case Manager visited the home and found that they had an active door alarm on the front door. The Case Manager is not aware of anyone in the home who has a behavior plan in the home with this restriction. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**
- C. November 20, 2023, Crescent Home, residential I/DD, MOKA. A Recipient had fallen out of bed and sustained a laceration above his eye for which he needed medical attention. A family member does not believe that the Recipient did not accidentally fall out of bed but was injured by a staff member. **The investigation into ABUSE CLASS II-NON ACCIDENTAL ACT is not substantiated. During the investigation it was found that the Staff involved did not follow proper procedures, the investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The Staff involved transferred to a different home within MOKA.**
- D. November 27, 2023, West Lake Cottage 3, residential mixed, Hope Network. A staff member did not agree with how his coworkers were handling situations with a Recipient and felt they needed additional physical management training. **The investigation into**

MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The Staff involved were provided additional training.

- E. December 04, 2023, a Recipient served by HealthWest, MI Adult Case Management, said that he believes that a HealthWest staff that works with his ex-girlfriend told her confidential information about his treatment. **The investigation into DISCLOSURE OF CONFIDENTIAL INFORMATION is not substantiated.**
- F. December 14, 2023, a Recipient served by HealthWest, MI Adult Case Management, said that she would like to attend Clubhouse Interactions but is unable to due to accessibility issues. She uses a wheelchair and needs transportation. She was told that the Clubhouse is not able to provide her transportation but that she could use GO2 Transportation and pay a fee. She states she cannot afford this every month. She states that others in her building are provided transportation without having to pay for it. The Recipient feels that this is unfair. The recipient also states that the Clubhouse is not accessible, which prevents her from being able to participate as well. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**
- G. January 09, 2024, Mararebecah Home, residential I/DD, Samaritas. A recipient said that she was sent to the MOKA program without being given breakfast or having her wet brief changed. **The investigation into DIGNITY AND RESPECT is not substantiated.**
- H. January 10, 2024, Black Creek Cove, residential I/DD HGA. Staff was overheard to say, “Stop Betty or I’ll knock you out” while assisting the Recipient in the restroom. **The investigation into DIGNITY AND RESPECT is not substantiated.**
- I. January 11, 2024, a Recipient served by HealthWest I/DD Adult Case Management med box was not filled with the appropriate medications. She was not provided one of her prescribed medications for three months. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The Recipient was assigned to a new Case Manager, The Staff involved received Disciplinary Action and is scheduled to retake medication training.**
- J. January 17, 2024, Forest Trail Home, residential I/DD, MOKA. Staff say that a recipient was found absolutely drenched in urine from head to toe when they came in for their shift. Staff reported that the bed was also completely soaked. The responsible staff said that the Recipient had refused to use the bathroom or be changed. **The investigation into SAFE, SANITARY, AND HUMANE TREATMENT ENVIORMENT is substantiated. The Staff involved will be required to retake Recipient Rights, complete some additional trainings and was given an official final written reprimand.**
- K. January 22, 2024, a Recipient served by HealthWest, MI Adult Case Management. A Recipient said that her Primary Care Doctor was contacted without her permission by her med team at HealthWest. **The investigation into DISCLOSURE OF CONFIDENTIAL**

INFORMATION was not completed. NOTE: On January 23, 2024, the Recipient/Complainant asked to withdraw her complaint as she no longer wishes to have it investigated. The investigation was closed as of January 24, 2024.

- L. January 22, 2024, Walker Home, residential I/DD HGA. A Guardian filed a complaint that for the past year and a half, HGA Services has not provided a Recipient with good care including not ensuring that the Recipient's wheelchair was working appropriately. The Guardian feels that this is because of staff turnover. **The investigation MENTAL HEALTH SERVICES SUITED TO CONDITION is not substantiated.**

New Business:

- A. January 29, 2024, Morton Terrace, mixed residential, Beacon Specialized. The Home Manager reported that while completing a random check in on the home, a staff member was observed sitting in a kitchen chair and was asleep. **The investigation into SAFE, SANITARY, AND HUMANE TREATMENT ENVIROMENT is substantiated. The Staff involved was terminated.**
- M. February 01, 2024, Forest Trail Home, residential I/DD, MOKA. Home Manager returned from vacation and was told by several staff about an incident where a staff member had an altercation with a Recipient, during which the Recipient was slightly injured. **The investigation into DIGNITY AND RESPECT is substantiated. The Staff involved will be required to retake Recipient Rights, complete some additional trainings and was given an official final written reprimand.**
- B. February 08, 2024, Lilac Home, residential I/DD HGA. A Guardian contacted the Recipient Rights Office to express her deep concern about the conditions she observed during her last visit. She found the residence to be extremely dirty, with a pervasive smell of urine and garbage scattered in the yard. The Guardian also had concerns about the personal care of her two wards and if their diabetic diets were being followed. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITON is not substantiated.** During the investigation new information was discovered. **The investigation into Individualized Written Plan of Service is substantiated. The All Staff involved received additional training.**
- C. February 12, 2024, Mararebecah Home, residential I/DD, Samaritas. The Recipient was sitting in the AFC van outside of Family Dollar without a caregiver. The caregiver was in the store shopping while the resident was outside in the van with another Recipient. During the investigation, the identity of the other Recipient left in the van without a caregiver was discovered and they were added to the complaint. **The investigation into NEGLECT-CLASS III is substantiated. The Staff involved was terminated.**
- D. February 15, 2024, Mararebecah Home, residential I/DD, Samaritas. A friend of a Recipient said that cash and checks have been sent to the home and no one knows where the

money is. The friend said that the sister of the recipient has sent her money, and it has not been accounted for. The friend would like an accounting of the funds. **The investigation into ABUSE-CLASS II EXPLOYTATION is not substantiated.**

- E. February 20, 2024, Eastwood II, *mixed residential*, Turning Leaf. A HealthWest staff was told by the Recipient that he had a recent conflict with an employee at his home. The Recipient showed the HealthWest Staff a dime size bruise on the top of his hand that appeared to be healing. The Recipient said that he received the bruise when the Home Staff slammed his hand in his bedroom door. **The investigation into SAFE, SANITARY AND HUMANE TREATMENT ENVIORMENT is substantiated.** It was also determined during the investigation that several staff had failed to report incidents that had occurred in the home. **The investigation into NEGLECT-CLASS II-FAILURE TO REPORT is substantiated. The Staff involved was required to review policies, retake Recipient Rights Training and was given written disciplinary action according to policy.**
- F. February 26, 2024, Beacon Home at Luddington, *mixed residential*, Beacon Specialized. A Staff of the home was in a bad mood and was very snappy and rude all day. **The investigation into DIGNITY AND RESPECT is substantiated. The Staff involved received training and issued a letter of apology to the Recipient.**
- G. March 4, 2024, Recipient receiving services from Pioneer CLS Group, The Recipient was in the community when a staff person was pushing the Recipients wheelchair while pulling another Recipient in a wheelchair. The Recipient's tire caught the curb tipping over and the Recipient received an injury to the forehead that required stitches. The complaint goes on to state that the details of the incident were not accurate in the Incident Report and that there is a video of the incident which shows the staff was negligent. **The investigation into NEGLECT-CLASS III is substantiated. The Staff involved received verbal/written discipline and all staff were re-trained on mobility assistance training.**
- H. March 8, 2024, Sheridan Home, *residential I/DD*, Pioneer Resources. Case Manager was made aware that the Recipient had been referred to a specialist, but the home had not followed up on the referral. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is substantiated. The corrective action plan is pending.**
- I. March 25, 2024, Brooks Home, *residential I/DD*, Samaritas. HealthWest Staff stated that the AFC home is not getting the Recipient to her appointments as required by what is written in the IPOS intervention. Medication review scheduled with the psychiatrist on 3/20/2024. Recipient was not seen at the office; the case manager contacted the home manager who stated she would look into it. Not much later, an email was sent stating the home just called to cancel the appointment and reschedule due to "construction in the facility". Her appointment was rescheduled to 4/3/2024. She will be out of medication due to this rescheduling as a medication bridge was already sent

in once to cover the late scheduling. The Integrated Health Clinic report the home called and cancelled a scheduled appointment on 10/20/2023 then no-showed. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is not complete.**

- J. March 25, 2024, Forest Trail Home, residential I/DD, MOKA. A Recipient attached a staff person and then fell and his face which caused bleeding and a laceration on his top lip which was about half an inch and swollen, his left eye was very swollen and was starting to bruise. When asked by another staff, what happened, the recipient said that he hit the guy (the other staff). The Recipient was taken to urgent care for medical treatment. **The investigation into ABUSE CLASS II-UNREASONABLE FORCE is not substantiated.**
- K. March 26, 2024, Turning Leaf SIL, mixed residential. Team RN was informed by injection clinic staff that client has received their medication injection on 3/16 by staff at Turning Leaf SIL where client resides. Staff at the SIL are not trained on administering injection. **The investigation into NEGLECT CLASS III is not complete.**
- L. March 26, 2024, Ducey Home, residential I/DD, Samaritas. HealthWest Team has received many incident reports regarding recipient eating dirt while outside or falling while trying to come back inside. Behavioral support plan states that client must be watched 24/7 when he is outside. **The investigation into MENTAL HEALTH SERVICES SUITED TO CONDITION is not complete.**
- M. March 27, 2024, Lilac Home, residential I/DD, HGA. HealthWest Case Manager stated that HGA management is not allowing home staff to spend Recipients personal funds above \$40.00 without consulting with them first. HGA is not allowing for personal choice as they are not allowing the Recipient to purchase a specific type of shoe that he has voiced he want to purchase as well as his right to celebrate his birthday. The Recipient has also stated that he wants a haircut and to go out to eat at Bob Evans. **The investigation into PERSONAL PROPERTY-LIMITATIONS is not complete.**
- N. March 27, 2024, Lilac Home, residential I/DD. HeathWest Case Manager stated that HGA management is not allowing home staff to assist Recipient in spending their funds for personal needs/wants. The Recipient needs new clothes, belt, shoes, underwear, socks, recliner, new DVD player, etc. HGA does not allow personal choice as they are not allowing the Recipient to buy personal necessities. **The investigation into PERSONAL PROPERTY-LIMITATIONS is not complete.**
- O. March 27, 2024, Forest Trail Home, residential I/DD, MOKA. The Home Manager at Forest Trail asked a Recipients Guardian to speak with the Recipient about taking his PM medications and not spitting them out. The Guardian said that she had the Recipient stay overnight on March 15, 2024, and when giving him his PM meds the Guardian talked about him taking them. The Recipient told his Guardian he did not want to take

the medication no more. The Guardian said that is when the Recipient told her that a staff person at Forest Trail crushed the meds put them on a spoon and shoved it into his mouth. The Guardian notified Forest Trail staff what Recipient told her. **The investigation into DIGNITY AND RESPECT is not complete.**

V. INTERVENTIONS

Old Business: n/a

New Business:

- A. February 24, 2024, Beechwood Crisis-Pine Rest, Grand Rapids. A Recipient receiving inpatient services was given the wrong medication. The recipient was monitored for the next eight hours. **This is out of our Jurisdiction and referred to the Office of Recipient Rights at Pine Rest.**

VI. SUBSTANCE USE DISORDER

Old Business: n/a

New Business:

VII. DEATHS

- A. January 30, 2024, 62 year old male, who resided at Joseph's Home AFC and received I/DD Case Management, died unexpectedly from Pneumonia/Covid-19.
- B. February 04, 2024, 55 year old male who resided at the Lawrence AFC Home and received I/DD Case Management, died of natural causes. The Recipient had been placed on hospice after a brief hospitalization.
- C. February 19, 2024, 79 year old male who resided at the Riverwood AFC Home and received I/DD Case Management, died expectantly from choking while at home.
- D. February 27, 2024, 39 year old female receiving MI Adult Case Management, died of an unknown cause. Health issues included: uncontrolled diabetes, gastroparesis, and substance use.
- E. March 23, 2024, 44 year old female receiving MI Adult Case Management died of an accidental/natural death after being seen for a hernia on March 18, 2024. She was living independently in the community when she began to having breathing issues and died at home.

CONFIDENTIALITY

○ A VOW TO KEEP INFORMATION
PRIVATE AND OUT OF PUBLIC VIEW



This Photo by Unknown Author is licensed under [CC BY-SA-NC](#)

HIPAA

HIPAA is a federal law that protects *health information*.

In many cases, it would allow information to be shared that the more protective **Michigan Mental Health Code** will not allow.

OPEN ACCESS

[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

PRIVILEGED
INFORMATION

INFORMATION THAT IS
SHARED BETWEEN THE
RECIPIENT
AND
A MENTAL HEALTH
PROFESSIONAL



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



MANDATORY DISCLOSURE

DISCRETIONARY WITH CONSENT

DISCRETIONARY

THE DREADED PHONE CALLS

A preferred method for answering the phone so as not to disclose information

"I'm here to assist you, but please understand that we prioritize the confidentiality of our clients. Let's discuss your concerns in a way that protects everyone's privacy."



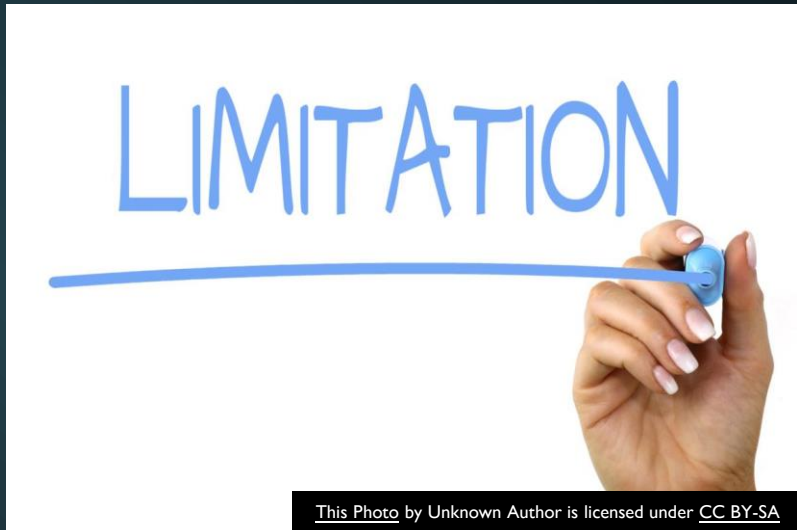
This Photo by Unknown Author is licensed under [CC BY](#)

PRIVILEGED COMMUNICATIONS

- Mail, email
- Telephone, cellphone, text messages
- Visitors



LIMITATIONS



The Mental Health Code guarantees that persons receiving services in a hospital or residential setting shall be assured that some basic rights will be protected. These rights may be limited due to the nature of your treatment. If limitations are imposed, you (or our legal representative) must agree to them as part of your plan of service. General restrictions (visiting hours, telephone usage, access to property) can be established for inpatient settings. Revised Home and Community-Based Service rules do not allow restrictions to be enforced in residential settings.

ACCESS TO RECORDS

PRIVILEGED INFORMATION

Access to their Records.

- Consumers have the right to see their treatment records.
- Consumers receiving services have the right to get a second opinion if they are not in agreement with some aspect of the service plan.
- Recipients have the right to refuse to participate if they disagree with their individual plan of service.

Privileged Information. Any and all information about a recipient is confidential and is only to be discussed at work with appropriate staff members.