DEPARTMENT:	Compliance	**ORIGINAL APPROVAL:**	04/14/2003
POLICY #:	CO298	**LAST APPROVAL:**	02/25/2019
TITLE:	Member Privacy		
APPROVED BY:	Ethics Committee		
DEPENDENCIES:	*Member Privacy – PHI and Member Rights* procedure (CO315) *Member Privacy – PHI Use & Disclosure* procedure (CO316) *Information Privacy – Workforce Member Responsibilities* procedure (CO317) *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367) *HIPAA & Privacy/Security Safeguards Violations* policy (CO325) P*rivacy Incidents & Breach Notifications* policy (CO311) *Privacy Incidents & Breach Notifications* procedure (CO312) *Compliance Education Program* policy (CO293) *HIPAA Security* policy (CO330) *Employee Network and Facility Access Authorization MAC Form* procedure (CO335) *Corrective Action & Discipline* policy (EE204)		

PURPOSE

This policy is designed to ensure Community Health Plan of Washington's (CHPW) compliance with the Health Insurance Portability and Accountability Act (HIPAA), Privacy and Security Rules, and related state and federal regulatory privacy and security requirements.

NOTE: Refer to *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367) for substance use disorder treatment records considerations and refer to *HIPAA Security* policy (CO330) for security provisions and additional technical and administrative safeguards.

POLICY

CHPW, in accordance with HIPAA and to meet the requirements of related federal and state laws, ensures the privacy and security of member's protected health information (PHI) and other sensitive, confidential, and proprietary business information. CHPW's workforce members[1] and Business Associates (BA) must comply with this policy.

PRIVACY OFFICER[2] ADMINISTRATION OF MEMBER PRIVACY PRACTICES

CHPW shall designate a Privacy Officer to administer its privacy practices (45 CFR § 164.530(a)(1)).[3] The Privacy Officer shall develop, implement, and maintain the following:

[1] The term "workforce members" is defined as an employee (including the CEO, Senior Administrator, Manager, governing body) and may be referred to throughout the document as staff, temp staff, volunteer, agent, and employee.

[2] References to the Privacy Officer, refers to CHPW's Compliance Officer.

[3] NCQA RR 4 G

- Policies and procedures to protect PHI and sensitive, confidential, and proprietary business information, including protections for PHI sent to plan sponsors
- Mechanisms to oversee the application of CHPW's privacy policies and procedures
- Levels of user access
- A process to identify unnecessary PHI collection
- Mechanisms to limit access to PHI
- A process to review non-routine requests to use PHI
- Processes for managing physical and electronic access to sensitive, confidential, and proprietary business information
- Processes for taking appropriate action when policies regarding internal protections of oral, written, and electronic information protections are violated or prove insufficient
- Mechanisms to ensure that the appropriate state and federal agencies are notified in the event of a privacy incident
- Processes to ensure that members have access to information about their rights under HIPAA and CHPW's privacy policies and procedures, including through the availability and dissemination of CHPW's *Notice of Privacy Practices*
- Mechanisms to receive and answer member privacy complaints
- Mechanisms to review written requests from members exercising their rights under HIPAA
- Processes to ensure that CHPW complies with HIPAA's provisions regarding BA and that CHPW has a HIPAA-compliant Business Associate Agreement (BAA)
- Processes to ensure that HIPAA-related training is delivered to CHPW workforce members on at least an annual basis
- Processes to report all of the above, as appropriate, to the Compliance and Ethics Committees

ACCOUNTABILITY & RESPONSIBILITY: ANNUAL WORK PLAN[4]

Annually, the Privacy Officer with the support of the Compliance department shall design and implement privacy and security monitoring and auditing activities as part of the annual *Compliance Program Work Plan*. Privacy and security activities shall be designed around industry best practices, regulatory recommendations, and self-discovery resulting from prior internal/external auditing, monitoring, and survey results.

The Compliance department conducts a quarterly Privacy and Security Audit to check adherence to CHPW privacy and security policies and related procedures, to verify workforce members understand compliance requirements, and to identify and report areas of risk and

[4] NCQA RR 4 F.1

process improvement opportunities to CHPW's Executive Leadership Team (ELT) and Compliance Committee.

Additional related information may be gathered and logged on an ongoing basis through ad hoc reports from workforce members, first tier, downstream, and related entities (FDR), and members.

The Privacy Officer will involve the Compliance Committee, which is comprised of high-level staff across departments, in periodic discussion to identify unnecessary PHI collection. If identified, the Privacy Officer will engage key staff to design mitigations and address root cause(s).

Reporting Impermissible Uses or Disclosures[5]

Workforce members shall be trained to identify impermissible uses and disclosures of sensitive information to be referred through Privacy Incident Reports to the Privacy Officer or their designee for logging, investigation, risk assessment, and member/agency notification (when applicable) as describe herein and in policy *Privacy Incidents & Breach Notifications* (CO311) and procedure *Information Privacy: Workforce Member Responsibilities* (CO317).

The results of privacy and security audits, Privacy Incident Reports, and other relevant data shall be summarized and reported to the Compliance Committee and the Ethics Committees for review and recommendation.

Non-compliant behavior discovered by the Compliance department shall be reported timely, as applicable based on the severity of the instance, to appropriate management and the Human Resources department. Corrective actions shall be applied as described below under "Sanctions" and associated policies *HIPAA & Privacy/Security Safeguards Violations* (CO325) and *Corrective Action and Discipline* (EE204).

HIPAA PRIVACY & SECURITY RULE & PHI

The HIPAA Privacy Rule established standards for the protection of certain health information, known as protected health information (PHI). PHI goes beyond a member's name, and includes demographic or other information that can reasonably be used to identify a member. The HIPAA Security Rule establishes standards for protecting PHI that is held or transferred in electronic form, such as information contained in an electronic health record system and information transmitted by a computer or mobile device. By their nature, social media HIPAA incidents are bound by both the Privacy and Security rules.

[5] NCQA RR 4 F.2

PHI includes all individually identifiable health information collected from an individual, including demographic information, that:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and,
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and:
  - Identifies the individual; or,
  - Gives a reasonable basis to believe that the information can be used to identify the individual.

NOTE: PHI also includes race/ethnicity and language information[6].

Any PHI which is created, stored, transmitted, or received electronically is referred to as Electronic Protected Health Information (ePHI). For the purposes of this policy, ePHI will be referred to as PHI.

PHI & MEMBER RIGHTS

CHPW shall honor its members' right to:

1. Access and inspect their own PHI
2. Request changes or corrections to their own PHI
3. Request restrictions on the use and disclosure of their own PHI
4. Obtain an accounting of certain PHI disclosures that CHPW has shared with others
5. Request alternate ways to receive communications about their own PHI
6. Receive a *Notice of Privacy Practices*

No Waiver of HIPAA Privacy Rights

It is CHPW's policy that no member shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility.

Member Communications of PHI Use and Disclosure[7]

CHPW shall ensure that members are informed about their rights and about CHPW's PHI use and disclosure practices, through its *Notice of Privacy Practice*. The *Notice of Privacy Practices* is mailed to members upon enrollment. After enrollment, members are notified annually by mail that *The Notice of Privacy Practices* is available on CHPW's websites (www.chpw.org and http://healthfirst.chpw.org) and that a paper copy may be requested by contacting CHPW's

[6] NCQA MHC 1.C

[7] NCQA RR 4 E

Customer Service team. Members shall be sent a copy of the Notice within 60 days of a material change.

The Notice of Privacy Practices includes information about:

- The routine use and disclosure of PHI
- The use of authorizations
- How a member may access, request restrictions on use and disclosure, request amendments, and request an accounting of disclosures of his or her PHI
- Procedures CHPW uses internally to protect oral, written and electronic PHI
- Protections CHPW requires when information is disclosed to plan sponsors or employers
- CHPW's complaint procedure with a mailing address and phone number to contact the Privacy Officer for further information
- The date of the notice

Additional information on member rights and a copy of the *Notice of Privacy Practices* may be found in procedure *Member Privacy: PHI & Member Rights* (CO315).

USE & DISCLOSURE

Under the Privacy Rule and the provisions of this policy, CHPW may not use or disclose PHI except:

- As the Privacy Rule requires (*mandatory* use and disclosure)
- As the Privacy Rule permits (*permitted* use and disclosure)
- As the member who is the subject of the information (or their personal representative) authorizes in writing

Procedure *Member Privacy: PHI Use and Disclosure* (CO316) details the ways in which PHI may be used and disclosed and the steps CHPW takes to maintain member privacy rights related to use and disclosure.

Minimum Necessary Standard

CHPW shall observe the minimum necessary standard by making reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

CHPW shall restrict workforce member access to PHI in cooperation with all departments and with oversight by the Privacy Officer.

Workforce Member Confidentiality Agreement

It is a provision of this policy that workforce members must sign an *Employee Confidentiality Agreement* (Appendix A) as a condition of employment. Any breach of confidential member

information may be grounds for dismissal. Contracted providers must agree to have policies and procedures in place in their offices to preserve member confidentiality and to ensure compliance with HIPAA. Such an agreement is a term of the provider's contractual relationship with CHPW.

Mitigation of Impermissible Disclosures of PHI

CHPW shall mitigate, to the extent possible, any harmful effects that become known from the use or disclosure of an individual's PHI in violation of HIPAA regulations or CHPW policies and procedures. If workforce members, contractors, consultants, or Business Associate's (BAs) become aware of an impermissible use or disclosure of PHI, they must immediately report the incident to the Compliance department via the *Privacy/Security Incident Form* found on the Compliance department's page on Inside CHPW. The Privacy Officer or their designee will investigate the incident and determine appropriate actions to mitigate harm to the individual. Detailed information about reporting privacy incidents may be found in *Information Privacy: Workforce Member Responsibilities* procedure (CO317) and the *Privacy Incidents & Breach Notification* policy (CO311) and procedure (CO312).

INTERNAL PROTECTIONS OF ORAL, WRITTEN & ELECTRONIC INFORMATION

The HIPAA Security Rule relates to the electronic and physical security of PHI. Under the provisions of this policy and its associated procedures, CHPW shall protect PHI through the use of administrative, physical, and technical security safeguards. Policy *HIPAA Security* (CO330) describes administrative and technical safeguards in addition to the provisions outlined herein.

Administrative Safeguards

CHPW maintains written policies and procedures for maintaining the privacy and security of member privacy. To ensure compliance with HIPAA and all related Federal and State regulations, CHPW reviews and approves its policies and procedures annually.

Physical Safeguards and Protections for Physical Facility Access[8]

CHPW shall control physical access to PHI to prevent inappropriate access to protected data through the provision of measures such as locking filing cabinets and by controlling facility access through a badge security system. Access doors to CHPW's facilities, server room, Intermediate Distribution Frame (IDF) closets, and contract rooms shall be kept locked at all times.

It is the policy of CHPW that full and part-time workforce members, temporary workforce members, contractors, vendors, providers and their staff (whether contracted or non-

[8] NCQA RR 4 B.1

contracted), board members, and all other visitors must visibly wear an ID badge while at its facility. In addition, visitors must be escorted by a CHPW employee at all times.
Access card holders are not to tailgate (follow another through a secured door without swiping their badge first). Workforce members must stop anyone they observe tailgating and should remind them to swipe their badge before entering.
Note: if a workforce member forgets their badge at their workstation, another workforce member may escort them to their desk to retrieve their access card.

Anyone issued a badge shall immediately report any lost or stolen badge and any unsecured access point of CHPW's facility to the Privacy Officer and the Facilities department.
Workforce members shall be trained at minimum annually on the physical safeguard provisions of this policy and its associated procedures, and adherence shall be routinely monitored by the Compliance department.

Specific provisions for the physical security of PHI are detailed in procedure *Information Privacy: Workforce Member Responsibilities* (CO317) and additional provisions for facility security are described in CHPW's *Facility Badge Access* procedure (FA303).

Technical Safeguards and Protections for Electronic Access

CHPW shall control access to its computer systems and networks to protect electronically transmitted communications containing PHI from being intercepted by anyone other than the intended recipient. CHPW shall grant workforce members access to its systems based on role as described in procedure *Member Privacy: PHI Use and Disclosure* (CO316) and procedure *Employee Network and Facility Access Authorization MAC Form* (CO335). Please see policy *HIPAA Security* (CO330) for information on additional safeguards.

PROTECTIONS FOR PHI SENT TO PLAN SPONSORS[9]

CHPW prohibits the sharing of member PHI with a sponsor of the Plan that does not amend its documents and incorporate provisions therein to:

- Not use or disclose PHI other than as permitted by the provision of this policy and its associated procedures, or as required by law
- Ensure that agents and subcontractors of the plan sponsor agree to the same restrictions and conditions as the plan sponsor with regard to PHI
- Prohibit the use of PHI by the Plan sponsor for employment or other benefit-related decisions
- Notify CHPW of any use or disclosure of PHI that is inconsistent with use and disclosure as provided by this policy and its associated procedures
- Allow members to access and amend their own PHI

[9] NCQA RR 4 C.1-9

- Make necessary information available to CHPW in order to provide individuals with accountings of disclosure
- Return, destroy, and restrict further use of PHI as proscribed by this policy and its associated procedures
- Identify the sponsor staff who have access to PHI

CHPW will take action against any sponsor or sponsor staff that inappropriately use or disclose PHI.

SANCTIONS[10]

Sanctions for using or disclosing PHI in violation of HIPAA regulations or CHPW's policies and procedures are imposed according to procedure *HIPAA & Privacy/Security Safeguards Violations* (CO325) and policy *Corrective Action and Discipline* (EE204). Violations may result in corrective action, up to and including termination of employment or contract.

Corrective Action for Business Associate Violations

BAs who do not meet CHPW performance standards or who violate laws and regulations, including those related to HIPAA privacy and security, may be placed on a corrective action plan or may face additional sanctions, up to and including termination of the BA's contract as described in procedure *HIPAA & Privacy/Security Safeguards Violations* (CO325).

Additional Penalties for Violations of State or Federal Laws and Regulations

Workforce members or BA's who knowingly or willfully violate state or federal law for improper use or disclosure of an individual's PHI are subject to criminal investigation and prosecution, as well as potential civil monetary penalties.

Duty to Report

Any workforce member or BA who observes, becomes aware, or suspects a security issue or wrongful access, use, or disclosure of PHI maintained by CHPW is required to immediately report such to their supervisor, CHPW business contact, or the Privacy Officer. Failure to report may result in disciplinary action.

No Intimidating or Retaliatory Acts

No workforce member or BA shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice. Any intimidating or retaliatory acts by a CHPW workforce member or BA may result in criminal penalties and termination of employment or contract.

[10] NCQA RR 4 F.3

Exceptions to HIPAA Sanctions

Whistleblower Protections

HIPAA sanctions do not apply to whistleblowers when a workforce member who discloses PHI believes in good faith that CHPW has engaged in conduct that is unlawful or otherwise violates professional standards, or that the care, services, or conditions provided by CHPW potentially endangers one or more members, workers, or the public, and the disclosure is made to:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or,
- An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options of the workforce member with regard to the conduct in question.

Workforce Crime Victims

HIPAA sanctions do not apply to a member of the workforce who, as the victim of a criminal act, discloses PHI to a law enforcement official, provided that the PHI disclosed is:

- About the suspected perpetrator of the criminal act, and
- Limited to the following:
  - Name and address
  - Date and place of birth
  - Social Security number
  - ABO blood type and RH factor
  - Type of injury
  - Date and time of treatment
  - Date and time of death, if applicable
  - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos

Exceptions for Individuals Who Take Certain Actions

HIPAA sanctions do not apply to workforce members who use and/or disclose PHI in the course of:

- Filing a complaint with HHS under the HIPAA administrative simplification enforcement provisions
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the administrative simplification provisions of HIPAA

- Opposing any act or practice that is unlawful under the privacy rule, if the individual has a good faith belief that the act or practice is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI that violates the Privacy Rule

EDUCATION & TRAINING

It is CHPW's policy to annually train and educate workforce members and contractors who provide administrative or health care services related to CHPW members on HIPAA as described in CHPW's *Compliance Education Program* policy (CO293).

DOCUMENTATION & RECORD RETENTION

This policy and its associated procedures shall be reviewed and updated annually or changed as necessary to comply with changes in the law, regulations, standards, requirements, and implementation specifications. In accordance with HIPAA, CHPW's *Member Privacy* policy and procedures shall be documented and maintained for at least ten years from the date last in effect.

CHPW shall document, in either written or electronic form, certain events or actions (including authorizations to release information, requests for information, sanctions, and complaints) relating to a member's privacy rights. CHPW will maintain such documentation for a period of at least ten years.

LIST OF APPENDICES

A. Employee Confidentiality Agreement

CITATIONS & REFERENCES

CFR	45 CFR §160,162,164	
WAC	WAC 284-04-500 Health information privacy policies and procedures	
RCW		
CONTRACT CITATION	☒ WAH	
	☒ MA	
	☒ IMC	
OTHER REQUIREMENTS	– PUBLIC LAW 104-191, AUGUST 21, 1996,HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (FOR DEFINITIONS AND SUBSTANCE)	
NCQA ELEMENTS	NCQA RR4: PRIVACY AND CONFIDENTIALITY	

REVISION HISTORY

REVISION DATE	REVISION DESCRIPTION	REVISION MADE BY
04/14/2003	Original	Maryann Schwab
04/02/2006	Formatting	Maryann Schwab
09/02/2008	Formatting and content	Sunny Otake
09/17/2008	Review	Alan Brandon
10/20/2008	Approval	Marilee McGuire
10/02/2009	Revised policy to remove procedure information.	Alan Brandon
10/27/2009	Reformatted; summarize associated procedures in policy; add NCQA citations; attach appendices	Jennifer Carlisle
10/27/2009	Review, edit, and comment	Marie Harris Alan Brandon
11/23/2009	Approved	Alan Brandon
03/25/2010	Revised to meet NCQA requirements; incorporated policy FA302 (Facility Access) and retired FA302	Jen Carlisle, Alan Brandon
04/05/2010	Approval	Alan Brandon
04/20/2010	Updated NCQA Citation Footnotes	Jen Carlisle
09/30/2010	Approval	Alan Brandon
12/09/2010	Approval	Ethics Committee
12/22/2010	Detailed how members are notified of privacy rights	Jen Carlisle
12/27/2010	Provisional Approval	Marie Zerda
11/14/2011	Annual review with minor edits for clarity	Jen Carlisle, Marie Zerda
11/30/2011	Provisional Approval	Marie Zerda
12/08/2011	Minor revision to badge access; Approval	Ethics Committee
11/03/2012	Annual review with minor edits for accuracy	Jen Carlisle
11/06/2012	Provisional Approval	Marie Zerda
11/14/2012	Approval	Ethics Committee
12/06/2013	Provisional Approval	Marie Zerda
11/11/2014	Annual Review	Josh Martin
11/25/2014	Provisional Approval	Marie Zerda
	Review – updated confidentiality agreement	Josh Martin
12/15/2014	Provisional Approval	Marie Zerda
04/15/2015	Approval	Ethics Committee

04/11/2016	Review	Wendie Levy
04/13/2016	Provisional Approval	Marie Zerda
05/25/2016	Approval	Ethics Committee
07/12/2016	Provisional Approval	Marie Zerda
09/22/2016	Approval	Ethics Committee
04/26/2017	Review	Amie Schippa
04/28/2017	Provisional Approval	Marie Zerda
06/15/2017	Approval	Ethics Committee
02/22/2018	Review & Provisional Approval	Marie Zerda
03/21/2018	Approval	Ethics Committee
02/25/2019	Review	Amie Schippa
02/25/2019	Provisional Approval	Marie Zerda
	Approval	Ethics Committee

INDEX OF NCQA CITATION FOOTNOTES

NCQA RR 4 B.1 6

NCQA RR 4 C.1-9 7

NCQA RR 4 E 5

NCQA RR 4 F.1 3

NCQA RR 4 F.2 3

NCQA RR 4 F.3 8

NCQA RR 4 G 1-6 2

NCQA MHC 1.C

APPENDIX A: EMPLOYEE CONFIDENTIALITY AGREEMENT

Community Health Plan of Washington
Community Health Network of Washington

EMPLOYEE CONFIDENTIALITY AGREEMENT

I understand and agree that, as an employee, short-term or long-term contractor or consultant, or intern of Community Health Plan/Community Health Network, I am responsible for maintaining and protecting the security and confidentiality of all information received because of my employment and/or contract. This responsibility includes, but is not limited to client health care information, information concerning other employees of Community Health Plan/Community Health Network, and confidential business information. Confidential information includes, but is not restricted to: medical records, case histories, diagnoses, identification numbers, financial reports, patient and/or group billing and accounting data, personnel records, payroll information, technical or operational materials, provider and payor contracts.

I agree not to access/disclose information I receive because of my employment or contractual employment with Community Health Plan/Community Health Network, except to the extent necessary to carry out my job responsibilities.

I understand that any unauthorized disclosure of information or violation of policies, procedures or laws resulting in a breach of confidentiality, security or compromise of proprietary business information shall be cause for disciplinary action, up to and including termination of employment or possible legal action under applicable state and federal laws.

I have read, understand, and agree to comply with Community Health Plan's Confidentiality Policy.

Employee Name (please print clearly):

_____

_____ _____

Employee Signature Date